European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 11, 2020

Enhanced Ntru Public Key Crypto System Using Ear Feature Extraction

[1]A.Poornima, **[2]Dr.D.Maheswari**
[1]Research Scholar, RathinavelSubramaniam College of Arts and Science, Sulur, Coimbatore.
[2]Associate Professor, Head & Research Co-Ordinator, School Of Computer Studies, Rathinavelsubramaniam College Of Arts And Science, Sulur, Coimbatore.

Abstract –Distributed computing environments have become a cost-effective and popular choice to achieve high performance and to solve large scale computational problems. Computers are interconnected through network to serve huge number of applications and achieve high performance. With growing rate of internet occupied a big percentage of network traffic. Secured load balancing leads to secured communication between client, load balancer and server in the network and also optimizes the server's performance. This research aims at improvising two vital factors namely security and load balancing in heterogeneous clustered web servers. The environment in which heterogeneous of different types of request (video, voice, email) are handled. With the implication of digital certificates intrusion attacks are possible leads to packet drop and causes security breach. Dynamic keys are generated to provide more secured communication. This leads to more computational cost. To overcome this situation, each request it is encrypted using NTRU encrypt public key crypto system whose public and private keys are obtained by the corresponding user's Ear Feature extraction and representing them in the format of RNA sequence. This strongly highlights the strength of security in clustered web servers.
Keywords:NTRU Crypto system, Server security, Server cluster.

1. INTRODUCTION

Each request is secured by providing NTRU file cryptosystem with Biometric key generation scheme. The next process is assigning the priority to each request by the intuitionistic fuzzy Inference system to overcome the uncertainty in load balancing. Finally, the local schedulers, schedules the request to the optimal web server in a specific cluster by using nature inspired behavioral approach known as fish swarm intelligence. The detailed description of this research methodology is presented in the following sub sections.

2. NEED FOR SECURE LOAD BALANCING IN DISTRIBUTED NETWORKS

With the continuous increase in the amount of internet service data, "distributed computing" technology is actively being applied to the procedures for processing information from a large amount of raw data, management of structured information storage, and analysis for extracting useful information.However, since the traditional network infrastructure is implemented mainly for communication between people, it is difficult to effectively accommodate the variety of types of data traffic that various objects emit in real time. The human communications can be predictable with a set of traffic patterns in a conventional mode of communication. But with the advancement of IoT there are wider varieties of traffic patterns in which handling such traffic in such infrastructure is very tough.

As such, the management of distributed data becomes a major issue as various data services become available in the fog computing environment. Security vulnerabilities and privacy violations by malicious attackers or internal users can arise from various types of data transactions (such as sharing and utilization). In the future, as the amount of information handled by e-governments and private enterprises gradually increases in scale, sensing information must be digitized, and information sharing will be essential to enable intelligent services. However, there may be various vulnerabilities and threats as the sensing information can include personal information and there can be a number of stake-holders in information access rights.

The objective of utilizing data service and sharing it is generalized, regardless of the users' needs in IoT. As, sensing information is digitized and stored by a centrally managed controller in the data center, if it is improperly used by the user, it can lead to a violation of the individual's privacy. Therefore, in order for intelligent service to be activated, it is necessary to protect the confidentiality of information shared and to manage the access rights.

The scheme described in this chapter, uses NTRU file cryptosystem which encrypts and decrypts the data using lattice method. The secret key is generated by using users' ear feature extraction which will be more secure during data encryption. The intuitionistic inference system is used to determine the priority order of each job request. The fish swarm intelligence highly helps in allocation of job request by the load scheduler among web server clusters.

3. LITERATURE SURVEY

Natarajan M. et. al. (2015) discussed the Multi-modal crypto-biometric system based on session key navigation for secure transactions. They have discussed the importance of cryptography in maintaining secrecy. It is related to data security in networks. To restrict unauthorized access of data from hackers or intruders they developed one system that deals with multi-modal biometric features with finger knuckle print and fingerprint recognition. In this methodology, a random key is precipitated from users' distinct samples. To generate random keys Random triangle hashing methods are used. The system detects if there is any change in data, identifies the source, and prevents an entry from opposing preceding actions.

