SECURE DISTRIBUTED DATABASE COMMUNICATION USING NTRU ALGORITHM

[1]Amneet Kaur, [2]Mrs. Meenakshi Bansal
[1]M.Tech Student, [2]Assistant Professor
Computer Engineering Department, Yadavindra College of Engineering,Talwandi Sabo,
Punjabi University, Patiala
Email-[1]aksekhon487@gmail.com, [2]ermeenu10@gmail.com

ABSTRACT

Distributed database plays a vital role in day to day life because in the present era, business environment is increasing at very fast rate so our basic desire is to get reliable information from any source. Since our database is distributed, means data is located at different geographical locations and finally helps to easily access our valuable & precious data. We propose an architecture that integrates cloud database services with data integrity and the possibility of executing concurrent operations on encrypted data. It is the solution supporting geographically distributed clients to connect directly to an encrypted cloud database, and to execute the concurrent and the independent operations including those modifying the database structure. Distributed database is the emerging technique which focuses on concurrency control and security issues under this distributed database. In this research work, data security is enhanced by using NTRU (N-th degree Truncated polynomial Ring Unit or Number Theory Research Unit) asymmetric key algorithm in which the different keys are used for encryption of plaintext and decryption of ciphertext. These keys are named as public and private keys. NTRU being fast and secure hashing algorithm which will provide more security to the system, in terms of throughput and their processing speed. Its main characteristics are the low memory and computational requirements as providing a high security level. It is a very well-organized public-key cryptosystem. MD5 hash function is also used for checking data integrity during the authentication process.

Keywords: Distributed database, Cloud database, Concurrency control, NTRU, Security, MD5 hash function, Encryption, Decryption.

I. INTRODUCTION

A distributed database is defined as a database in which the storage devices are not all connected to a common processing unit such as CPU, controlled by a distributed database management system. It may be stored in multiple computers, located in the same physical location or may be dispersed over the network of interconnected computers. The distributed database system consists of the loosely coupled sites that will share no physical components. The system administrators can distribute the collections of data across the multiple physical locations. A distributed database can reside on the network servers on Internet or on the other company networks because they store the data across the multiple computers, the distributed databases can improve performance at end-user worksites.

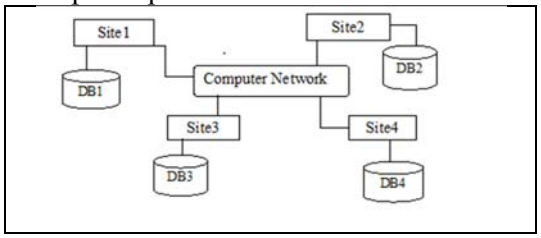


Figure 1.1: Distributed Database Systems [10]

In Figure1.1 of distributed database their present three sites with their respective databases, all of

these are connected through the means of computer network. Distributed database has many benefits due to which it is widely used in business organization because main factor which it includes is performance.

Cloud database management system (CDBMS) is defined as the distributed database that delivers a query service across multiple distributed database nodes located in the multiple geographically-distributed data centers, both corporate with the cloud data centers. Database accessible to the clients from the cloud will be delivered to the users on demand via Internet from a cloud database provider's servers.

But Security of distributed database system is main issue. There are various encryption algorithms used for security of data packets or files send from a one system to other system on Distributed Network. Encryption is a process of converting information in hidden form. So that it is intelligible only to someone who knows how to decrypt it. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. In our work, Encryption and Decryption of data over distributed network have been performed by using NTRU encryption algorithm. In our work we also implemented the MD5 hash function which is used for checking the data integrity during the authentication process so that only the authorized user can access the distributed database system.

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 encryption time, decryption time and authentication time.

Bhullar *et al.* [4], addressed that the 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. In this paper we are going to analyze the NTRU algorithm, based Encryption decryption technique for security to Distributed Database System.

Ferretti *et al.* [5], revealed that placing critical data in the hands of a cloud provider should come with guarantee of security and availability for data at rest, and in motion. Some alternatives exist for the storage services, while the data confidentiality solutions for the database as a service paradigm are still immature. It describes the architecture that integrates cloud database services with data confidentiality and the possibility of executing the concurrent operations on encrypted data.

Li J. *et al.* [16], informed that data de-duplication is a technique for eliminating duplicate copies of data, and has been widely used in cloud storage to reduce storage space and upload bandwidth. However, there is only one copy for each file stored in cloud even if such a file is owned by a huge number of users. As a result, de-duplication system improves storage utilization while reducing reliability. Furthermore, the challenge of privacy for sensitive data also arises when they are outsourced by users to cloud. Aiming to address the above security challenges, this paper makes the first attempt to formalize the notion of distributed reliable de-duplication system by using ramp secret sharing scheme.

