European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 06, 2020

Securing The Predicting Data Using Rjb20 Algorithm

R. Jaichandran[1], S. Muthuselvan[3], P. Malli Karjun Reddy[4],
L. Sriharinath Reddy[5], And Kona Ricky Martin[6]

[1,3,4,5,6]Department Of Computer Science And Engineering
AarupadaiVeeduInstitute OfTechnology
VinayakaMission'S Research Foundation
Paiyanoor-603 104,Tamil Nadu, India.

[1]rjaichandran@avit.ac.in, [3]muthuselvan@avit.ac.in,
[4]jackson.malli08@gmail.com
[5]harinathsri20@gmail.com, [6]rickylovely777@gmai.com

Dr. Avinash Sharma[2**]

[2]*Professor, CSE Department, M.M. Deemed to be University, Mullana, Haryana, India, 133207*
asharma@mmumullana.org
Corresponding Author: Dr. Avinash Sharma[2]**

ABSTRACT. The current world is information world; without this information can't make due in present stage. This information created more from web- based media; this media information is public information; This public infor- mation did not have well security; so we applying the proposed method and it has 2 steps; 1. Addition property of the matrix;2. Perfect numbers swapped. The proposed method gives well security while comparing with Salsa method.

Key words: Commutative Property, RJB20, Salsa, Encryption, Decryption.

1. INTRODUCTION

The current world is information world; without this information can't make due in present stage. This information created more from web-based media; this media information is public information; This public information did not have well security; so to conquer this matter we apply the Salsa strategy. This strategy effectively hack the information from the programmers.The additional rotations XOR for ChaCha is fault attack [1]. This author is used new hash concept for key guessing and halting condition [2]. Author was introduced thw bricklayer attack for analysis of ChaCha [3]. They mainly focuse the security for Double A [4]. They made new design for secure fast and flexible algorithm [5]. SRB18 method used to give security for data [6]. SRB21 method used to give security for data [7]. CBB21 method used to provide security for data [8]. CBB22 method used to provide security for data [9]. Introducedthenew method RJB20 (RajaprakashJaichandran and BagathBasha) 20 for this problem.

2. METHODS

Commutative property of addition (CP): This property discuss in Table 1 and Table2.

3. ENCRYPTION

"A is analyzed matrix"; and "B is secret matrix". [10]

"Equation (1)"

$$\text{“A} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}\text{”}\ \text{“B} = \begin{pmatrix} 2 & 4 & 3 \\ 5 & 6 & 1 \\ 7 & 9 & 8 \end{pmatrix}\text{”}$$

$$\text{“CP} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}\text{”} + \text{“} \begin{pmatrix} 2 & 4 & 3 \\ 5 & 6 & 1 \\ 7 & 9 & 8 \end{pmatrix}\text{”}$$

$$\text{CP} = \begin{pmatrix} 3 & 6 & 6 \\ 9 & 11 & 7 \\ 14 & 17 & 17 \end{pmatrix}$$

Equations “(2)”

“Pair-1 (3, 0)”

$$\text{PN} = \begin{pmatrix} 9 & 6 & 6 \\ 3 & 11 & 7 \\ 14 & 17 & 17 \end{pmatrix}$$

“Pair-2 (1, 0)”

$$\text{PN} = \begin{pmatrix} 6 & 9 & 6 \\ 3 & 11 & 7 \\ 14 & 17 & 17 \end{pmatrix}$$

"Pair-3 (4, 0)""Pair-4 (2, 0)""Pair-5 (4, 5)""Pair-6 (3, 0)""Pair-7 (4, 0)"

"Pair-8 (5, 1)"

$$\text{PN} = \begin{pmatrix} 7 & 6 & 11 \\ 6 & 3 & 9 \\ 14 & 17 & 17 \end{pmatrix}$$

"Pair-9 (0, 4)"

$$\text{EM} = \begin{pmatrix} 3 & 6 & 11 \\ 6 & 7 & 9 \\ 14 & 17 & 17 \end{pmatrix}$$

TABLE 1. RJB20 Secure Encryption

STEPS	RJB20 SECURE ENCRYPTION
i	" The data analyzed from social data".
ii	"The data will form a matrix"
iii	"The commutative property (CP) concept applied in matrix CP" ”$CP = A + B = B + A$” **(1)**
iv	"Prime numbers in the Matrix A".
v	"$PN = (e^{k-1})(e^{k}) - 1$"**(2)**.
vi	"$EM = PN$ " where EM is EncryptedMatrix

