ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 5, No.17 , September 2015
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

APPLIED CRYPTOGRAPHY IN PASSWORD ENCRYPTION USING NEURAL NETWORKS

Venkata Karthik Gullapalli[1], Ishan Khanka[1] and Rishi Verma[1]

[1] School of Computing Science and Engineering, VIT University,
Vellore, Tamil Nadu, India
gvkarthik93@gmail.com

Abstract

Today the world depends on computers and information systems for processing information in various fields. These systems must be developed in such a way that they are less vulnerable to attacks and more reliable and secured. These systems are more vulnerable to technical issues and many cases of data trawling have been reported as a result of password breaches. Encryption and decryption plays a major role in the modern era as the rate of data flow increased tremendously. Social networking sites such as Facebook and Google stores the most important and private data of people electronically in the servers. Artificial intelligence took over many functions of computer systems in different fields including data security. Neural networks process information with care and certainty like human mind does. This paper proposes a methodology to implement encryption and decryption using the feed forward neural networks and to improve the security of information systems.

Keywords: *Cryptography, Neural Networks, Security, Data Structures, Binary Trees*

1. Introduction

Internet is the biggest platform to perform various operations by individuals, organizations and government sectors and most of these operations must be classified and protected against security breach. In today's world it is not just enough to protect the data that is stored in the servers but it is really important to protect the data from thefts by also providing security systems towards the client side of the system. All the data stored in these servers should be secured so that they cannot be breached. Cryptography is one such security measure that is used to protect the data. Many cases have been reported on data loss and majority of these cases claim that the passwords of the users were breached and compromised. Security has to be made a priority to prevent such data loss. Password breach has been pointed out as the top cause for the loss of data and also the misappropriate use of the data. A basic example shows that people go to internet cafes and checks the mails, Facebook and uses the computers in the internet cafes for various purposes. The password used to login in to the systems have been noted down and the accounts were hacked and used for different purposes. Doctors in hospitals login into their accounts and go for inspections. With the emergency cases coming up, it is highly unlikely that doctors spend time to logout of these systems. Very crucial data such as the medical history and the healthcare analysis reports of patients can be accessed through these systems. The only smart thing to do is keep changing the passwords to all the accounts related to social networking, emails and many more at regular intervals of time. This annoys users as they have to change their passwords each and every time they login into any other system which is not owned by them. Computers created a platform for committing cybercrimes and also became the targets for committing frauds. Abuse of information and potential frauds are the biggest challenges faced by the technology world. Identity theft is the most common problem due to access towards the private information of people through password breach. Transactions worth billions of dollars are carried out every day all over the world and these transactions are based on password protection as an integral part of this system. If a server is breached then the damage caused by the classified data will be catastrophic. The application of neural networks depends on the applications it is designed for. Neural networks can be used to build efficient encryption systems. Although biometric systems such as fingerprint or facial recognition systems are more popular methods to protect the systems from vulnerable attacks, they are considered to be next generation security systems. Most people are still afraid to buy things online because they are afraid of internet frauds and interceptions in transactions. Cryptosystems are helpful for maintaining the integrity, confidentiality, and authenticity of all the information resources. A proper encryption and decryption system has to be implemented to stop the password breaches and protect the data. One such method is discussed in this paper using the concepts of neural networks and data structures.