Ratha .N.K et. al. (2001) illustrated reinforcing security and secrecy in biometrics-based authentication systems. Traditional security mechanisms are limited to some extent and are unable to handle some security issues. Biometrics replaced that gap and provides enhanced security in any area that involves any sensitive information. Privacy is enhanced with the introduction of biometrics. The pattern recognition model is in use for confirmation purposes. Various security signatures such as fingerprints, faces, and iris are used as identity recognition in security-related areas. A threat model is developed for biometric recognition and a methodology is proposed for enhancing secured features for fingerprint and iris biometrics.

Rishika Jain (2014) proposed Ear Biometric Cryptosystem for securing information. Bio cryptography is a continuous technology in the art of science for providing security and secrecy. Biometric features encrypt and decrypt data. In this approach ear biometric template is used for cryptography and the key gained is intended for authentication motives. In this approach, there are two models key generation module and encryption-decryption module. In the first module, the key is generated by capturing an image from the digital camera. Ear image template is generated by pre-processing the image's region of interest. With the normalization process, the image is transfigured to a rectangular box textured with a fixed size. 128 bit is extracted from the ear template. For confidential purposes, the AES algorithm is used. Future work can be enhanced with high-quality properties and with other different crypto algorithms.

4. NEED FOR BIO METRIC EAR FEATURE EXTRACTION

Biometric methods are more effective way of identifying an individual. It is based on physiological behavioral feature. So, it is used for authentication and identification methods. It provides distinctive information and will be unique for each individual. This type of authentication is needed in sharing sensitive information like e-banking transactions. With the use of biometric technology high individual identification accuracy is achieved. There are very less chances in getting damaged or cannot be changed suddenly. In the proposed methodology ear feature is chosen for key extraction.

The usage of biometrics has many advantages other than security which include:

- Difficult to forge or crack unlike passwords
- Convenient and easy o use
- Non conveyable
- A small change in users life style
- Minimal storage templates

5. NTRU CRYPTO SYSTEM

5.1 *Key Generation*

- Arbitrarily select a polynomial e $\in LT_e$ such that e is invertible in modulo r and modulo s.
- Calculate $e_r \equiv e^{-1}$ modulo r & $e_s \equiv e^{-1}$ modulo s
- Arbitrarily select a polynomial h $\in LT_h$.
- Calculate $k \equiv h * e_s \pmod{s}$.
- Distribute the public key (M, k) and the set of parameters r, s, LT_e ,LT_h, $LT_t$and LT_v.
- Preserve the private key (e, e_r).

5.2 Encryption

- Signify the message as a polynomial v $\in LT_v$.
- Arbitrarily select a polynomial t $\in LT_t$.
- Encrypt v with the public key (M, k) using the rule $\hat{E} \equiv r * t * k + v \pmod{s}$.

5.3 Decryption

- The receiver calculates $b \equiv e * g \pmod{s}$.
- By means of a centering process, change b to a polynomial with coefficients in the interval $[-\frac{s}{2}, \frac{s}{2}]$.
- Calculate $v \equiv e_r * b \pmod{r}$.

The decryption procedure is exact if the polynomial $r * t * h + e * v \pmod{s}$ is really equivalent to $r * t * h + e * v \in Z[\chi]/(\chi^M - 1)$, it resources without using modulo s. It obtains

$b \equiv e * h$ modulo s
$\equiv e * (r * t * k + v) \pmod{s}$
$\equiv e * t * (r * h * e_h) + e * v \pmod{s}$
$\equiv r * t * h * e * e_h + e * v \pmod{s}$
$\equiv r * t * h + e * v \pmod{s}$

Hereafter,

if $(b = r * t * h + e * v \in Z[\chi]/(\chi^M - 1))$, then
$b * e_r \equiv (r * t * h + e * v) * e_r * v$ modulo r

It has been observed that if the parameters are selected correctly, the process of decryption will never fail. An adequate constraint for this is to select s much larger than r. If parameter values M = 503, r = 3 and s = 256 are assigned then it will be in highest security.

6. NTRU ALGORITHM

Using K array, the key pair for NTRU Encryption and Decryption are done as shown:
i) Generate two empty arrays KP and KQ of size 512.
ii) Add values of K from index 0 TO 511 in KP and 512 to 1023 into KQ.

iii) Translate these values of array to decimal values KPD and KQD by bearing in mind the arrays values as bits and its indexes as bits position.

iv) Compute r and s as:

r= next_prime(KPD).

s= next_prime(KQD).