TABLE 2. RJB20 Secure Decryption

STEPS	RJB20 SECURE DECRYPTION
i	"Prime numbers in the Matrix EM".
ii	$PN = (d^{k-1})(d^{k}) - 1$ **(3)**
iii	$DM\ 1 = PN$ where DM1 is Decrypted Matrix 1
iv	"Minus the secret key matrix B with the matrix DM1". $DM\ 2 = DM\ 1 - B$ **(4)** where DM2 is Decrypted Matrix 2

Equation "(3)"

"Pair-1 (4, 0)"

$$PN = \begin{pmatrix} 7 & 6 & 11 \\ 6 & 3 & 9 \\ 14 & 17 & 17 \end{pmatrix}$$

"Pair-2 (1, 5)"

$$PN = \begin{pmatrix} 7 & 9 & 11 \\ 6 & 3 & 6 \\ 14 & 17 & 17 \end{pmatrix}$$

"Pair-3 (0, 4)""Pair-4 (0, 3)""Pair-5 (5, 4)""Pair-6 (0, 2)""Pair-7 (0, 4)"

"Pair-8 (0, 1)"

$$PN = \begin{pmatrix} 9 & 6 & 6 \\ 3 & 11 & 7 \\ 14 & 17 & 17 \end{pmatrix}$$

"Pair-9 (0, 3)"

$$DM1 = \begin{pmatrix} 3 & 6 & 6 \\ 9 & 11 & 7 \\ 14 & 17 & 17 \end{pmatrix}$$

"Equation (4)". "DM2 = DM1 - B"

$$DM2 = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

4. CONCLUSION

Prediction of an environmental parameter is possible using sensing[16-20] or IoT [21-23] mechanism but prediction of security is based on features of data or Big Data[24,25]. Different kinds of prediction possible using various techniques including ML[26,27].

The current world is information world; without this information can'tmake due in present stage. This information created more from web-based media; this media information is public information; This public information did not have well security; so we applied the RJB20 method and it has 2 steps; 1. Ad- dition property of the matrix;2. Perfect numbers swapped. The RJB20 method giveswellsecuritywhilecomparingwithSalsamethod

REFERENCES

[1] P.A.BABUANDJ.J.THOMAS:*APRACTICALFAULTATTACKonARX-likeCipherswithACASE Study on CHACHA20,* Wo. onFa. Di. andTo. inCr. (2017),33-40.

[2] S. V. D. KUMAR, S. PATRANABIS, J. BREIER, D. MUKHOPADHYAY, S. BHASIN, A. CHATTOPADHYAY,ANDA.BAKS:*Freestyle,ARANDOMIZEDversionofCHACHAforresisting offline brute-force ANDDICTIONARY ATTACKS,* IE. tr. on In. Fo. and Se.(2018).

[3] ALEXANDRE ADOMNICAI, JACQUES J. A. FOURNIER, AND LAURENT MASSON: *Brick-LAYERATTACK:ASIDE-CHANNELANALYSISontheCHACHAQUARTERRound,*Pro.in Cry.Ind.,Lec. Not. in Com. Sci., Spr.65-84.

[4] BODHISATWA MAZUMDAR, SK SUBIDH ALI AND OZGUR SINANOGLU: *Power ANALYSISATTACKSonARX:AnAPPLICATIONtoSALSA20*,On-.Tes.Sym.IEE.(2015),40-43.

[5] C. WATT, J. RENNER, N. POPESCU, S. CAULIGI, AND D. STEFAN: *CT-WASM:Type-DrivenSecureCRYPTOGRAPHYfortheWebEcosystem*,Pr.ACMPr.La.PO.(2019),77:1-77:29.

[6] C. BAGATH BASHA, S. RAJAPRAKASH: *ENHANCING The Security Using SRB18 Method of Embedding Computing,* Mir. andMic 103125,(2020).

[7] C. B. BASHA, S. RAJAPRAKASH:*SecuringTwitterDATAUsingSrb21PHASEIMethod-ology*,Int.Jou.ofSci.andTec.Res.**8**(12)(2019),1952–1955.

[8] C. B. BASHA, S. RAJAPRAKASH: *Applying The CBB21 PHASE 2 Method For Securing Twitter ANALYSED DATA,* Ad. In Ma. : Sc. Jo. **9**(3) (2020),1085-1091.

[9] C. B. BASHA, S. RAJAPRAKASH, V. V. A. HARISH, M. S. KRISHNA, K. PRABHAS:*SecuringTwitterANALYSEDDATAUsingCBB22Algorithm*,Ad.InMa.:Sc. Jo. **9**(3) (2020),1093-1100.

