iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XI **Month of publication:** November 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

A Hybrid Soft Computing Approach on Security Algorithm of Cryptography

Vikas Sagar[1], Krishan Kumar[2]
[1, 2] *Department of Computer Science, Faculty Of Technology Gurukul Kangri University, Haridwar*

***Abstract*: Cryptography is a security mechanism to secure data from unauthorized access during the data transmission over the public channels. Ubiquitous use of internet over public channel makes easy to data retrieval from data transmission. Many algorithms are already exited as such RSA, DES, BLOWFISH and many more. In this paper we will proposed and implement an effective cryptography security method based on soft -computing techniques (neural network and Genetic). So the result is going to be additional correct then previously implemented methods. In depth experiments demonstrate that our new proposed method achieves fascinating performance on real-life events over other methods. Proposed system our main aim to find an easy and fast solution for users to send data with a more secure and trusted way over the public channels. So that their personal information not captured by any unauthorized entity.**

***Keywords*: Cryptography, Symmetric key, Asymmetric key, RSA, DES, Neural Network.**

I. INTRODUCTION

Security is a simple need in human environment in all perspective. These days the vast majority conveys over open channel and there, they transmit data that is extremely delicate and individual.

So plainly security is extremely and essential worry in present time. Cryptography is a route by which we can secure our information from unapproved get to or illicit passage of obscure substance. In cryptography we utilize some numerical technique that progressions the first information so it cannot be perused without a key.

The primary target of this paper is to applying the neural system in cryptography for secure information correspondence and to enhance the proficiency of cryptographic calculation.

Essentially neural system used to take care of the intricate issue like: predication, self association, self learning, irregular number and so forth. The principle qualities of neural system are system structure, adaptation to non-critical failure, aggregate arrangement, learning capacity, parallel handling, and conveyed memory.

Here with the utilization of neural system we propose another successful cryptographic calculation for secure information correspondence.

II. CRYPTOGRAPHY

We utilize cryptography to guarantee that data is avoided anybody for whom it is not expected, even the individuals who can see the encoded information. It is utilized from antiquated time for secure information interchanges. Cryptography is very important part of a few fields: data security and related issues, especially, validation, and get to control. From the conventional methodologies of cryptographic calculation encryption and decoding procedure are finished by the utilization of complex numerical capacities. In all cases, the beginning decoded information is alluded to as plaintext (P) which is the unique message. It is encoded into ciphertext (C), which will in transform be decoded into usable plaintext by utilizing key (K).

C=Encrypt (K, P), P=Decrypt (K, C).

The prime aims of cryptography are given as:

A. Confidentiality

Confidentiality is the basic security benefit gave by cryptography. It is a security administration that keeps the data from an unapproved individual. It is some of the time alluded to as security or mystery.

B. Data integrity

Data integrity implies information may get adjusted by an unapproved element purposefully or accidently. Information controls take impacts, for example, information alteration, addition and cancellation. Respectability benefit likewise affirms that whether information is in place or not since it was last made, transmitted, or put away by an approved client.

©IJRASET (UGC Approved Journal): All Rights are Reserved

C. Authentication

Confirmation identified with recognizable proof, implies an administration ought to be bona fide or genuine. It affirms to the collector that the information got has been sent just by a recognized and checked sender. Authentication service has two variants:

D. Non-repudiation

This security benefit guarantees that a substance can't decline on their past activity. It is guarantee that the sender or beneficiary of the information can't preclude for their activity from claiming sending or getting of the information. Non-denial is a property that is most alluring in circumstances where there are odds of a disagreement regarding the trading of information.

III.OVERVIEW OF SYMMETRIC KEY CRYPTOGRAPHY

As the name demonstrates, in symmetric key cryptography just a single key is utilized for both encryption and decoding [11]. Symmetric cryptography, likewise called private-key cryptography. Symmetric key figures are executed in two routes as: Stream figures or Block figures. A stream figure enciphers contribution to individual characters of plaintext instead of, the pieces input frame utilized by a square figure.

