International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Implementation of Novel Symmetric Encryption Algorithm to secure Information - Two Layer DNA-RSA Hybrid Cryptosystem

[1]Omkar Pujeri, [2]Uma Pujeri, [3]Trupti Baraskar, [4]Pallavi Parlewar

Submitted: 23/05/2023 **Revised**: 09/07/2023 **Accepted**: 28/07/2023

Abstract: Cryptography was used since ancient days where plain text or confidential message was converted to a message which is in unreadable format or cipher text using secret key and an encryption algorithm and cipher text is converted to plaintext using decryption algorithm and a secret key. Cryptography ensured secured communication of messages and also provided integrity, confidentiality and availability of the information RSA is an asymmetric algorithm most widely used since 1977. Researchers and cryptanalysis have looked for ways to attack RSA. Some common attacks on RSA are discussed in this research work.

Objective – The Main objective of this research was to study RSA algorithm, its weakness and attacks on RSA and to work on to make existing RSA algorithm stronger. Attack like the chosen cipher text attack, partial key exposure attack, common modulus attack and low decryption exposure attack are frequently targeted attacks for RSA algorithm.

Findings – RSA algorithm can be partially or fully cracked if not implemented correctly. Proposed Work – In this research a new algorithm has been proposed using two layer DNA cryptography [1] and proposed algorithm is added on the top of RSA algorithm to make the RSA algorithm stronger. Message is first encrypted with proposed two-layer DNA
algorithm and output of this is input to RSA algorithm.

Implications – Algorithm can be applied to encrypt small ATM pin, small secret messages etc.

Result, Outcome and Originality - Security analysis of proposed system has proven good. Algorithm uses two-layer DNA cryptography with different function and encoding tables. Indian copyright is granted for the algorithm under the registration number L-120035/2022

Keywords **-** *RSA, encryption algorithm, DNA cryptography, DNA sequence.*

1. Introduction

Cryptography plays a very vital role in securing user's confidential private data in the presence of adversaries. The goal of cryptography is to pro- vide privacy/confidentiality, integrity, authentication, non-repudiation for user data. Cryptosystem can be classified into two types based on number of keys involved in encrypting the plain text or secret information.

Symmetric Key Cryptography – Symmetric Key Cryptographic are the algorithm which uses common shared secret shared keys at both sender and receiver side to encrypt plain text to cipher text using an encryption/decryption algorithm. At the sender's end, the plaintext undergoes a transformation into cipher text through the use of the common secret key and an encryption algorithm. The resultant cipher text, which is indecipherable, is then transmitted via a secure communication channel to the recipient. To recover the original plaintext, the recipient decrypts the cipher text utilizing the same secret key and decryption algorithm.

In Asymmetric Key Cryptography, a pair of keys, comprising the public key (for encryption) and the private key (for decryption), are employed for encryption and decryption operations. The sender selects the receiver's public key and encryption algorithm to transform plaintext to cipher text. The resulting unreadable cipher text is then transmitted to the receiver through a secure communication channel. To recover the original plaintext, the receiver decrypts the cipher text using the decryption algorithm and his or her private key.

While cryptography is a science to convert plain text to cipher text using key, cryptanalysis is related study of analyzing the cipher text and study of breaking the cipher text. Cryptanalyst and scientist have done several research on RSA attack. The research paper discusses main attacks against RSA cryptosystem like common modulus attack, blinding attack, chosen cipher text attack, partial key exposure attack, low decryption exponent at- tack

DNA-based cryptography has been recognized as an innovative modality for safeguarding data in the form of DNA sequence A,G,C,T. This methodology utilizes

1,2,3School of Computer Engineering and Technology, Dr. Vishwanath Karad MIT World Peace University,
Pune, 411038, Maharashtra, India
4Shri Ramdeobaba College of Engineering and Management, Nagpur
[1]omkar.pujeri@mitwpu.edu.in; [2]uma.pujeri@mitwpu.edu.in;
[3]trupti.baraskar@mitwpu.edu.in; [4]parlewarpk@rknec.edu.in

DNA strands to veil the information. DNA cryptography ensures confidentiality and integrity during the transmission of data over a network.