Compute gcd(r,s)==1 ;

v) Generate a random polynomial using Shamir secret polynomial generation f $\in$ R, with coefficient reduced modulo r, using the extracted features of K[1..n]

vi) Choose a random polynomial, g $\in$ S, with coefficients reduced modulo r, and

vii) Compute the inverse polynomial Fs of the secret key f modulo s.

viii) Once the above has been completed, the public key, h, is found as

h = Fs * g (mod s)

ix) Encryption

e = g * h + m (mod s)

Calculate Temp= $FK[i+512]*2^{512} + FK[i+511]* 2^{511} + \ldots.. + FK[i+1]* 2^{1} + FK[i]* 2^{0}$

a. Calculate e=next_prime(Temp).
b. If (r< s)) &&gcd(r,s)=1, break;

x) Decryption

a. Calculate a = f *e (mod s)
b. shift coefficients of a to the range (-s/2, s/2)
c. d = Fr * a (mod r).
d. The above generated keys f mod r and f mod s can now be used for NTRU encryption and decryption respectively.

Thus the process of NRTU based secure encrytpion is done with the fusion of featuer extraciton, RNA strucutre representation and shamir secret key sharing has been done.

Message will be in the below format with coefficients -1,0 and 1. Encryption is in hexadecimal format.

Message = 1,0,1,0,1,1,1

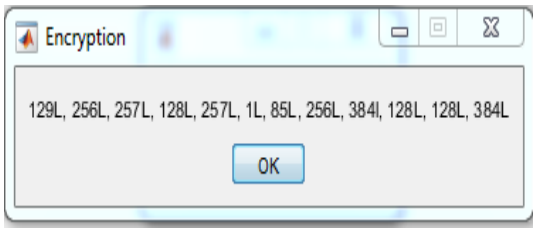

Figure 1: Encryption Data

Encrypted format of this message is 129L, 256L, 257L, 128L, 257L, 1L, 85L, 256L, 384l, 128L, 128L, 384L

Decrypted Message is 1L, 0L, 1L, 0L, 1L, 1L, 1L

A Ntru crypto screen for encrypting username and password and its decryption is depicted in Figure – 2.