[10] C.B.BASHA,K.SOMASUNDARAM:*ACOMPARATIVEStudyofTwitterSentimentANAL-ysis Using MACHINELEARNING Algorithms in Big DATA*, Int. Jou. of Rec. Tec. and Eng. **8**(1) (2019),591-599.

[11] Somasekar, J. & Sharma, A. & Reddy, N. & Reddy, Y.. (2020). IMAGE ANALYSIS FOR AUTOMATIC ENUMERATION OF RBC INFECTED WITH PLASMODIUM

PARASITES-IMPLICATIONS FOR MALARIA DIAGNOSIS. Advances in Mathematics: Scientific Journal. 9. 1221-1230. 10.37418/amsj.9.3.48.

[12] A. SHARMA AND J. SOMASEKAR "Contrast Image Construction Technique for Medical Imaging" published in Advances in Mathematics: Scientific Journal (Adv. Math., Sci. J.) vol-9-no-6-2020 (pp 3325–3329)

[13] *Rohini Goel, Avinash Sharma, and Rajiv Kapoor,* "Object Recognition Using Deep Learning" published in Journal of Computational and Theoretical Nanoscience Vol. 16, 4044–4052, 2019

[14] Santosh, Mamta & Sharma, Avinash. (2019). A Proposed Framework for Emotion Recognition Using Canberra Distance Classifier. Journal of Computational and Theoretical Nanoscience. 16. 3778-3782. 10.1166/jctn.2019.8250.

[15] Mamta Santosh, Avinash Sharma, "Facial Expression Recognition using Fusion of LBP and HoG Features" published in International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-8 June, 2019

[16] Varsha, N. Kumar, Energy Efficient TABU Optimization Routing Protocol for WSN,IngenieríaSolidaria, Universidad Cooperativa de Colombia, Issue- 33, July 2020.

[17] G.Arora, A.Kumar, Versha, N.Kumar, "Swarm Intelligence based QoS optimized routing in WSN", Test Engineering & Management, Vol.-82, 2020.pp-12880-12885.

[18] Varsha, M. B., Kumar, M., & Kumar, N. Hybrid TABU-GA Search For Energy Efficient Routing In WSN. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4, November 2019.P.-3250-3256.

[19] Varsha, M. B., Kumar, M., & Kumar, N. Development of QoS optimized routing using Artificial bee colony and TABU-GA with a mobile base station in Wireless Sensor Network, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-1, November 2019.

[20] Awadhesh Kumar Maurya,Varsha, Neeraj, Ajay Kumar, Neeraj Kumar, "Improved chain based cooperative routing protocol in wsn", FEST, Journal of Physics: Conference series, IOP Publishing, 1478,1-8, 13/05/2020.

[21] N. Kumar, A. Agrawal,R. A. Khan, "METHWORK: An Approach for Ranking in Research Trends with a Case Study for IoET, Recent advances in Computer Science and Communication (formerly Recent Patents on Computer Science), 2019.

[22] Neeraj Kumar; PareshGoyal; GayatriKapil; AlkaAgrawal; Raees A Khan, "Flood Risk Finder for IoT based Mechanism using Fuzzy Logic", Materials Today: Proceedings, Elsevier, 2020.

[23] Kumar, Neeraj, AlkaAgrawal, and R. A. Khan. "Cost estimation of cellularly deployed IoT-enabled network for flood detection." *Iran Journal of Computer Science* , issue 2, no. 1 (2019), Springer Nature: 53-64.

[24] V. Velvizhi; Satish R Billewar; GauravLondhe; PravinKshirsagar; Neeraj Kumar, "Big Data for Time Series and Trend Analysis of Poly Waste Management in India", Materials Today: Proceedings, Elsevier, 2020.

[25] G. Arora, A. K. Maurya,N. Kumar, A. K. Mishra, "Application of big data generated by IoT environment for HealthCare using Voice Recognition", International journal of research in engineering, IT and Social Sciences, vol.-08, issue-11, November 2018, page. 132-136.

[26] Manoj Diwakar, AmrendraTripathi, Kapil Joshi, MinakshiMemoria , Prabhishek Singh, Neerajkumar, "Latest Trends on Heart Disease Prediction using Machine Learning and Image Fusion", Materials Today: Proceedings,Elsevier, 2020.

[27] ParthWadhwa; Aishwarya; AmrendraTripathi; Prabhishek Singh; Manoj Diwakar; Neeraj Kumar, "Predicting the Time Period of Extension of Lockdown due to Increase in Rate of COVID-19 Cases in India using Machine Learning", Materials Today: Proceedings Elsevier, 2020.