In this paper we have proposed new algorithm name Two Layer DNA-RSA Hybrid Cryptosystem to make encryption process stronger and practically very difficult for hacker to retriever original plain text. In our proposed algorithm two layer DNA cryptographic algorithm is implement and message is first encrypted using two- layer DNA algorithm. Output of this two-layer DNA algorithm is given as input to RSA algorithm and message is encrypted using RSA algorithm.

2. Theory And Formula

This section gives brief introduction about RSA algorithm, Common attacks on RSA algorithm and DNA cryptography.

2.1 RSA algorithm [9] [10] is widely used asymmetric encryption algorithm as it's used was found securing the data transmission over internet providing confidentiality, integrity and authentication to email and was one of the pillar to make e-commerce success over the inter- net. Algorithm for RSA encryption and decryption [11] [12] uses the receiver's public key to cipher the confidential communication, and the receiver's end user uses the receiver's private key to convert the cipher text back to plain text.

2.2.1 Common attacks on RSA

Attack on RSA algorithm can be classified into two categories a) Weak choice of exponent, pub- lic exponents, bad padding i.e. in setting the values of parameters that are vulnerable to security attack b) Implementation attacks on RSA .Few RSA attacks are discussed along with their im- plementation in this paper

2.2.2 Low Decryption exponent attack against RSA – In RSA algorithm to get plain text from cipher text we use following formula

$$P = C^{d} \bmod n$$

Where P is the plain text, C is the cipher text, d is exponent key and n is the product of p and q. Hence the computational complexity of the RSA decryption algorithm is directly proportional to the magnitude of the private exponent. Consequently, selecting a very small private exponent, such as d, may lead to the total breakdown of the RSA cryptosystem. This is particularly evident in practical applications that require improved computational efficiency, such as smart card technology, where encryption processes are performed on low-power devices using small values of d. It is important to note that choosing small values of d can have a severe impact on the security of the RSA cryptosystem.

2.2.3 Partial Key Exposure attack - A cryptosystem proposed by Boneh Durfee and Frankell states that, an attacker can easily reconstruct the entire private key d in a linear period of time (e log (e)), where e is the public key exponent, if the attacker knows the (k/4) least significant bit of the private key d. According to the algorithm, when e is small, the disclosure of only a quarter of d's bits can result in the recovery of the full private key.

2.2.4 Chosen Cipher Attack - In Chosen Cipher text attack the attacker chooses the cipher text and recovers the plaintext original message without knowledge of private key d.

2.2.5 Shor's Algorithm – Shor's algorithm is a quantum computing method for deter- mining an integer's prime factors. RSA algorithm is based on the assumption that factoring large integers are intractable the statement is true for all non-quantum computing algorithms. Shor's algorithm uses quantum computers to factor the numbers in polynomial time. Shor's algorithm can be used to hack RSA algorithms and other secure data form.

2.2.6 Hack RSA by choosing small prime numbers – RSA algorithm can be defeated if the prime number p and q are chosen are small but it is difficult to defeat RSA if value of p and q are large .Sample code to hack RSA cipher with small prime numbers is provided in appendix.

3. Prevention And Countermeasures

Following points should be followed to make RSA algorithm stronger.

Key Size – RSA key chosen should large enough to resist any security attack and break RSA cryptosystem

Strong Prime – Prime Numbers p and q should be large enough. The prime factors of

(p– 1) and (q – 1) should be large enough.

Public Exponent – Public exponent e should be large enough to make RSA cryptosystem

stronger

Private Exponent – To make RSA algorithm stronger the private exponent key should be at least 300 bits long.

4. DNA Cryptography

DNA cryptography [13] [14] [15] is a technique which

encrypts and decrypts the plaintext using DNA sequence Adenine(A), Cytosine(C), Guanine(G), Thymine(T) .In DNA cryptog- raphy [16] [17]message is hidden in DNA sequence. Each character in a plaintext message is converted to binary form. These binary bits are grouped into two bits and these bits are mapped to DNA base for example 00 bits are mapped to DNA base A, 01 bits are mapped to DNA base T, 10 bits are mapped to DNA base C and 11 bits are mapped to DNA base