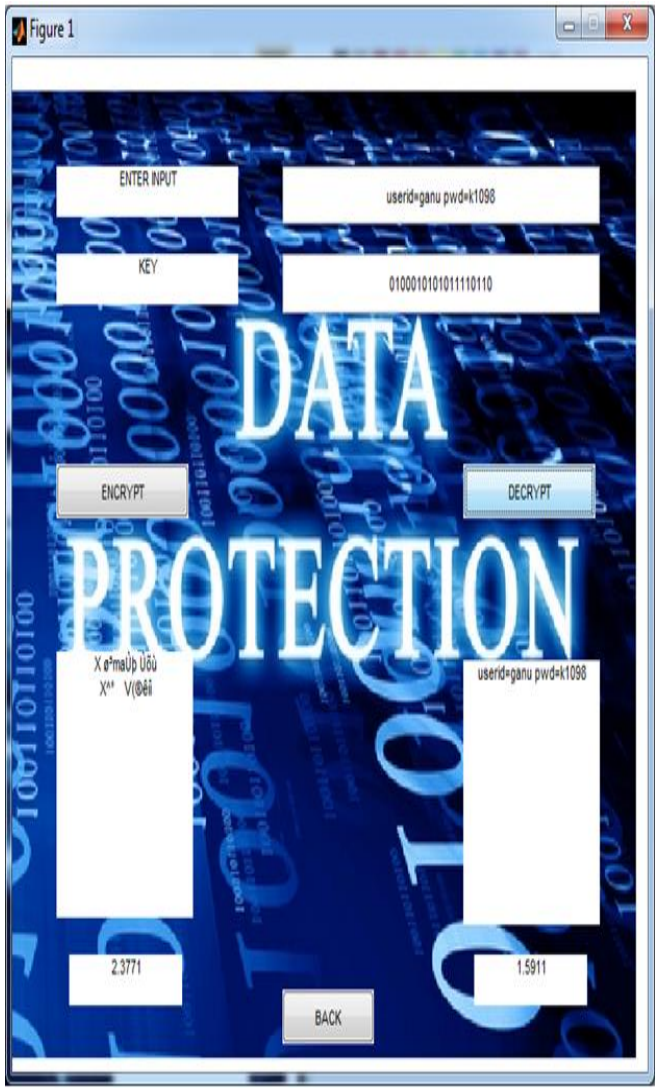

Figure 2: Ntru key system for sensitive data

7. RESULTS AND DISCUSSION

This research work transforms the ear features into binary format in the representation of strings of RNA. It is performed by using RNA coding approach. The coding of RNA string is denoted in Table-1.

The concept of the RNA conversion is if the ear binary string is '00' then it is converted to AA or if it is '11' then it is transformed to 'GG', for the binary string '01' then it is converted to 'U' and the bianry string '10' is converted to 'C' . This process continues to convert all the binary information of ear feature extracted into a RNA sequence. In case if the length of the ear binary data is not even, the last two rows help us to convert correctly.

Binary Data	RNA Data
00	AA
01	U
10	C
11	GG
0	A
1	G

Table-1: Binary data – RNA Coding Technique

The binay format of the image is shown in the below Figure – 3.

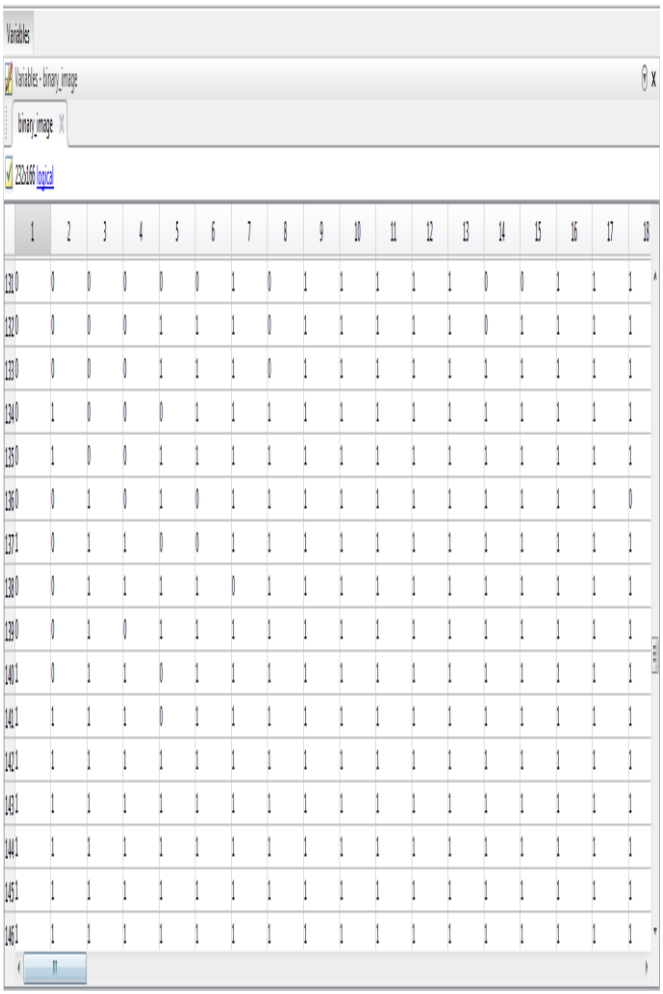

Figure – 3: Binary values of ear image

The sample binary string representaiton is supposed to be in this format :
00101001001001001001001001001001001001011010010100100100101001001010111011010000010010101001101010101001001001001010011111100101110101100100100100101001001010001001000001011110100100100110110.
The value of ear binary string, which is based on the proposed RNA coding technology, is as follows:
AACCUAACUAACTAACUAACUAACGGUUACCUAACUUACCGGCGGUAAAAUAACCAAGGUUUUCUAACUAACCUUGGGGCUUGGUCUAACUAACCUAACCAAUAAAAUUGGGGUAACUAUCGGA
This work chooses a RNA secret key with a key length of 512 bit randomly from the resultant RNA code based ear feature extraction.