Mekala *et al.* [18], described that cloud computing is one of the most increasing one with the increase number of cloud users. In today's environment every user wants to access their data at any time and at anywhere. In an organization they store the data only on their computers, if they want their data during the roaming situation means it is not possible one to carry the data at every time, this is a difficult factors for an organization. The Cloud computing can address this problem by providing data storage mechanism to access the data at anywhere.

Mote *et al* [20], said about the 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. The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks by hackers and its speed and efficiency.

Ranjan R. et al. [21], stated 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.

Wang *et al.* [26]**,** stated that due to its simplicity, portability and robustness, two-factor authentication has received much interest in the past two decades. Security-related issues have been well studied. Kim–Kim presented an efficient two-factor authentication scheme that attempts to provide user anonymity and to guard against various known attacks, offering many merits over existing works. However, in this paper we shall show that user privacy of Kim–Kim's scheme is achieved. As the main contribution, an enhanced scheme with provable security is suggested.

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 Figure 3. [10]

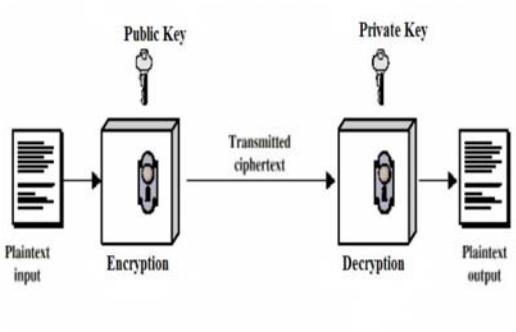


Figure 3 Working of NTRU algorithm

It is based on polynomial arithmetic; therefore it provides very fast computation for the encryption and decryption of the message. NTRU has less complexity. 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:

$$a = a_0 + a_1 X + a_2 X^2 + \ldots + a_{N-2} X^{N-2} + a_{N-1} X^{N-1}$$

Actually the NTRU is a parameterized 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 cipher text:

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

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

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

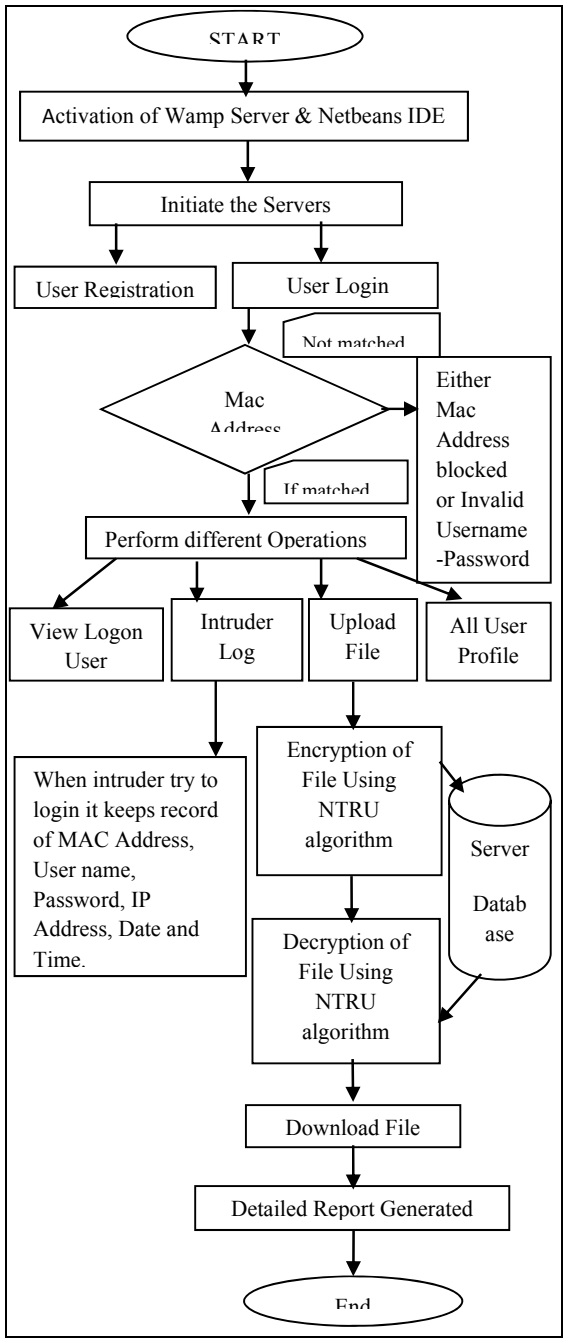
Bob then selects a ε R to satisfy this congruence and to lie in a certain pre-specified subset of R. He next does the mod p computation fq-1 * a (mod p) and the value he calculates is equal to m modulo p [11]. The main characteristics of NTRU algorithm are low computational and memory requirements for providing a high level security. In this algorithm the difficulty is faced during the factorization 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, RSSS (Ramp Secret Sharing Scheme) was implemented for Secure Distributed Deduplication Systems with Improved Reliability. The shares of a file are shared across multiple cloud storage servers in a secure way. But the time taken for encryption and decryption of file using this scheme is more due to which some problems may occur related to the security of file sharing on distributed network .To overcome it NTRU algorithm is used in this research work. In the previous work SHA1 hash function is used for checking integrity and consistency of data during authentication process but now in this work we have implemented the MD5 hash function which is less time consuming and more secure.