G. Thus the cipher text is the sequence of A,T,G,C [18] [19] [20].

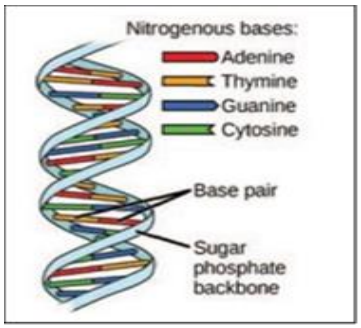

Fig 1: DNA Structure

5. Experimental Setup

In our proposed work we have combined two level of DNA cryptography algorithm with RSA algorithm which resulted in two level DNA RSA cryptographic system. In our proposed system the input message is first converted to series of "AGCT" text using two level of DNA crypto- graphic algorithm and output of this two level DNA cryptographic algorithm is input to the RSA algorithm, output of RSA algorithm is converted to asci values of string that is number making it a challenge for an intruder to break the encryption algorithm. In our proposed system values of P, Q of RSA algorithm are chosen big prime numbers, similarly e and d are of RSA algorithm chosen large numbers. Objective of this research to make RSA algorithm stronger. In this research the RSA algorithm is embedded in new two-layer DNA Computing algorithm implemented in our research center.

The Message is first encrypted using two-layer encryption algorithm and output of this encoding algorithm is input to RSA encryption algorithm. This algorithm can be used to encrypt very small secret message. The algorithm is efficient for small short message.

Modules In Encryption Algorithm

Encryption Algorithm - In encryption algo- rithm message is converted to binary. This binary string is encoded to DNA series message(AGCT) using secret encoding table. This is first layer of DNA cryptographic algorithm. The DNA se- ries message is converted to binary. One's com- plement is done of these binary string. Bits are shifted by left by three and again these bits are encoded to DNA series message using second se- cret encoding table. This is Second layer of DNA cryptographic algorithm. This DNA series message is encoded using second secret encoding table encryption algorithm

Step 1 – Input string from the user that has to be encrypted

Step 2 – Convert the inputted string to bi- nary

Step 3 - Group the binary bits into group of two bits

Step 4 - Encode the group of two bits us- ing encoding table1. [Note Encoding table have hidden; it is only shared with authorised user. En- coding table used in mentioned in Appendix]

Step 5 – Create a first layer of DNA series of encrypted message using DNA encoding table 1

Step 6 – Layer 2: Convert the DNA series of encrypted message to binary

Step 7 –Find One's complement of binary string

Step 8 – Left shift bits by 3

Step 9 – Group the bits into group of 2 bits

Step 10 – Encode the bits using encoding table 2 [Note Encoding table have hidden; it is only shared with authorised user. Encoding ta- ble2 used in mentioned in Appendix]

Step -11 Create DNA series of encrypted message from encoding table 2

Step 12 – Send the DNA series of encrypted message to RSA Encryption Algorithm

Step 13 – Encrypt the output received from DNA series algorithm using RSA encryption

Step 14 – Send the encrypted Message to the receiver

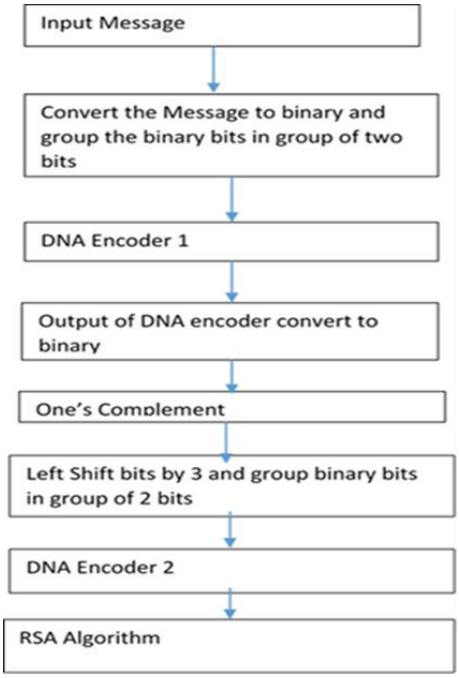

Fig 2: Modules In Encryption Algorithm

Module in Decryption Algorithm

Decryption Algorithm – Decryption algorithm is the opposite process of encryption algorithm. In decryption algorithm cipher text received from sender is decrypted using RSA algorithm. Out- put of RSA algorithm is given as an input to DNA layer 2 decoding algorithm. Message is decoded to DNA series using secret decoding table. Bits are shifted to right by 3. Find one's complement. Convert this binary to string. Decode this string using second secret decoding table. Convert the decoded binary string to string and original message is retrieved.

Step 1 – Decrypt the message received from sender using RSA decryption algorithm.