A. There are five main components in symmetric key cryptography scheme

1) *Plaintext:* Information that can be perused and comprehended with no unique measures is called plaintext and it is send by sender to beneficiary over people in general channel.
2) *Encryption Algorithm: The* strategy by which we can shroud the substance of plaintext is called Encryption calculation. Different substitutions and changes mixes perform over the plaintext as indicated by the encryption systems by which the plaintext make convoluted.
3) *Secret Key:* Mystery enters utilized as a part of the encryption and decoding process. The mystery key is critical in cryptography. Substitutions and stages operation in the calculation likewise rely on upon the key size and each time the calculation will create an alternate yield contingent upon the particular key being utilized around then
4) *Ciphertext:* Ciphertext is the last garbage type of plaintext that is created with the assistance of encryption calculation. The many-sided quality of Ciphertext is diverse each time and relies on upon the plaintext and size of the key and in addition encryption calculation.
5) *Decryption Algorithm:* The way toward returning ciphertext to its unique plaintext is called decoding. Unscrambling procedure is recently turned around procedure of the encryption calculation. [2], [5], [12].
6) *Cryptanalysis:* The study of ciphertext in an attempt to restore the message to plain text. In cryptography there will Conventional encryption algorithms, public key cryptography algorithms were proposed by authors. In the next section we are going to survey on recent encryption algorithms by several authors.

IV. GENETIC ALGORITHM

Genetic Algorithm (GA) was firstly utilized as a part of Natural and Artificial Systems of 1975 by John Holland Adaptation. Hereditary calculations are a group of computational models having a place with the class of developmental calculations, a portion of manmade brainpower. They are frequently seen as capacity streamlining agents. Genetic Algorithms are the heuristic inquiry and streamlining systems that copy the procedure of characteristic advancement. An implementation of a Genetic algorithm shown in figure 1:

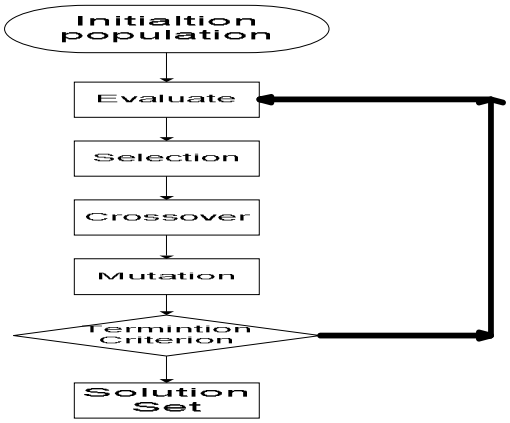


Fig.1. Basic Architecture of Genetic Algorithm

©IJRASET (UGC Approved Journal): All Rights are Reserved

1) Initialization: as the name demonstrates starting populace is make arbitrarily over the search space. It can likewise be or characterized by the client.
2) Evaluation: Evaluation is the second phase after the initialization of population, where the fitness values are evaluated.
3) Selection: The fittest chromosomes that have highest ability and probability is to be selected. This selection is done for the next generation. This process is called selection. We must compute the fitness of each chromosome to find out the fittest probability chromosome.
4) Crossover: Crossover plays in the outline and usage of powerful developmental frameworks. At least two sections of parental answers for make new, conceivably better arrangements are named Crossover consolidate. There are diverse strategies for Crossover.
5) Mutation: Mutation is a randomly modification in the solution that is perform just after the crossover operates on two or more parental chromosomes. There are different types of method of mutation. The process of mutation is done by replacing the gen at random position with a new value [8], [9].

We use GA with uniform crossover and single point mutation for the encryption in proposed cryptography algorithm.

A. Uniform Crossover

The Uniform Crossover takes settled proportion between two irregular chose guardians. The uniform hybrid used to makes the information confused in this cryptographic calculation. In this hereditary technique we apply hybrid over the paired type of plaintext to expand the many-sided quality of the encryption side. The uniform crossover shown in figure 5:

B. Single point mutation

Point transformation happens at a certain point. It is an arbitrary transformation in the deoxyribonucleic corrosive (DNA). Point transformation occurs amid DNA replication so that there is a change inside a quality (twofold numbers) in which one base combine in the DNA grouping is adjusted. We play out this single point transformation when we get the information originating from hybrid segment [11], [12], [14].