8. NTRU ALGORITHM

Using K array, the key pair for NTRU Encryption and Decryption are done as shown:

i) Generate two empty arrays KP and KQ of size 512.

ii) Add values of K from index 0 TO 511 in KP and 512 to 1023 into KQ.

iii) Translate these values of array to decimal values KPD and KQD by bearing in mind the arrays values as bits and its indexes as bits position.

iv) Compute r and s as:

r= next_prime(KPD).

s= next_prime(KQD).

Compute gcd(r,s)==1 ;

v) Generate a random polynomial using Shamir secret polynomial generation f $\in$ R, with coefficient reduced modulo r, using the extracted features of K[1..n]

vi) Choose a random polynomial, g $\in$ S, with coefficients reduced modulo r, and

vii) Compute the inverse polynomial Fs of the secret key f modulo s.

viii) Once the above has been completed, the public key, h, is found as

h = Fs * g (mod s)

ix) Encryption

e = g * h + m (mod s)

Calculate Temp= $FK[i+512]*2^{512} + FK[i+511]* 2^{511} + \ldots.. + FK[i+1]* 2^{1} + FK[i]* 2^{0}$

c. Calculate e=next_prime(Temp).

d. If (r< s)) &&gcd(r,s)=1, break;

x) Decryption

e. Calculate a = f *e (mod s)

f. shift coefficients of a to the range (-s/2, s/2)

g. d = Fr * a (mod r).

h. The above generated keys f mod r and f mod s can now be used for NTRU encryption and decryption respectively.

Thus the process of NRTU based secure encrytpion is done with the fusion of featuer extraciton, RNA strucutre representation and shamir secret key sharing has been done.

Message will be in the below format with coefficients -1,0 and 1. Encryption is in hexadecimal format.

Message = 1,0,1,0,1,1,1

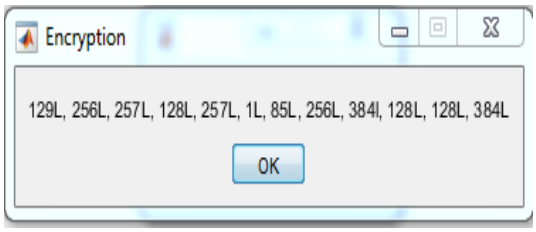

Figure 4: Encryption Data

Encrypted format of this message is 129L, 256L, 257L, 128L, 257L, 1L, 85L, 256L, 384l, 128L, 128L, 384L

Decrypted Message is 1L, 0L, 1L, 0L, 1L, 1L, 1L

A Ntru crypto screen for encrypting username and password and its decryption is depicted in Figure – 5.

Figure – 5 Ntru key system for sensitive data

9. CONCLUSION

This paper discusses about the main modules inovled in the process of security based load balancing. The main process of security services is explained with various techniques combined together to develop a strong security model, during the transmission of data and load balancing in an effective way. The Ear extraction is used to generate the private key or secret key with the represention of RNA coding to make the brute force attacker tough challenge. The NTRU is a primay crytpographic scheme combined with shamir secret sharing policy for providing more conifidentialy, availablity and accountability in distributed environment. After security process then proposed work moves to the next process load balancing of

requests. In the forth coming chapter Intutionistic fuzzy inference system is used to prioritize the requets. Later artifiical fish swarm optimziaiton is mainly used for search of optimzied resoruce allocation.

REFERENCES

[1]AkshayDaryapurkar, Mrs. V.M. Deshmukh, 2013, "Efficient Load Balancing Algorithm in Cloud Environment", International Journal Of Computer Science And Applications Vol. 6, No.2, pp.308-312.

[2] Alla H.B., Alla, S.B., Ezzati, A. and Mouhsen, A., 2016, "A novel architecture with dynamic queues based on fuzzy logic and particle swarm optimization algorithm for task scheduling in cloud computing". In International Symposium on Ubiquitous Networking Springer, Singapore. pp. 205-217.

[3]Alhassan Mohammed &Adjei-Quaye, Alexander, 2017, "Information Security in an Organization", International Journal of Computer (IJC), pp 100-116.