1.1 Neural Networks

Neural networks are designed to create programs that mimic brain. Neural network is a processing device that takes the input and process it based on the function and application it is designed for and produces the output with precision and uncertainty. Neural networks are very flexible and learn by example from the precious data inputs. They are information processing systems that are designed to perform tasks in the same way the human brain works. Neural networks contain different layers and interconnected processing elements which acts as nodes to solve a problem logically. Neural networks process information faster than the human brain and this gave them an important role in the field of artificial intelligence. The output of one node in a layer is connected as an input to the other node in different layer. Each node can be programmed to perform different operations. Activation functions are used to activate the nodes when a certain input is given to the node. Neural networks follow parallel architecture by interconnecting nodes of one layer to the other. Neuron is a processing and computational unit that takes the input and processes it and sends the output to the other node and the procedure repeats until all the nodes in the network are processed and the final output is received. The connection between the nodes in the neural networks is associated with weights. These weights may differ for different connections. For higher computational processes, multilayer neural networks are used with nonlinear activation functions. Learning rate is used to control the amount of weight that needs to be added from one corresponding layer to the other layer. Neural networks handle noisy and unambiguous data to provide tractable solution. Artificial neural networks store information in contiguous blocks of memory. The proposed method uses feed forward neural network and the architecture of the feed forward neural network is given as figure 1. In figure 1, W_{ij} represents the weights connecting the input layer and hidden layer neurons. It gives the strength of the connection between the neurons. The weights can be positive or negative. Positive weights represents that the connection between the layers is excitatory and negative weights represents that the connection between the layers is inhibitory. The cycle time for execution and processing in neural networks is fee Nano seconds which makes the neural network architecture highly suitable for encryption and decryption. Neural networks can also perform several parallel functions simultaneously with encryption and decryption such as alerting the user and the system at the same time which also reduces the processing time and execution time. This adds value for the proposed encryption and decryption architecture. The size and complexity of the neural network depends upon the number of characters in the password and the length of the message strings that are being transmitted from source to destination. Depending on these lengths, the number of nodes vary in the neural network. The proposed neural network encryption and decryption architecture is coded for three nodes which can take passwords up to three characters and transmit messages with strings of length three characters. The size and number of nodes in the neural network can be varied and the same neural network architecture can be implemented for more than three characters and the implementation can be done using the proposed algorithm given in the below sections.

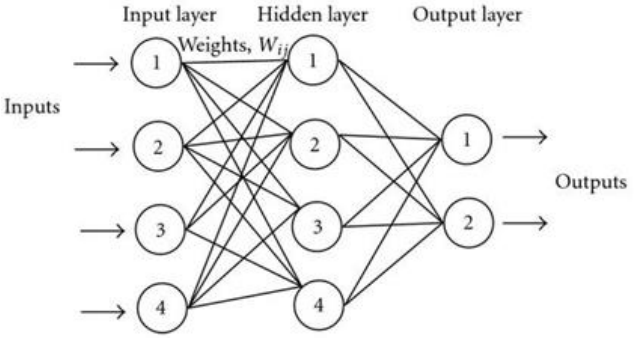

Fig 1. Feed Forward Neural Network Architecture

The characters in a password in the neural network are added in the contiguous blocks of memory. The information and messages get corrupted if the interconnections between the node layers get disconnected during the process.

1.2 Binary Trees

Different graph algorithms are used by tech giants such as Facebook and Google. Tree is also a kind of graph with nodes. A normal tree can contain any number of nodes that are connected in no specific format. A binary tree is a hierarchal data structure and it is a common tree that is used for various practical applications and computational processes. Binary trees are a type of data structures that contain nodes with information attached to these nodes. The information can be processed in any way such that the nodes in the tree can be traversed from top to bottom or from left to right or right to left or bottom to top or any other possible ways. The nodes in the binary tree can be navigated in many different ways. One such possible way is taken and an encryption and decryption algorithm is proposed using the nodes of these binary trees and neural networks. Some restrictions are imposed over these nodes and the information these nodes contain for a secure transmission of data from the source to the destination. A binary tree is a tree where every node has at most degree as

2 and levels are labelled along with the name of the nodes such as leaf nodes and child nodes. Elements can be inserted in the nodes of a binary tree and they can be traversed from one node to another node. Binary search trees are used for searching elements in binary tree through traversing in different possible ways possible. The root node is distinguished from every other node in a binary tree and all the nodes can be reached from the root node by traversing from the root node. Tree is a restricted form of graph and it does not contain cycles and it comes under the category of acyclic graphs in graph theory and applications.