V. OVERVIEW OF ARTIFICIAL NEURAL NETWORK

The present day period of neural system research is credited with the work done by neuron-physiologist, Warren McCulloch and Walter Pitts in 1943. McCulloch had put in 20 years of life contemplating the "occasion" in the sensory system that permitted to us to think, feel, and so on. The following real advancement in neural system innovation touched base in 1949 with a book, "The Organization of Behaviour" composed by Donald Hebb. The natural neuron has distinctive components. An organic neuron has one Nucleus and numerous Dendrites, Axon and Synapse. Common neurons get motions through neurotransmitter which are situated on the dendrites and radiates a flag however the Axon. Artificial neural network is the complex artificial copy of the biological neuron system like brain [4], [8], [16].

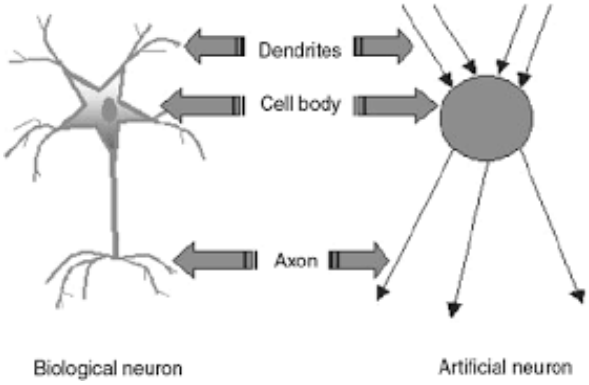


Figure.2. Biological Neuron vs. Artificial Neuron

A. Basic elements which we have to take care to make an artificial neuron are-

1) Input
2) Weights
3) Activation function

©IJRASET (UGC Approved Journal): All Rights are Reserved

4) Total signal reaching at output are given by:

5) Output (y) =

$$\sum_{i=1}^{n} Wi\ Xi$$

6) Output may be more than one it depends on number of neuron i.e. multiple neuron will cause multiple output.

7) A number of artificial neurons make an artificial neural network which help to process information.

B. Counter propagation method

CPN presented by R. Hecht-Nielsen in 1987. Bidirectional mapping is utilized for learning in CPN. There are three layers in CPN: Input layer, Kohonen layer and Grossberg layer. The CPN are of two types

1) Full CPN

2) Forward Only CPN

The basic structure of the CPN is shown in the figure below

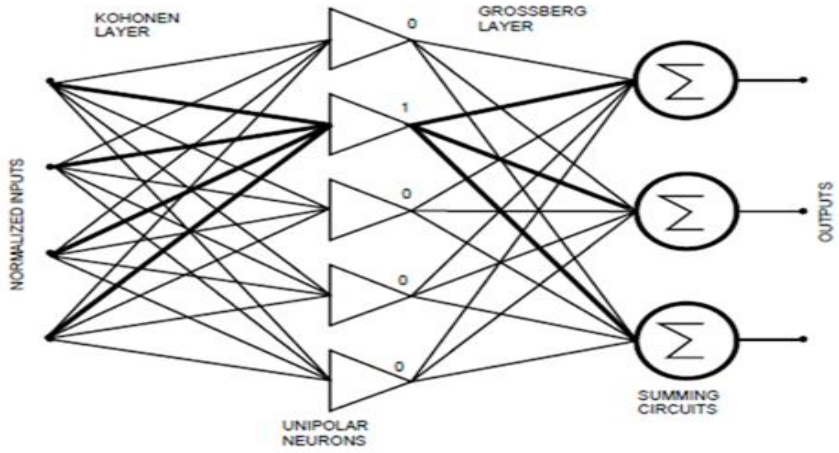


Figure.3.Structure of CPN

There are two learning scheme used in CPN: supervised learning scheme and unsupervised learning scheme. The unsupervised learning scheme used in Kohonen layer and the supervised learning scheme work over Grossberg layer. The weights are change according to the learning process automatically [1], [15].