Step 2 – Output of RSA decryption algorithm will be input to DNA 2 layer decoding algorithm

Step 3 -Convert the DNA series message received from DNA 2 layer decoding al- gorithm to binary using DNA decoding table [Note Decoding table have hidden; it is only shared with authorised user. Decoding table used in mentioned in Appendix]

Step 4 – Right shift the binary bits obtained from step 1 by 3 bits

Step 5 - Find One's complement of binary string

Step 6 – Convert the binary bits obtained from step 5 to string

Step 7 – Decode the string using second de- coding table2. [Note Decoding table have hidden; it is only shared with authorised user. Decoding table2 used in mentioned in Appendix]

Step 8 – Convert this decoded DNA series of binary bits obtained from step 7 to string

Step 9 – Original message retrieved

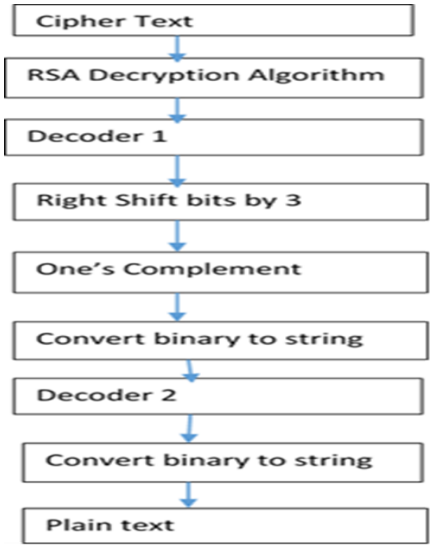

Fig 3: Modules In Decryption Algorith

6. Result Discussions

This session discusses the results of the working algorithm. Session 4.1 discusses how plain text is converted to DNA two encryption algorithm and then to final cipher text using RSA algorithm. Session 4.2 discuses encryption and decryption time required for the proposed algorithm.

4.1 Encryption of Letters – A table shows the encrypted text for single letter, two letters, three letter, four letter words and five letter words.

Encryption and Decryption Time – Time required for encrypting the message and de- scripting the message is measured in seconds. Table shows time required for one letter, two letters three letters, four letters and five letters word with respect to encryption and decryption

TABLES

Encryption of Message Using Proposed Algorithm.

Table 1. Plain Text to Cipher Text Using Proposed Algorithm Two Layer DNA-RSA Hybrid Cryptosystem

Sr. No	No of Words In Plain Text	Plain Text	Cipher Text 1 (DNA Cryptography Layer 1 output)	Cipher Text 2 (Cipher Text 1 is input to Proposed Algorithm, Output of Proposed Algorithm Layer 2 Output)
1	One	@	GCTTGGTTGGTTG- GTT	[114735, 8038, 25862, 25862, 114735, 114735, 25862, 25862, 114735, 114735, 25862, 25862, 114735, 114735, 25862, 25862]
2	Two	My	GCTTGATTTTGT- GCTTGCTTTTGT- GATTGCTT	[114735, 8038, 25862, 25862, 114735, 0, 25862, 25862, 25862, 25862, 114735, 5862, 114735, 8038, 25862, 25862, 114735, 8038, 25862, 25862,

				25862, 25862, 114735, 25862, 114735, 0, 25862, 25862, 114735, 8038, 25862, 25862]
3	Three	MAT	GCTTGATTTTGT-GCTTGCTTGATTG-GTTGCTTGCTTTTGT-GCTTGGTT	[114735, 8038, 25862, 25862, 114735, 0, 25862, 25862, 25862, 25862, 114735, 25862, 114735, 8038, 25862, 25862, 114735, 8038, 25862, 25862, 114735, 0, 25862, 25862, 114735, 114735, 25862, 25862, 114735, 8038, 25862, 25862, 114735, 8038, 25862, 25862, 25862, 25862, 114735, 25862, 114735, 8038, 25862, 25862, 114735, 114735, 25862, 25862]
4	Four	GOOD	GCTTGATTGCTTTTGT GCTTGATTTTGTTTGT GCTTGATTTTGTTTGT GCTTGATTGCTTG-GTT	[114735, 8038, 25862, 25862, 114735, 0, 25862, 25862, 114735, 8038, 25862, 25862, 25862, 25862, 114735, 25862, 114735, 8038, 25862, 25862, 114735, 0, 25862, 25862, 25862, 25862, 114735, 25862, 25862, 25862, 114735, 25862, 114735, 8038, 25862, 25862, 114735, 0, 25862, 25862, 25862, 25862, 114735, 25862, 25862, 25862, 25862, 114735, 114735, 25862, 25862]