The first objective of proposed work is to develop a secure distributed database so that only the authorized user can access the database for uploading and downloading file on distributed

network. The next objective is to keep the track of every user who has done log in, during tracking it will keep the record of date, time and IP address of the user who has performed the login operation so that we can find any vulnerability. The last objective is to securely sharing file on distributed network from user to main server and main server to another disturbed database servers.



V. METHODOLOGY USED

The research is focused on the implementation of an algorithm that provides a better security by using combination of NTRU algorithm and MD5 hash function. So the distributed databases are more protected from adversaries. The main design for such approach is as following:

1. The methodology of the work will require the implementation of MD5 hash function which is used for authentication purpose and NTRU algorithm which is used to provide security for uploading, downloading document and then this algorithm will perform their encryption and decryption of text document.
2. Use java platform to implement algorithm.
3. Calculated and analyzed these parameters which are described as: Encryption time, Decryption time and Authentication time.

The implementation of the proposed research work goes through various steps which are described as following and shown in Figure 5.1.

Step 1: Activation of Wamp Server and NetBeans IDE the very first step of the proposed work is to run the Wamp server which is used as backend to store the database and Netbeans IDE as a front end where algorithms are implemented in java language.

Step 2: Initiate the Servers In this phase, we have to initiate all the servers that are used to process the user requests.

Step 3: User Registration and User Login In this, if the user is registered then he/she can login in order to see user's request and user can login for sending the request otherwise he has to do registration first.

Step 4: MAC address comparison for the authentication of the valid user during login process the MAC address of the system is compared which is stored as encrypted way in the database. If it is matched then further operations are performed otherwise not. It shows the MAC address blocked message or invalid username-password message.

Figure 5.1 Flow Chart of Proposed Work

Step 5: Perform Different operation during this phase different operations are performed as view logon user, all user profile, intruder log and upload a file. The intruder log keep the record of intruder party details as record of MAC Address, User name, Password, IP Address, Date and Time.

Step 6: Upload File this phase includes the uploading of file by the user, which is to be encrypted and stored in the database server.

Server receives the file and generates a unique key.

Step 7: Encryption of File this phase includes the encryption of the file uploaded by the user with help of encryption /decryption algorithm i.e. NTRU algorithm. Then, the encrypted file is stored in the database as shown in Figure 5.2 and Figure 5.3.

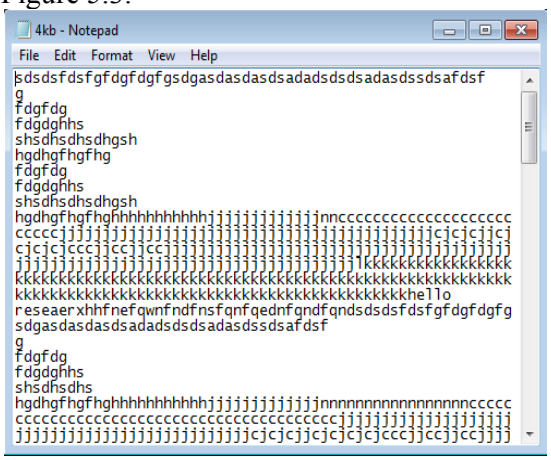


Figure 5.2 Before the Encryption

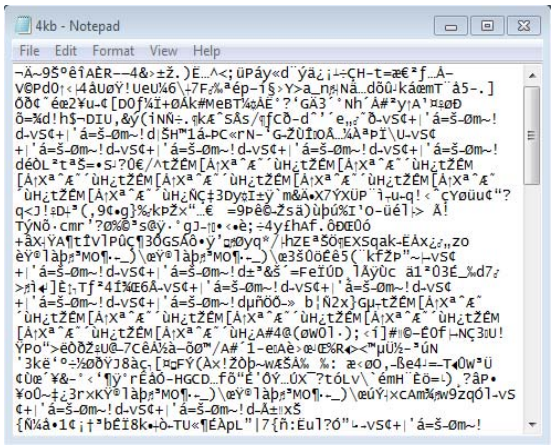


Figure 5.3 After the Encryption

Step 8: Decryption of File this phase include the decryption of the file using NTRU that is stored in the database and should be downloaded by the user.