The learning Process:

$v_{ij}(new) = v_{ij}(old) + a[x_i - v_{ij}(old)]$, i= 1 to n

$w_{kj}(new) = w_{kj}(old) + \beta[y_k - w_{kj}(old)]$, k= 1 to n

Where

x= input training vector

y= target output

v_{ij}= weight from X-input layer unit

w_{kj}= weight from Y-input layer unit

$u_{ik}(new) = u_{jk}(old) + a[y_k - u_{jk}(old)]$, k= 1 to m

$t_{ji}(new) = t_{ji}(old) + b[x_i - t_{ji}(old)]$, i= 1 to n

Where

u_{ik}= weight from cluster layer unit to y output layer

t_{ji}= weight from cluster layer unit to x output layer

©IJRASET (UGC Approved Journal): All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

C. Error back propagation neural network (EBP-NN)

Error back propagation neural system is a usually utilized regulated supervised neural system. This system is straight forward and plan. The Error back propagation neural system is combination of basic handling components (nodes or neurons) which orchestrate in layers and cooperating to create an intricate yield. Subsequent to picking the weights of the system arbitrarily, the Error back propagation neural system calculation utilized to figure the fundamental redresses. [12], [13].

D. The Forward Pass

The main info layer takes the information vectors and engender to the centre layer.

Centre layer hubs acknowledge the contribution from info layer and register values, which execute as contributions to the hubs of the shrouded layers or yield layer.

At long last the yield layer hubs process the system yield for the specific info vector.

E. Calculating the Total Error

Now here calculate the error for each output neuron using the squared error function and sum them to get the total error:

$$E_{total} = \sum \frac{1}{2}(target - output)^2$$

F. The Backwards Pass

Finally update the weights in the network so that the network can achieves the target output by minimizing the error.

1) Algorithm: The Proposed Hybrid neural cryptography algorithm.

G. Encryption Phase

The data that sender wants to send is called Plaintext.

1) Apply this plaintext as input information.
2) Transform the plaintext in ASCII format.
3) Change Change the ASCII esteem into twofold esteem assume N bits (utilize this double an incentive as "Target esteem" for the Error back proliferation neural system. Send Target an incentive to EBPNN by secure channel).
4) Divide data information into two equivalent sizes (N/2 bits, N/2 bits) Block.
5) Block 1: (N/2)

