International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST52411186

Design And Implementation of Network Security Using Neural Network

Pankaj Sadhukhan[1], Aniruddha Karmokar[2], Arkodip Ganguly[3], Soumya Paul[4]

[1-3]Student, Bachelor of Computer Science, Ramakrishna Mission Vivekananda Centenary College, Rahara, West Bengal, India

[4]Principal and Professor in Computer Science Engineering, St. Mary's Technical Campus Kolkata, West Bengal, India

ARTICLEINFO

Article History:

Accepted: 20 Feb 2024
Published: 03 March 2024

Publication Issue :
Volume 11, Issue 2
March-April-2024
Page Number :
22-27

ABSTRACT

The number of internet users is increasing day by day. To keep internet surfing safe from vulnerable exploits we need to design new powerful algorithm. Hence this paper is mainly concerns with implementation of Neural Network using symmetric key cryptography to ensure confidentiality, authentication, integrity and message non-repudiation. In order to achieve the above objectives first an encryption algorithm is developed and implemented. The program takes a plain text as an input from the user to generate an intermediate cipher text and sends it to the source node of the neural network. At this point the intermediate cypher text is passed through some successive hidden layers of neural network's concept to produce final cipher text. Now to recover the plain text from the final cipher text a decryption algorithm is developed and implemented.

Keywords : Symmetric Key cryptography, Neural Network.

I. INTRODUCTION

A. Network Security

Network security consists of the provisions and policies to prevent and monitor unauthorized access, misuse, modification or denial of a computer network and network - accessible resource. Network Security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned a password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everybody jobs conducting transactions and communications among business, government agencies and individuals.

B. Neural Network

The concept of neural-based cryptography was first introduced by Laurie in

1990.Artificial neural networks have motivated from their inception by the recognition that the brain computers in an entirely different way from the conventional digital computer. The brain contains billions of neurons with massive interconnections. Similarly, neural networks are massively parallel distributed p rocessors that are made up of artificial neurons with interconnections. These are nonlinear dynamic machines which expand the expansion of input data as a linear combination of inputs to synapse and then perform a nonlinear transformation to compute output.

C. Symmetric Key

Symmetric key algorithm creates a fixed length of bits known as a BLOCK CIPHER with a secrete key that the creator/sender uses to encipher data (encryption) and the receiver uses to decipher it.

II. PROBLEM STATEMENT

The goal of this project is to develop an encryption algorithm using neural network algorithm techniques for data security in long hall transmission through computer networks. The algorithm will be designed to take in plain text as input and produce a corresponding cipher text as output. The cipher text will be difficult to decipher without knowledge of the key used in the encryption process. Finally, the encrypted cipher text will be decrypted at the receiver end applying the symmetric key to get the main text back into its old format.

III. PROPOSED ALGORITHM

A. Proposed Encryption Heuristic

Input: Plain text is given. Output: Encrypted cipher text.

Step 1: Start.

Step 2: Take input from the user and store it into a string array (Say strarr). Step 3: Fill the blank spaces using special character "^".

Step 4: Take the ASCII value of each array element.

Step 5: Now calculate the no. of the even index elements and assign it to count_1. Also calculate the no. of odd index elements assign it count_2.

Step 6: Add count_1 value with each even index element and add cont_2 value with odd index element.

Step 7: Merge even index value and odd index value alternatively and store it into keyarr.

Step 8: Stop.

B. Proposed Encryption Heuristic Using Neural Network

Input: Cipher text is obtained in initial encryption. Output: Successively encrypted cipher text.

Step 1: Start.

Step 2: Take the plain text string array strarr.

Step 3: Merge strarr and keyarr alternatively to obtain the locked with key. Step 4: Now take the locked with key array take the ASCII list.

Step 5: Divide the array into even index and odd index and send it to Node 1 and Node 2 respectively after adding 2 with each even index element and subtract 2 with each odd index element

Step 6: Write the character value of the corresponding ASCI value of Node 1 and Node 2.

Step 7: Now reverse the Non-vowels of The Node 1 and send it to Node 3. Step 8: Reverse the vowels of the Node 2 and send it to Node 4.

Step 9: Merge the Node 3 and Node 4 alternatively to get the final cipher text. Step 10: Stop.

C. Proposed Decryption Heuristic Using Neural Network

Input: Encrypted Cipher text

Output: Decrypted Cipher

Step 1: Start.

Step 2: Take the cipher text into list format.

Step 3: Divide the list according to even and odd position into Dnode 1 and Dnode 2. Step 4: Interchange the Non-vowels of Dnode 1.

Step 5: Interchange the vowels of Dnode 2.

Step 6: Now take the ASCII list of Dnode1 and Dnode 2.

Step 7: Subtract 2 from each even index element of Dnode 1 and send it to Dnode 3. Step 8: Add 2 with each odd index element of Dnode 2 and send it to Dnode 4.

Step 9: Write the character value of the corresponding ASCII list of Dnode 3 and Dnode 4.

Step 10: Merge Dnode 3 and Dnode 4 alternatively to get the locked with key. Step 11: Stop.

D. Proposed Decryption Heuristic Input: Decrypted Cypher Text. Output: Plain Text.

Step 1: Start.