1.3 Encryption and Decryption

Cryptography is a study of sending and receiving encrypted messages from the source and the destination. Companies are using various encryption techniques for protecting the data during transactions and accessing mails. The interleaving of chaos and cryptography has been the aim of a large set of works since the beginning of the nineties [1]. Chaotic system has several significant features, such as sensitive dependence on initial conditions and pseudo-randomness [2]. Encryption offers protection by keeping the content hidden from the view of unauthorized users and restricts the access only to certain authorized users. The analysis on how the systems can be breached and how the systems can be secured using encryption and decryption programs is cryptanalysis. A good encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough to make brute force attacks infeasible [3]. The message that is encrypted at the source is called as cipher text. The cipher text is decrypted to the original message at the destination. The process of encoding a message into a different format so that the meaning of this input string is not obvious is encryption and the process of decoding it is decryption which gives the original message.

Cryptography is basically a process and it contains a lot of individual parts like plaintext that is the original intelligible message and then there is cipher text, which is the transformed message. The list continues with parts like cipher which requires an algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods, and then we have keys that are the critical and crucial information used by the cipher, known only to the sender and receiver. A piece of confidential information is retrievable if and only if a right user share is available [4]. Cryptographic systems are generally categorized in three independent dimensions. The type of process used for transforming plain text to cipher text, all the encryption algorithms are based on two basic laws which are substitution in which each element in the plaintext is mapped into another element and transposition in which elements in the plaintext are rearranged. The number of keys used, this can vary from system to system and If the sender and receiver uses same key then it is said to be symmetric key encryption, which is also known as single key or conventional key. And if the sender and receiver use different keys then it is said to be public key encryption. The processes involved in processing of plain text are the block cipher processes where the input block of elements are processed at a time, producing output block for each input block and a stream cipher processes where the input elements are sent continuously, producing output element one by one as it goes on. The reliability, performance, continuous operation, safety, maintenance and protection of critical infrastructures are national priorities for countries around the world [5].

Public key encryption is considered to be a better and safe encryption technique than the private key encryption technique. In public key encryption technique, one public key and one private key are used which are created through mathematical analysis. The longer the key, the safer the data is and it is hard to decipher the message. This system uses the concept of encapsulation such that the key that is wrapped along with the algorithm is not accessible to the outside world. Companies have been collecting data for decades, building massive data warehouses in which to store it and even though this data is available, very few companies have been able to realize the actual value stored in it [6]. These encryption systems assimilate secure authentication and message integrity and also ensure that the data is protected from any kind of interception. The process of encryption of data differentiates the various process of cryptography, in this way one rely upon the key features of the process whether they need speed in their system or they can compromise on speed but want a high level of encryption. Depending upon the encryption, the decryption will also take relative amount of time, and the longer the system is running in this process, the threats of breaching the system increases. Cryptography is closely related to cryptanalysis. Cryptanalysis is often referred only to the mathematical procedures and computer programs. However, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders. Cryptosystem have features and objectives like confidentiality, integrity, non-repudiation and authentication. Sometimes cryptanalysis is also known as science of attacking the cryptosystem that contains encrypted data and raw data. In a different point of view it is basically an algorithm to crack the key. The massive use of the communication networks for various purposes in the past few years has posed new serious security threats and increased the potential damage that violations may cause [7]. The cryptanalysis attacks are of two types. One is active attack where the attacker sends or alters the message pretending to be an authenticated person by defeating the cryptography authentication and cipher and the second type of attacks are passive attacks where

the attacker often tries to read the messaged being transmitted without proper authorization by defeating the cipher without the key. Cryptography enables the two parties to communicate over an insecure channel so that an attacker cannot understand and decrypt the original message [8].