Step 9: Detailed report generated this phase generates the report of the whole work .It represents the authentication time taken and the time taken for the encryption and decryption of file while sharing on distributed database system. Final results are validated. The given results are analyzed and provide the conclusion on the basis of results obtained.

VI. RESULTS AND DISCUSSION

The system designed consists of basic parameter which are described as following:

- **Encryption Time** It is defined as the system time which is used to encrypt plaintext into cipher text.
- **Decryption Time** It is the system time taken to decrypt cipher text to its corresponding message.
- **Authentication time** It is the time taken to check the consistency of data related to user login process.

The main idea behind using cryptographic algorithm is defense provided to the data being transferred across an un-trusted link. The adaption of any encryption algorithm depends upon the tradeoff between security and speed. If an algorithm offers great speed with greater protection against vulnerable attacks then it is widely accepted. Cryptosystems used the concept of block encryption suffered from the problem of producing the same output for same input and same encoding key which make them vulnerable to replay attacks. However, a stream cipher suffers from speed issue as they take a lot of time for execution. In order to do performance analysis different metrics will be considered to evaluate the performance of proposed algorithm. The main focus of our research study is on to increase the security of file sharing in distributed database network and reducing the time taken for authentication process. This is done by applying NTRU algorithm and MD5 hash function. The main parameters of our research are encryption, decryption and authentication time. In the existing Ramp Secret Sharing Scheme technique the time taken for encryption and decryption of data is more. In this we show the comparison of existing and proposed technique by different graphs.

Table No. 6.1 Calculated parameters of Proposed Work

S. no.	File Size	Encryption Time	Decryption Time	Authentication time
1	4Kb	19.563µsec	26.727µsec	0.559µsec
2	4Mb	21058.826µsec	26473.953µsec	0.559µsec
3	10 Mb	63097.566µsec	79322.654µsec	0.559µsec

The above shown Table No.6.1 describes the output of proposed work of each operation performed on different files of size 4Kb, 4Mb, and 10Mb.

Table No. 6.2 Calculated parameters of Existing Work

S.no.	File Size	Encryption Time	Decryption Time	Authentication time
1	4Kb	25.196µsec	32.727µsec	0.756µsec
2	4Mb	30000µsec	34000µsec	0.756µsec
3	10 Mb	68000µsec	85000µsec	0.756µsec

The above shown Table No.6.2 describes the output of existing system of each operation performed on different files of size 4Kb, 4Mb, and 10Mb.

Figure 6.1 to Figure 6.5 shows the graphical representation of proposed work of each output of different files of different sizes and its comparison with the existing system.

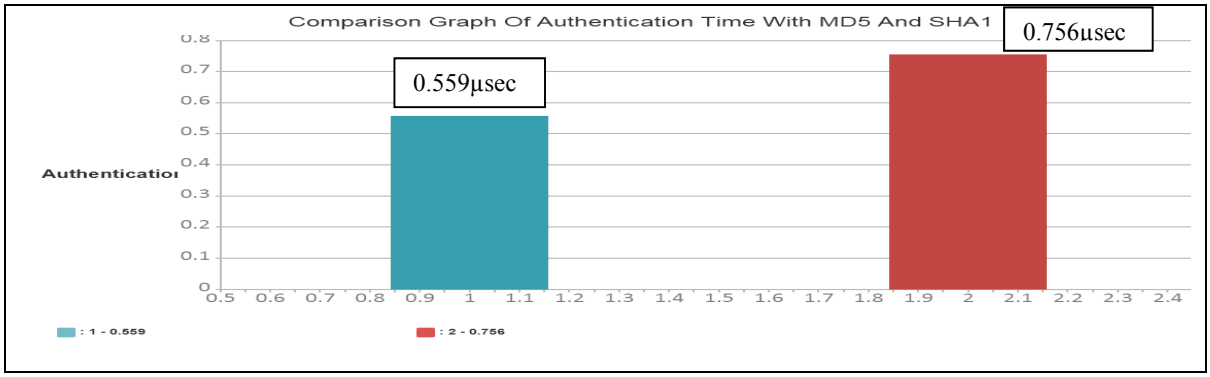


Figure 6.1 Performance evaluation of authentication time with MD5 and SHA1.