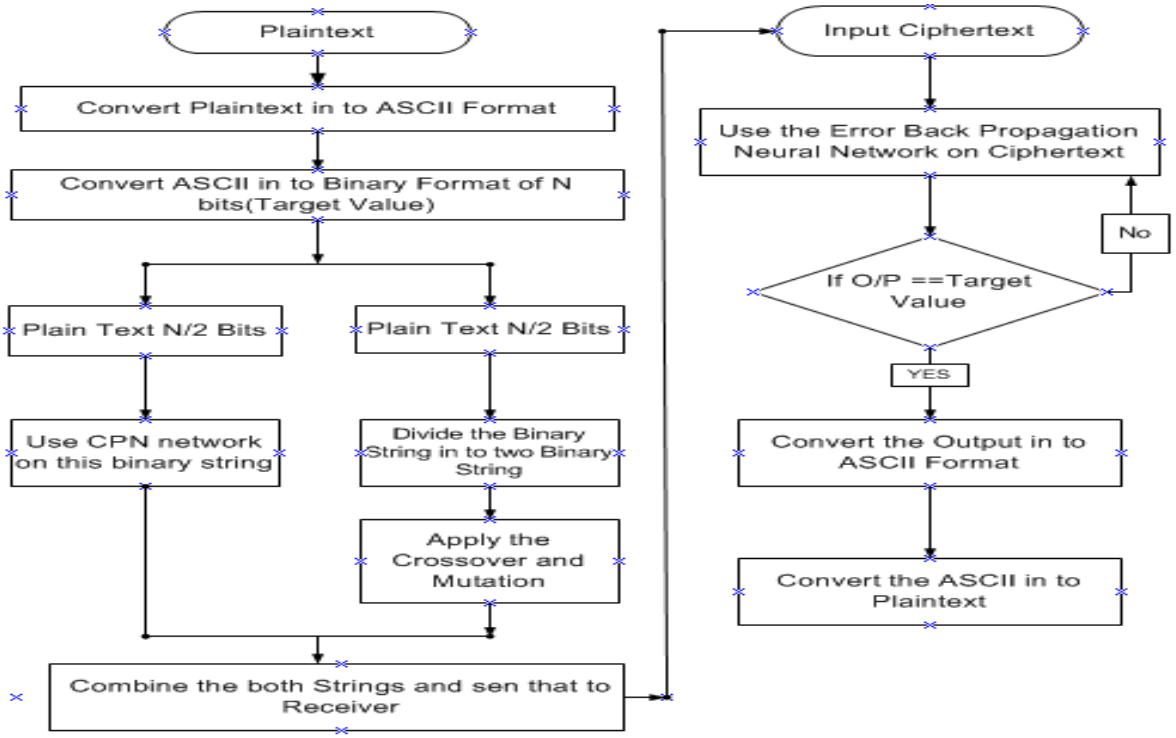


Fig.4. Flowchart of Algorithm

©IJRASET (UGC Approved Journal): All Rights are Reserved

VI. IMPLEMENTATION OF ALGORITHM

We implement the proposed algorithm utilizing Java language dialect as per Figure 12. The consequences of execution demonstrate the proposed cryptography is possible, and has a decent execution of encryption and decoding speed. e.g. In scratch pad PC of DELL INSPIRON 5000, the speed of information encryption and decoding tried are (398.0±4.2) KB/S (P=0.05) and (9332.4±148.4) kB/s (p=0.05), separately. The speed of information encryption for the proposed conspire utilizing programming actualizing is over that of RSA (45.8kbps) utilizing equipment actualizing. Coincidentally, any content with figure and table, or executable program can be encoded and safely transmitted by means of the Internet utilizing our product cryptosystem.

VII. SIMULATION RESULT

Here we present some of simulation results with respect to size and time of different cryptographic algorithms (AES, DES, RSA and New Algo). The given Table 1 describe the time duration that is taken by different cryptographic algorithms on different data sizes.

Table -1 Experiment Result

S.no	Method	Data Size Bytes	Encryption Time (Second) T	Decryption Time (Second) T
1.	AES	N=128	1.71	.71
	DES		2.51	1.11
	RSA		3.21	1.95
	NEW ALGO		1.61	.60
2.	AES	N=256	1.90	.81
	DES		2.98	1.18
	RSA		4.41	2.20
	NEW ALGO		1.80	.76
3.	AES	N=512	2.01	1.01
	DES		3.25	1.96
	RSA		4.96	2.85
	NEW ALGO		2	1
4.	AES	N=1024	2.55	1.50
	DES		3.82	2.11
	RSA		5.08	3.25
	NEW ALGO		2.21	1.23

Where N=No of bytes of data
T= time in second
By analyzing the Table1 we plot a graph between sizes of data and time taken by different cryptographic algorithms.