Encryption and Decryption Time – Time required for encrypting the message and decrypting the message is measured in seconds. Table shows time required for one letter, two letters three letters, four letters and five letters word with respect to encryption and decryption time in seconds

Table 2: Encryption and Decryption Time of Proposed Algorithm

Number of Characters	Encoding Time in Seconds	Decoding time In Seconds
1	0.000616793	0.000616793
2	0.007749228	0.007732699
3	0.019477913	0.019340613
4	0.010381601	0.010366361
5	0.004856695	0.004030767
6	0.007863903	0.007875429
7	0.026236598	0.026806898
8	0.008113085	0.008015109
9	0.006899325	0.006883848
10	0.008568729	0.008937556

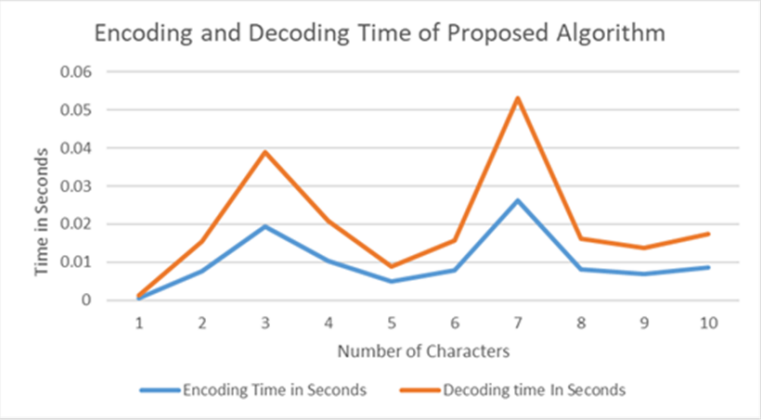

Fig 4: depicts the encoding and decoding time required for proposed algorithm.

7. Conclusion

In this research we studied RSA algorithm and various attacks on RSA algorithm. To make RSA algorithm stronger the proposed work used hybrid cryptosystem combining two layer DNA algorithms with RSA algorithm. The Plain text message is given as an input to two layer DAN cryptographic algorithm output of this algorithm is an input to RSA algorithm, thus DNA layers above RSA algorithm add more security making it difficult for intruder to decrypt or break

References

[1] P. Pavithran, S. Mathew, S. Namasudra, G. Srivastava, A novel cryptosystem based on DNA cryptog- raphy, hyperchaotic systems and a randomly gener- ated Moore machine for cyber physical systems, Computer Communications 188 (2022) 1–12.

[2] P. Uma, Member, K. Siddivinayak, P. Ramachandra, Smart Captcha to Provide High Security against Bots, Proceedings of the World Congress on Engineeing (2019).

[3] D. Pujeri, U. Pujeri, D. R, Symmetric Encryption Algorithm using ASCII, Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP 8 (2020) 2355–2359.

[4] U. Pujeri, P. S. Aithal, R. Pujeri, Survey of Lattice to Design Post Quantum Cryptographic Algorithm Using Lattice, International Journal of Engineering Trends and Technology 69 (1) (2021) 2231–5381.

[5] Increasing Randomization of Ciphertext in DNA Cryptography, In- ternational Journal of Advanced Computer Science and Applications(IJACSA) (10) (2021) 12–12.

[6] S. . Narendren, B. Yashas, C.-D. Yathish2, B. . Mohan, A Cryptosystem using Two Layers of Security - DNA and RSA Cryptography, International Journal of Pure and Applied Mathematics 119 (7) (2018) 217–224.

[7] N. P. Sable, M. D. Salunke, V. U. Rathod and P. Dhotre, "Network for Cross-Disease Attention to the Severity of Diabetic Macular Edema and Joint Retinopathy," 2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, 2022, pp. 1-7, doi: 10.1109/SMARTGENCON56628.2022.10083936.

[8] M. Karimi, Waleejhaider, Cryptography using DNA Nucleotides. Inter- national Journal of Computer Application 168 (2017) 16–18.