In Figure 6.1, the performance evaluation of authentication time using MD5 and SHA1 algorithms is shown. By using MD5 algorithm in our research work the authentication time value is 0.559µsec and with SHA1 algorithm in the previous research work its value is 0.756µsec.

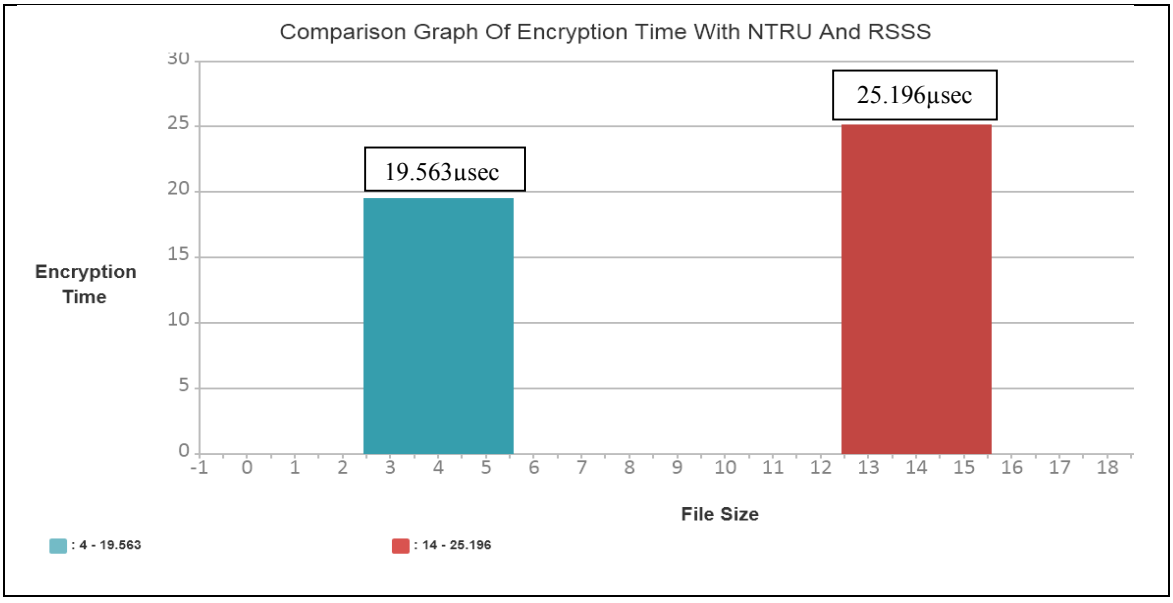


Figure 6.2 Performance evaluation of encryption time with NTRU and RSSS for 4Kb file size.

In Figure 6.2, the performance evaluation of encryption time using NTRU algorithm and RSSS scheme for 4Kb data file is shown. By using NTRU algorithm in our research work the encryption time value is 19.563µsec and with RSSS scheme in the previous research work its value is 25.196µsec for 4Kb file size.

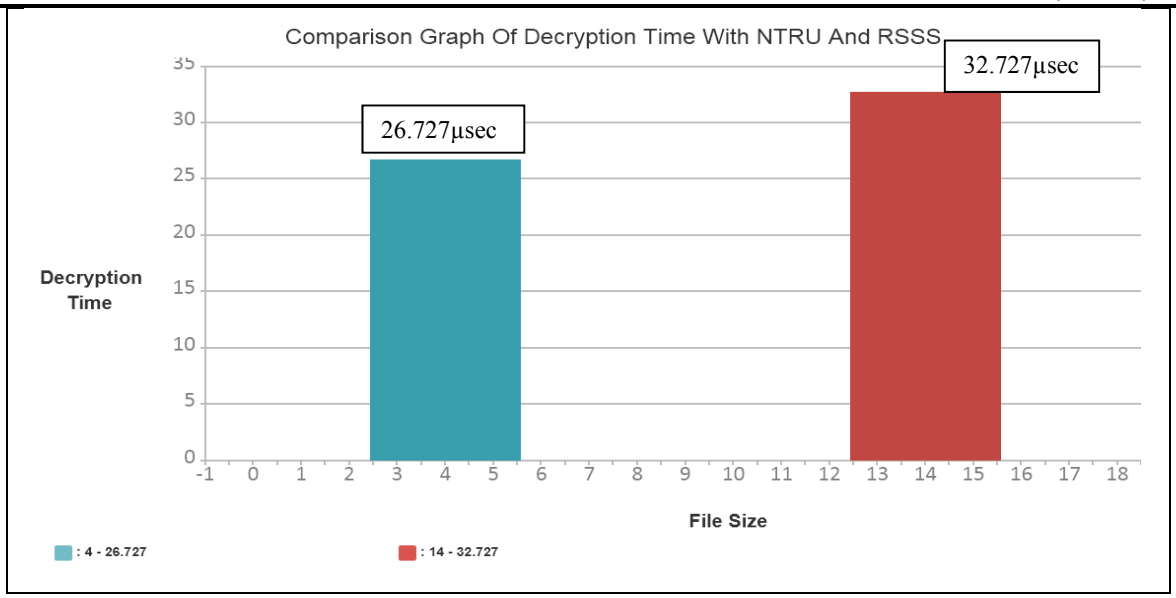


Figure 6.3 Performance evaluation of decryption time with NTRU and RSSS for 4Kb file size.