©IJRASET (UGC Approved Journal): All Rights are Reserved

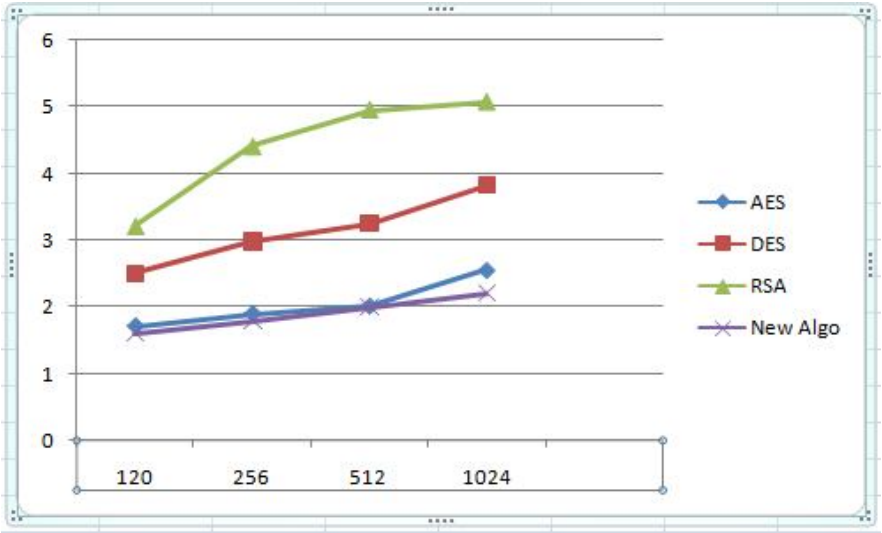


Fig.5. Comparison of Encryption Time among AES, DES RSA and New Algo

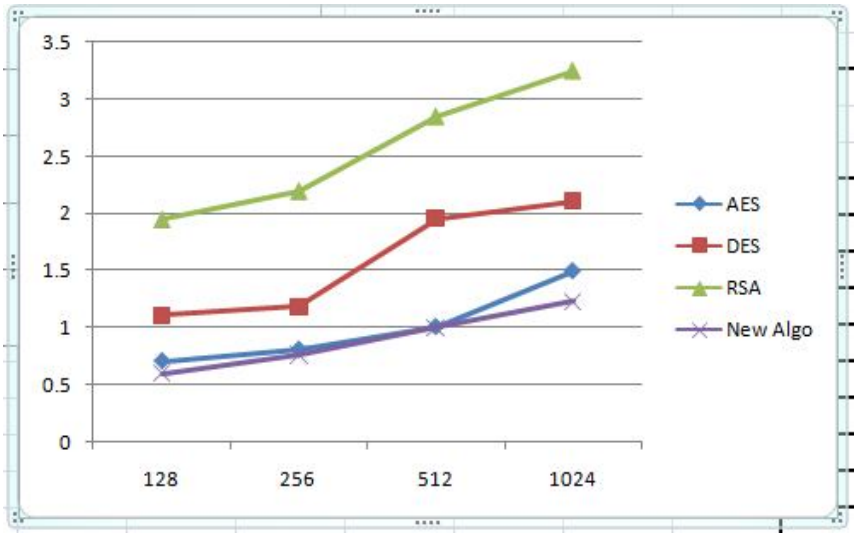


FIG.6. COMPARISON OF DECRYPTION TIME AMONG AES, DES RSA AND NEW ALGO

Fig-5 and Fig-6 demonstrates the time taken for encryption and decryption on different size of data. RSA calculation takes much longer time contrast with time taken by AES, DES and New Algo calculation. New Algo and DES calculation demonstrate extremely minor distinction in time taken for encryption and decoding prepare. Final result this shown that new algorithm perform better than previous implemented algorithms. Besides these we also have to check this algorithm's complexity and security against different attacks.