Step 2: Divide the locked with key array according to even and odd index and store it into L1 and L2 respectively.

Step 3: Now L2 is our key and L1 is the list which will generate our plain text. Step 4: Stop.

E. Proposed Cryptographic Algorithm

Step 1: Start.

Step 2: Take the plain text string as input. Step 3: Call the encryption algorithm. Step 4: Cipher text generated.

Step 5: Call the decryption algorithm.

Step 6: Palin text retrieved.

Step 7: Stop.

IV. Example Illustration

A. *Example Illustrating Key Generation Algorithm*

Plain Text: - Namaste India

- Text array generation

Corresponding plain text array-

N	a	m	a	s	t	e		I	n	d	i	a

- Key array generation

Empty spaces or blank space will be occupied by '^'

N	a	m	a	s	t	e	^	I	n	d	i	a

Take the ASCII value of the array-

78	97	109	97	115	116	101	94	73	110	100	105	97
[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]

- Now we have to do the following operation-

  Even index value + total no of even index
  Odd index value + total no of odd index

85	103	116	103	122	122	108	100	80	116	107	111	104

Take the character value of the modified array

U	g	t	g	z	z	l	d	p	t	k	o	h

So our key: - "Ugtgzzldptkoh"

B. *Example Illustrating Cipher Text Generation Algorithm*

Take the plain text array: -

N	a	m	a	s	t	e		I	n	d	i	a

Take the key array: -

U	g	t	g	z	z	l	d	p	t	k	o	h

Merge plain text array and key array alternatively: -

N	U	a	g	m	t	a	g	s	z	t	z	e	l		d	I	p	n	t	d	k	i	o	a	h

So the text now becomes:

"NUagmtagsztzel dIpntdkioah" which is to be send through neural network.

C. Neural Network

Intermediate Cipher text array: -

N	U	a	g	m	t	a	g	s	z	t	z	e	l		d	I	p	n	t	d	k	i	o	a	h

Take the ASCII value of the list

78	85	97	103	109	116	97	103	115	122	116	122	101	108

32	100	73	80	110	116	100	107	105	111	97	104

Divide the array into even index and odd index and send it to Node1 and Node2 after adding 2 with each even index element and subtract 2 with odd index element.

80	99	111	99	117	118	103	34	75	112	102	107	99

← Node 1

83	101	114	101	120	120	106	98	78	114	105	109	102

← Node 2

After changing to corresponding character value of Node1 and Node2 reverse the Non-vowels of Node1 and send it to Node3 and reverse the vowels of Node2 and send it to Node4.

c	k	o	f	u	p	K	“	g	v	c	c	P

← Node 3

S	i	r	e	x	x	j	b	N	r	e	m	f

← Node 4

Merging Node3 and Node4 alternatively we get our final encrypted text.

c	S	k	i	o	r	f	e	u	x	p	X	K	j	‘’	b	g	N	v	r	c	e	c	m	P	f

So our final encrypted cipher text `**cSkiorfeuxpXKj”bgNvrceecmPf`**

D. Decryption

Encrypted Text: - cSkiorfeuxpXKj”bgNvrceecmPf

Corresponding plain text array-

c	S	k	i	o	r	f	e	u	x	p	X	K	j	‘’	b	g	N	v	r	c	e	c	m	P	f
[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[17]	[18]							

Now send the even index element to Dnode1 and odd index element to Dnode2.

c	k	o	f	u	p	K	“	g	v	c	c	P

← Dnode1

S	i	r	e	x	x	j	b	N	r	e	m	f

← Dnode2

Now for Dnode1 interchange the Non-vowels and subtract 2 from their ASCII value and send to Dnode3.

P	c	o	c	u	v	g	“	K	p	f	k	c

78	97	109	97	115	116	101	32	73	110	100	105	97

← Dnode3

For Dnode2 interchange the vowels and add 2 with their ASCII value and send to Dnode4.

S	e	r	e	x	x	j	b	N	r	i	m	f

85	103	116	103	122	122	108	100	80	116	107	111	104

← Dnode4

After merging Dnode3 and Dnode4 alternatively change the ASCII value to their character value and we get back the intermediate cipher text.

N	U	a	g	m	t	a	g	s	z	t	z	e	l		d	I	p	n	t	d	k	i	o	a	h

Finally, as it is an Symmetric key concept, the main text is being finally decrypted by removing the key from the intermediate cipher text array.

Finally, we get the plain text: - Namaste India.

IV. CONCLUSION

In this work, Network security using neural network heuristic is being used. A symmetric key cryptography using mathematical function along with the neural network algorithm has been implemented to ensure confidentiality in transferring messages in the form of encrypted format.

V. REFERENCES

[1]. Cryptography and Network Security, Third Edition, by Atul Kahate.

[2]. An Introduction to Neural Networks, by Kevin Gurney, Kevin N. Gurney.

Cite this article as :

Pankaj Sadhukhan, Aniruddha Karmokar, Arkodip Ganguly, Soumya Paul, "Design And Implementation of Network Security Using Neural Network", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 11 Issue 2, pp. 22-27, March-April 2024. Available at doi : https://doi.org/10.32628/IJSRST52411186

Journal URL : https://ijsrst.com/IJSRST52411186