In Figure 6.3, the performance evaluation of decryption time using NTRU algorithm and RSSS scheme for 4Kb data file is shown. By using NTRU algorithm in our research work the encryption time value is 26.727µsec and with RSSS scheme in the previous research work its value is 32.727µsec for 4Kb file size.

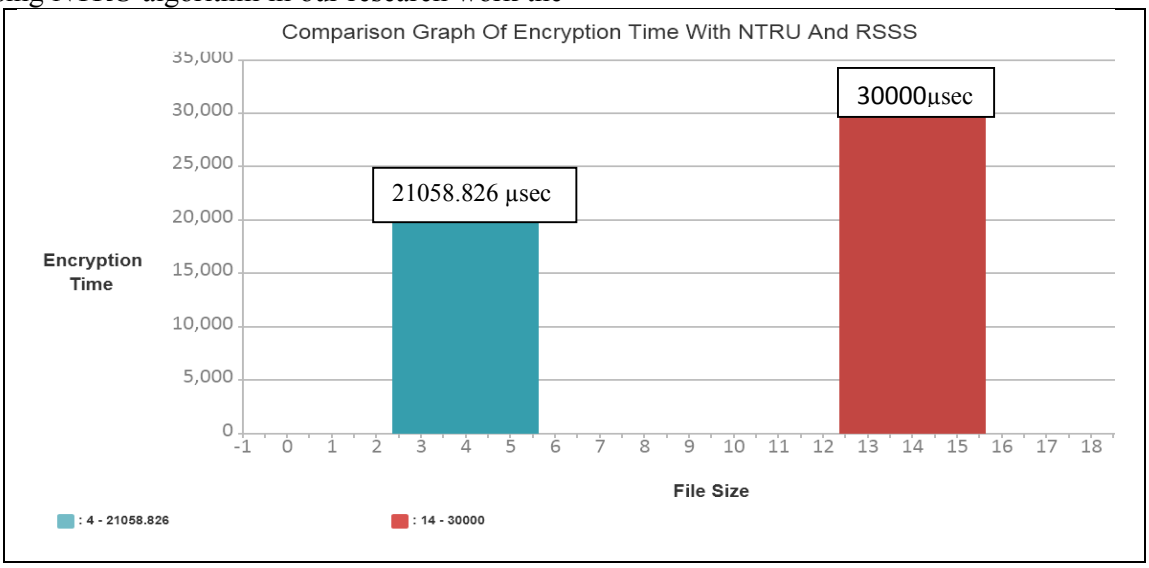
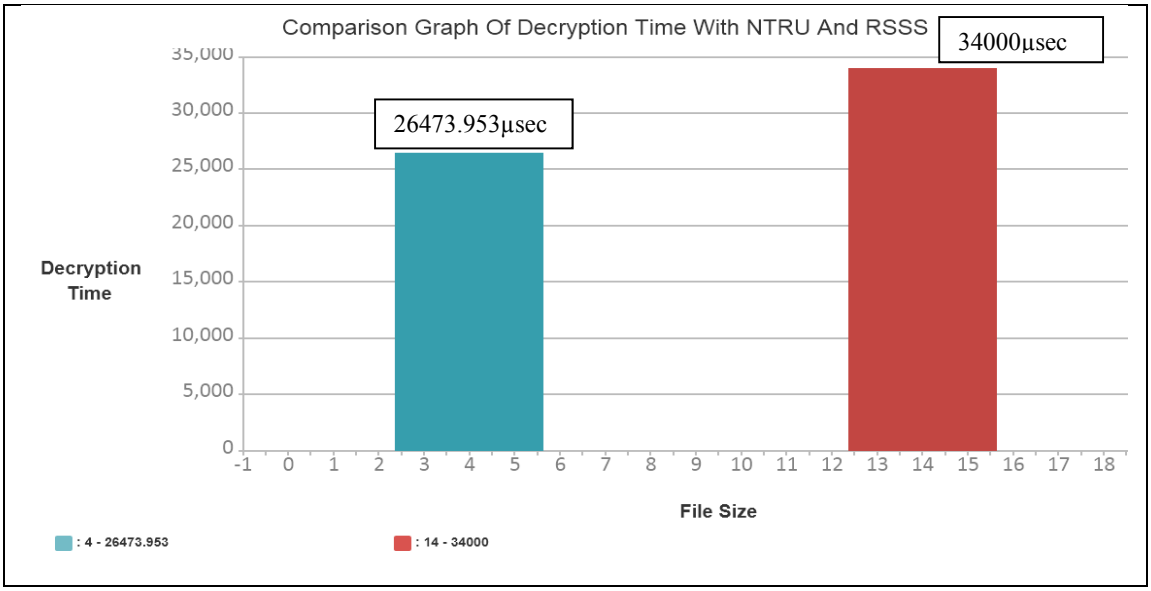