VIII. CONCLUSION

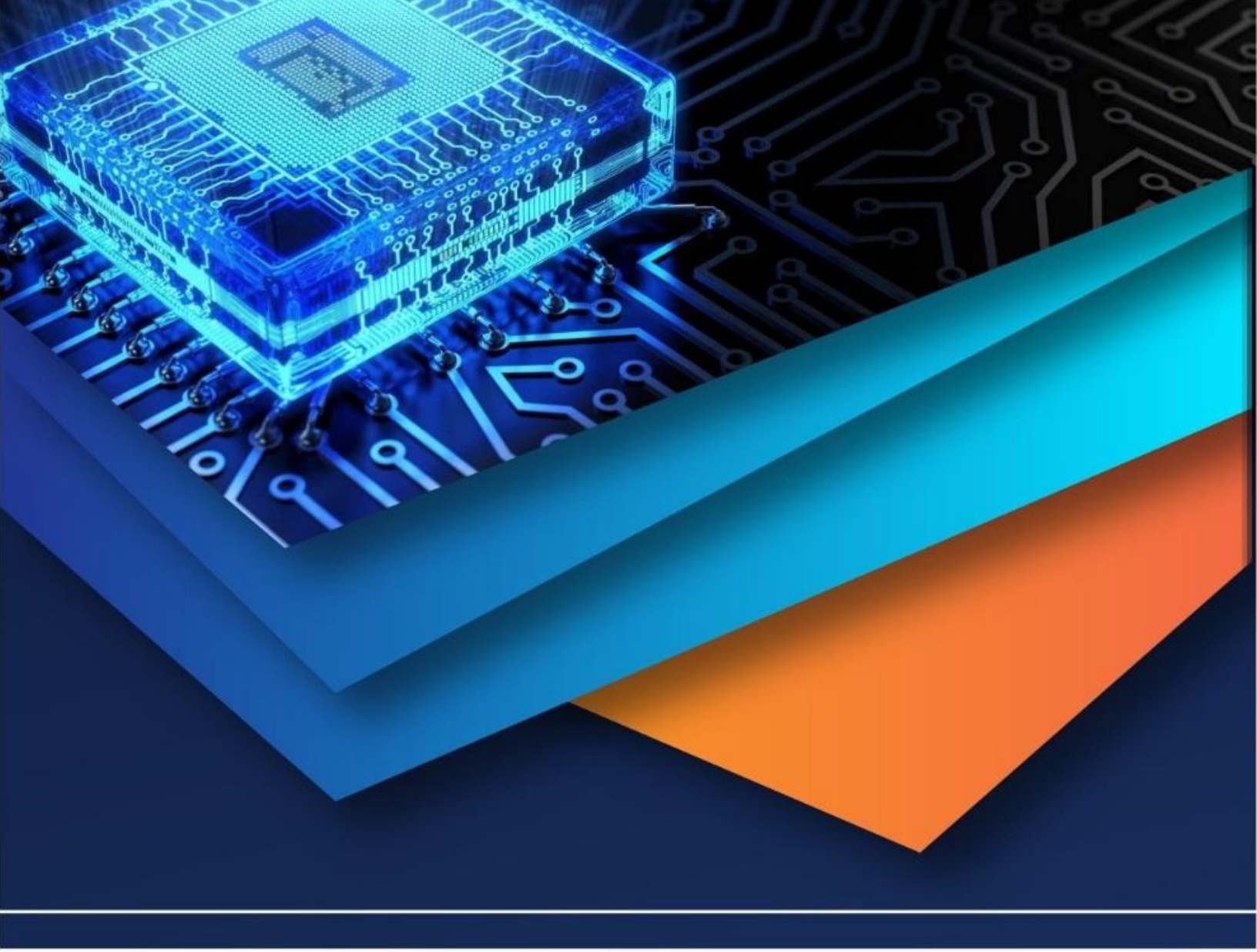
The prime target of this research paper is to create a hearty cross breed security calculation. This cross breed cryptographic calculation utilize hereditary calculation and neural systems through which correspondence over the wired or remote system medium can be perform with the compelling and proficiently. The information is more secure and unusual amid the correspondence by this calculation. This calculation fits to sending and getting the information safely with no effect over the execution because of low or high data transmission of system. This calculation assist of various key era so that lessening handling overhead and accomplishing lower memory utilization is the suitably for applications. Consequently the time multifaceted nature of this calculation will be less in contrast with the other conventional calculations like DES, AES, and RSA.