[9] Y. Zhang, DNA based random key generation and management for OTP encryption, BioSystems 159 (2017) 51–63.

[10] N. P. Sable, V. U. Rathod, P. N. Mahalle and D. R. Birari, "A Multiple Stage Deep Learning Model for NID in MANETs," 2022 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2022, pp. 1-6, doi: 10.1109/ESCI53509.2022.9758191.

[11] Common Attacks on RSA and its Vari- ants with Possible Countermeasures, International Journal of Emerging Research in Management &Technology 5 (5) (2016) 65–70.

[12] W. Diffie, M. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory 22 (6) (1976) 644–654.

[13] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosys- tems, Communications of the ACM 21 (2) (1978) 120–126. C. Cid (2003).

[14] V. U. Rathod and S. V. Gumaste, "Role of Routing Protocol in Mobile Ad-Hoc Network for Performance of Mobility Models," 2023 IEEE 8th International Conference for Convergence in Technology (I2CT), Lonavla, India, 2023, pp. 1-6, doi: 10.1109/I2CT57861.2023.10126390.

[15] N. Ubaidurrahman, R. Chithralekha-Balamurugan, A novel DNA computing based encryption and decryption algorithm, Procedia Computer Science 46 (2015) 463–475.

[16] P. Pavithran, S. Mathew, S. Namasudra (2022). [link].

[17] URL https://doi.org/10.1007/s10586-022-03653-9

[18] A. K. Kaundal, & A K Verma, Extending Feistel struc- ture to DNA Cryptography, Journal of Discrete Mathematical Sciences and Cryptography 18 (4) (2015) 349–362.

[19] S. . Karthiga, E. . Murugavalli, DNA CRYP-TOGRAPHY. International Research Journal of Engi- neering and Technology (IRJET) 5 (3) (2018) 3987–3991.

[20] N. P. . Sable, V. U. . Rathod, P. N. . Mahalle, and P. N. . Railkar, “An Efficient and Reliable Data Transmission Service using Network Coding Algorithms in Peer-to-Peer Network”, IJRITCC, vol. 10, no. 1s, pp. 144–154, Dec. 2022.

[21] E. M. S. Hossain, A DNA crypto- graphic technique based on dynamic DNA sequence table, Proceedings of the IEEE International Conference on Computer and Information Technology (ICCIT) (2016) 270– 275.

[22] N. P. . Sable, R. . Sonkamble, V. U. . Rathod, S. . Shirke, J. Y. Deshmukh, and G. T. . Chavan, “Web3 Chain Authentication and Authorization Security Standard (CAA)”, IJRITCC, vol. 11, no. 5, pp. 70–76, May 2023.

[23] N. P. Sable, V. U. Rathod, R. Sable and G. R. Shinde, "The Secure E-Wallet Powered by Blockchain and Distributed Ledger Technology," 2022 IEEE Pune Section International Conference (PuneCon), Pune, India, 2022, pp. 1-5, doi:

10.1109/PuneCon55413.2022.10014893.

[24] Y. Niu, Review on DNA cryptography, in: Proceedings of the International Conference on Bio-Inspired Computing: Theories and Applications, Springer, 2019, pp. 134–148.

[25] V. U. . Rathod and S. V. . Gumaste, “Role of Deep Learning in Mobile Ad-hoc Networks”, IJRITCC, vol. 10, no. 2s, pp. 237–246, Dec. 2022.

[26] Prof. Deepanita Mondal. (2018). Analysis and Evaluation of MAC Operators for Fast Fourier Transformation. International Journal of New Practices in Management and Engineering, 7(01), 01 - 07. https://doi.org/10.17762/ijnpme.v7i01.62

[27] García, A., Petrović, M., Ivanov, G., Smith, J., & Cohen, D. Enhancing Medical Diagnosis with Machine Learning and Image Processing. Kuwait Journal of Machine Learning, 1(4). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/143

[28] Gupta, S. K., Lanke, G. R., Pareek, M., Mittal, M., Dhabliya, D., Venkatesh, T., &

[29] Chakraborty, S. (2022). Anamoly detection in very large scale system using big data. Paper presented at the IEEE International Conference on Knowledge Engineering and Communication Systems, ICKES 2022, doi:10.1109/ICKECS56523.2022.10059870 Retrieved from www.scopus.com