Figure 6.4 Performance evaluation of encryption time with NTRU and RSSS for 4Mb file size.

In Figure 6.4, the performance evaluation of encryption time using NTRU algorithm and RSSS scheme for 4Mb data file is shown. By using NTRU algorithm in our research work the encryption time value is 21058.826 µsec and with RSSS scheme in the previous research work its value is 30000µsec for 4Mb file size.

Figure 6.5 Performance evaluation of decryption time with NTRU and RSSS for 4Mb file size.



In Figure 6.5, the performance evaluation of decryption time using NTRU algorithm and RSSS scheme for 4Mb data file is shown. By using NTRU algorithm in our research work the encryption time value is 26473.953 µsec and with RSSS scheme in the previous research work its value is 34000 µsec for 4Mb file size.

Hence it is shown that proposed work represents the more secure distributed database communication than the existing systems, this is because NTRU algorithm's speed is quite fast and it is more secure for file sharing purpose. The encryption and decryption time of NTRU algorithm is less than that of RSSS.

7. CONCLUSION AND FUTURE SCOPE

Now-a-days security has become one of the most important aspects in every field. Each information should be secured as any changes in information leads to very serious problem. Data should be secured from malicious attacks and unauthorized access.

In this research we mainly deal with the distributed database communication, and solved the concurrency control and security related problems. Security plays important role in this work as to protect our sensitive information from the unauthorized user. This dissertation has implemented the NTRU algorithm in net beans. In this research we have studied the existing Ramp Secret Sharing Scheme used for encryption and decryption of data and to improve the reliability of distributed de-duplication system. But there are some limitations of existing RSSS technique to overcome the limitations of existing technique NTRU algorithm is used. With the help of this research we analyzed the results for the authentication purpose by using MD5 hash function and compare it with the parameters of existing system using SHA1. The proposed technique requires less time for encryption and decryption of data while sharing the files in distributed database system and also takes less time for authentication purpose.

In the area of security, research area of distributed database security is very wide. Security is required in military, banking and radio or satellite communication. The future scope of our work

1) Implementation for audio, video and .exe (executable) files.
2) Usage for window smart phone.

8. REFERENCES

[1] Aruna, N.S, Anandhi N K. and A.P., (2013),"Assured Data Transfer under Auditing in Distributed Circumstances", *International Journal of Scientific and Research Publications*, 3(4), pp:1-4.

[2] Al-Abiachi A. M., Ahmad F., and Ruhana K., (2011),"A Competitive Study of Cryptography Techniques over Block Cipher", *13th International Conference on Computer Modelling and Simulation (UkSim)*, pp:415-419.

[3] Aljafer H., Malik Z., Alodib M. and Rezgui A. (2014) "A brief overview and an experimental evaluation of data confidentiality measures on the cloud" *Journal of innovation in digital ecosystem Production and Hosting by Elsevier B.V.*, pp:1-11.

[4] Bhullar G. and Kaur N., (2014),"Concurrency and Security Control with NTRU", *International Journal of Innovative Research in Computer and Communication Engineering,* 2(3), pp:3352-3357.

[5] Ferretti L., Colajanni M., and Marchetti M., (2014),"Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases", *Institute of Electrical and Electronics Engineers (IEEE),* 25(2), pp:437-446.

[6] Ferretti L., Pierazzi F., Colajanni M., and Marchetti M., (2014), "Scalable Architecture for Multi-User Encrypted SQL Operations on Cloud Database Services", *Institute of Electrical and Electronics Engineers (IEEE),* 2(4), pp:485-498.

[7]. Gill A., and Singh C.,(2014)," Security of N-Tier Architecture using NTRU" , *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(7), pp:1018-1022.

[8] Gupta V., Singh G. and Gupta R., (2012),"Advance cryptography algorithm for improving data security", *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(1), ISSN: 2277 128X.