©IJRASET (UGC Approved Journal): All Rights are Reserved

REFERENCES

[1] Fi-John Chang, Yen-Chang Chen ," A counter propagation fuzzy neural network modeling approach to real time stream flow prediction", journal of hydrology, ELSEVIER, 6 February 2001.
[2] Adel A. El-Zoghabi, Amr H. Yassin, Hany H. Hussien, " Survey Report on Cryptography based on Neural Network" International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459), Vol. 3, Issue 12, December 2013.
[3] O.S. Eluyode1 and Dipo Theophilus Akomolafe2 "Comparative study of biological and artificial neural networks" European journalof applied Engineering and scientific research, 2013,2,1. ISSN: 2278-0041.
[4] Khalil Shihab " A Back Propagation Neural Network For computer Network Security", Journal of Computer Science 2 (9): 710-715, 2006 ISSN 1549-3636.
[5] Eva Volna, Martin Kotyrba, Vaclav Kocian and Michal Janosek "Cryptography based on neural network" Proceedings 26th European Conference on Modelling and Simulation ©ECMS Klaus G. Troitzsch, Michael Möhring, Ulf Lotzmann (Editors) ISBN: 978-0-9564944-4-3 / ISBN: 978-0-9564944-5-0, ecms2012.
[6] Vikas Sagar, Krishan Kumar "A symmetric key cryptography using counter propagation neural network " International Conference on Information and Communication Technology for Competitive Strategies" ACM ICPS Proceedings Volume ISBN No 978-1-4503-3216-3.
[7] Khalil Shihab "A cryptographic scheam based on neural network" 10th WSEAS International Conference on COMMUNICATIONS, Vouliagmeni, Athens, Greece, July 10-12, 2006
[8] Man, K.F. "Genetic algorithms: concepts and applications" Industrial Electronics, IEEE Transactions on (Volume:43 , Issue: 5), ISSN 0278-0046.
[9] Vikas sagar, Krishan Kumar, " A Symmetric Key Cryptography using Genetic Algorithm and Error Back Propagation Neural Network", 2015 2nd International Conference on "Computing for Sustainable Global Development", 11th – 13th March, 2015 Bharati Vidyapeeth"s Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA).
[10] Sanjeev Kumar, Krishan Kumar and Anand Pandey, A Comparative Study of Call Admission Control in Mobile Multimedia Networks Using Soft Computing, International Journal of Computer Applications, (ISSN: 0975–8887), vol. 107, no. 16, December (2014).
[11] Vikas Gujral, "Cryptography using Artifical neural network", Engineering National Institute of Technology Rourkela-769008 Orissa, Session 2005-2009.
[12] Menezes, P. van Oorschot and S. Vanstone, "Handbook of Applied Cryptography". CRC Press, First ed., 1997J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
[13] Laurene Fausett(1994), "Fundamentals of Neural Networks , Architecutre, Algorithms and Applications', published by arrangement with Pearson Education, Inc. and Dorling Kindersley Publishing Inc.
[14] S. Kumar, K. Kumar and P. Kumar, Mobility Based Call Admission Control and Resource Estimation in Mobile Multimedia Networks Using Artificial Neural Network, In 1st International Conference on Next Generation Computing Technologies (NGCT-2015), ISBN 9781467368070, pp. 852–857, 4–5 September (2015).
[15] Zurada, Jacek M. (1999), 'Introduction to artificial neural systems', published by West Publishing Company, printed in United States of America.
[16] Sanjeev Kumar, Krishan Kumar and Anand Pandey, Dynamic Channel Allocation in Mobile Multimedia Networks Using Error Back Propagation and Hopfield Neural Network (EBP-HOP), Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016).
[17] Mohit Mittal, "Performance evaluation of cryptographic algorithms International Journal of Computer Applications, vol. 41, no 7, 2012, pp. 1-6.
[18] Mohit Mittal and Krishan Kumar, "Network lifetime enhancement of homogeneous sensor network using ART1 neural network", Sixth International conference on computational intelligence and communication networks, IEEE, 2014, pp. 472-475.
[19] M. Mittal and K. Kumar, "Delay Prediction in Wireless Sensor Network Routing Using ART1Neural Network," African Journal of Computing & ICT, Vol 8. No. 3, pp. 175 -180, 2015.
[20] M. Mittal and K. Kumar, "Energy Efficient Homogeneous Wireless Sensor Network Using Self- Organizing Map (SOM) Neural Networks," African Journal of Computing & ICT Vol 8. No. 1, pp. 179-184, 2015.
[21] S. Gangwar, K. Kumar & M. Mittal, "Cluster Head Selection in Mobile Ad-hoc Network (MANET) Using ART1 Neural Network," African Journal of Computing & ICT, Vol 8. No. 1, pp. 197-204, 2015.

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)