[4]Alkhudhayr .F, S. Alfarraj, B. Aljameeli and S. Elkhdiri, 2019, "Information Security:A Review of Information Security Issues and Techniques," International Conference on Computer Applications & Information Security (ICCAIS), pp. 1-6.

[5]Amit Gajbhiye, Dr. Shailendra Singh, 2017, "Global Server Load Balancing with Networked Load Balancers for Geographically Distributed Cloud Data-Centres", International Journal of Computer Science and Network, pp. 682-688.

[6]Androutsellis-Theotokis S. and Spinellis, D., 2004. A survey of peer-to-peer content distribution technologies. ACM computing surveys (CSUR), 36(4), pp.335-371.

[7]Anitha T.N, Dr.R.Balakrishna, 2011, "An Efficient and Scalable Content Based Dynamic Load Balancing Using Multiparameters on Load Aware Distributed Multi-Cluster Servers", International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 8, pp.6401-6411.

[8]Antonio Mana, HristoKoshutanski, Ernesto J. Pérez, 2012, "A trust negotiation based security framework for service provisioning in load-balancing clusters", Computers &Security,Volume 31, Issue 1, pp. 4-25.

[9] Anurag M., Dharmendr S., 2011, "An Improved Backfilling Algorithm: SJF-BF", International Journal on Recent Trends in Engineering & Technology;3 /10/2011, Vol. 5 Issue 2, pp.78.

[10] ArtiMishra , 2015, "Network Load Balancing and Its Performance Measures",International Journal of Computer Science Trends and Technology (IJCST), Volume 3 Issue 1, pp.77-81.

[11]Blej M. and Azizi, M., 2016. "Comparison of Mamdani-type and Sugeno-type fuzzy inference systems for fuzzy real time scheduling". International Journal of Applied Engineering Research, 11(22), pp.11071-11075.

[12]Bora A. and Bezboruah, T., 2020. "Some Aspects of Reliability Estimation of Loosely Coupled Web Services in Clustered Load Balancing Web Server". In Critical Approaches to Information Retrieval Research, IGI Global, pp. 198-209.

[13]Butt M. A., &Akram, M. (2016). "A new intuitionistic fuzzy rule-based decision-making system for an operating system process scheduler", Springer Plus, pp. 1-17.

[14]ChangjiangHou, Fei Liu, HongtaoBai&LanfangRen (2013), "Publickey encryption with keyword search from lattice", Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, pp. 336-339.

[15]Challa N. and Pradhan, J., (2007). "Performance analysis of public key cryptographic systems rsa and ntru". International Journal of Computer Science and Network Security, 7(8), pp.87-96.

[16]ChittiBabu .P, K.Karpagavalli, V.Nirmala, DjSamatha Naidu, 2014, "Prevention Techniques for syllabic time–relay attacks during implementation using public key cryptographic algorithms", IJESR Vol. 05, pp. 1490-1496.

[17]Dash Swikruti&Panigrahi, Amrutanshu&Sabat, Nihar, 2019, "Performance Analysis of Load Balancing Algorithm in Cloud Computing", International Journal of Innovative Research & Growth, pp.95-104.

[18]Dave A, B. Patel and G. Bhatt, 2016, "Load balancing in cloud computing using optimization techniques: A study," International Conference on Communication and Electronics Systems (ICCES), Coimbatore, pp. 1-6.

[19]Dave A, B. Patel, G. Bhatt and Y. Vora,2017, "Load balancing in cloud computing using particle swarm optimization on Xen Server," International Conference on Engineering (NUiCONE), Ahmedabad, 2017, pp. 1-6.

Natarajan M., Mekala, T., &Vikram, R., 2015, "Multi-Modal Crypto-Biometric System Based On Session Key Navigation for Secure Transaction", Corpus ID: 212572680.

[20]Ratha .N.K, J. H. Connell, and R. M. Bolle, 2001, "Enhancing security and privacy in biometrics based authentication systems", IBM Systems Journal, vol. 40, pp. 614-634.

[21]Rishika Jain, 2014, Ear Biometric Cryptosystem, International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, pp. 587-590.

[22]Natarajan M., Mekala, T., &Vikram, R., 2015, "Multi-Modal Crypto-Biometric System Based On Session Key Navigation for Secure Transaction", Corpus ID: 212572680.