[9] Gupta V.K., Sheetlani J., Gupta D. and Shukla B., (2012),"Data concurrency control and security issues of distributed database transaction*", NIMS University, Jaipur, Rajasthan, INDIA*, 1(2), pp:70-73.

[10] Hababeh I. O. (2010), "Intelligent Network Communications for Distributed Database Systems" , *Second International Conference on Advances in Databases, Knowledge, and Data Applications*, pp:69-74.

[11] Hsiao-Ying Lin, Shen S., Tzeng W. and Bao-Shuh., (2012),"Toward Data Confidentiality via Integrating Hybrid Encryption Schemes and Hadoop Distributed File System", *26th IEEE International Conference on Advanced Information Networking and Applications*, pp:740-747.

[12] Hu F., Wilhelm K., Schab M., and Xiao Y., "NTRU-based sensor network security: a low-power hardware implementation perspective" *Security and Communication Networks Copyright #2008 John Wiley & Sons, Ltd.*

[13] Kumar N S., Lakshmi G.V R. and Ba B., (2014), "Enhanced Attribute Based Encryption for Cloud Computing", *International Conference on Information and Communication Technologies (ICICT)*, pp:689-696.

[14] Kashif Qureshi M., (2013),"Security Aspects of Distributed Database", *IJAIR ISSN: 2278-7844*, pp:197-212.

[15] Kaur V., Bhardwaj V., (2014),"Concurrency And Security Control In Distributed Database", Universe of Emerging Technologies And Science ISSN: 2349-655x, 1(4), pp:1-7.

[16] Li J., Chen X., Huang X., Tang S. and Xiang Y., (2015),"Secure Distributed Deduplication Systems with Improved Reliability", *IEEE Transactions on Computers*, pp:1-12.

[17] Masram R., Shahare V., Abraham J and Moona R., (2014), "Analysis and comparison of symmetric key Cryptographic algorithms based on various File features", *International Journal of Network Security & Its Applications (IJNSA)*, 6(4), pp 43-52.

[18] Mekala S., Prabhu M.E, (2014),"Survey on Encrypted Database in Cloud", *International Journal of Advance Research in Computer and Communication Engineering*, 3(10), pp:8290-8293.

[19] Mittal M., Sangani R. and Srivastava K., (2015),"Testing Data Integrity in Distributed Systems", *International Conference on Advanced Computing Technologies and Applications (ICACTA)*, pp:446-452.

[20] Mote Y., Nehete P. and Gaikwad S., (2012),"Superior security data encryption algorithm", *Internationa lJournal of Engineering Science*, vol.6, pp:171-181.

[21] Ranjan R., Baghel A.S. and Kumar S.,(2012),"Improvement of NTRU Cryptosystem" *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(9), pp-79-84.

[22] Romero-Tris C., Castellà-Roca J. and Viejo A., (2014), "Distributed system for private web search with untrusted Partners", *Computer Networks 67*, pp:26–42.

[23] Singh S. and Majithia S., (2013),"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*, 3 (11), pp-100-104.

[24] Sheetlani J., and Gupta V.K, (2012),"Concurrency Issues of Distributed Advance Transaction Process*", Res. J. Recent Sci.,* 1(2), pp:426-429.

[25] Shu J., Shen Z. and Xue W., (2014), "Shield: A stackable secure storage system for

file sharing in public storage*", J. Parallel Distrib. Comput. 74*, pp:2872–2883.
[26] Wang D., Wang N., Wang P. and Qing S., (2015)," Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity", *Information Sciences*, pp:1-17.
[27] Wang G., Liu Q., Wub J. and Guo M., (2011),"Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers", *Computers & security 30*, pp:320-331.
[28] Wang T., Yao S., Xu Z., XiongL. and Gu X., (2015), "An effective strategy for improving small file problem in distributed file system", *2nd International Conference on Information Science and Control Engineering*, pp:123-126.
[29] Wazed Nafi K., Kar T.S. and Hoque S.A., (2012), "Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture", *International Journal of Advanced Computer Science and Applications*,3(10), pp:181-186.
[30] Wei L., Zhu H. , Cao Z. and Dong X., (2014),"Security and privacy for storage and computation in cloud Computing", *Information Sciences 258*, pp: 371–386.
[31] Yu H., Zhang F. and Wua Y., (2014),"Granary: A sharing oriented distributed storage system", *Future Generation Computer Systems 38*, pp:47–60.
[32] Zhou L., Varadharajan V. and Hitchens M., (2013),"Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage", *IEEE Transactions on information forensics and security*, 8(12), pp:1947-1960.