2. Proposed Encryption and Decryption Model

2.1 Proposed Method

With the increase in the usage and portability of devices such as mobiles and tablets, the need for increasing the security of the accounts over these devices plays a crucial role. In a world of high uncertainty and imprecision the decisions should be taken which provide results in an efficient way [9]. The need for the strong encryption and decryption program increases with the large amounts of data that is being uploaded and transferred every second. Internet has become a platform for the flow of data from the source to the destination rapidly. Password theft is an easiest way to gain access to a system and manipulate the data that is important. Different software programs are used to crack the passwords for a system or server. Users are requested to use different combinations of letters, numbers, symbols and many other characters to create a safe password. This imposes many rules on the users and reducing the computer-user interaction and friendliness. Safeguarding the passwords from the social vulnerabilities is the high priority and a responsibility that has to be taken by a company in order to provide secured access of data to its clients. The concepts of neural networks are well suited for the real time applications because of fast response and computational time [10].

An effective way of limiting the access is by establishing a powerful encryption and decryption algorithm that is developed with the concepts of neural networks. Neural networks with their remarkable ability to derive meaning from complicated or imprecise data can be used to extract patterns and detect trends that are too complex to be noticed by either humans or other computer techniques [11] [12] [13]. In this encryption and decryption algorithm, binary trees are used to store the encrypted data along with the key. The input string from the user at the source has to be encrypted and the encrypted cipher text has to be passed to the destination. Each character in the input string is converted into its corresponding ASCII value. The converted values are passed into an array in order. The array is converted into a square matrix and the order of the matrix is based on the number of elements in the array and this square matrix can be called as the data matrix as it contains the ASCII values of the input string. The overlap between an attacker and one of the parties at the synchronization time is reduced by the permutation among the weights, and the system is more robust with respect to advanced attacks [14]. The key is generated in the form of a diagonal matrix where the order of the key matrix is the order of the square matrix generated by the input string. The data matrix is then multiplied with the key matrix and the resulting square matrix values are stored. The binary tree is created at this stage and all the values of the resulting square matrix are inserted into the nodes of the binary tree in an order. The resultant matrix values are placed in the nodes with the odd values in the binary tree. These values are inserted in the nodes in the odd positions at each level of the tree. The nodes in the even positions in the tree are filled with the garbage values. The tree is parsed from top to bottom while parsing from left to right simultaneously after all the values in the resultant matrix are placed in the nodes of the tree. The data after parsing is put in the order back in a new array with the odd positions filled with the resultant values and even positions filled with the garbage values. There are different types of neural networks such as single layer neural network, multilayer neural network etc. In this paper, a feed forward multilayer neural network is used. Simple models of neural networks describe a wide variety of phenomena in neurobiology and information theory [14] [15] [16] [17]. The multilayer topology performs various functions. Two functions are implemented in this paper for experimental analysis and the two functions are to find if there is any mismatch in the input and the other function is to alert the system if there is any mismatch. When a user usually enters his password for entering his account like Facebook or Google, the password is sent over to the server for validation. The server receives the password verifies the password and then provides the access to the account. Facebook uses graph algorithms for encryption and decryption. The proposed method used binary trees along with the neural networks for this purpose and for providing a strong and unbreakable encryption. In the proposed method, when the user enters the string which is a password in general, the string of characters is converted to an array as explained above in the order. The resultant array that is formed from the process acts as an input to the neural network. Each character in the newly formed array is given as an input to each node of the neural network. The neural network then performs its operation and the final output of the neural network is the encrypted cipher. When a password is entered by the user, it is encrypted by the algorithm and the cipher is sent to the server. Now the nodes in the neural network can be programmed to perform different actions. The weights in the neural network can act as the second structure of key for further encryption. The function of the neural network varies for different applications. In the proposed method we took some basic functions like using logic gates and alert functions. The alert function is used in the neural network to alert the system if there is any kind of breach. Each node in the neural network receives a character of encrypted cipher and each node is programmed to do certain functions. One such function implemented in the proposed method is to alert system.

When there is a mismatch at any node in the neural network, that node is programmed to alert the system. So if there is any kind of interception while the message is being transmitted, the system alerts the user and the server and blocks the access till the system is cleared. The node is programmed to receive a specific character of encrypted cipher and when it receives a different character than the character it should actually receive as input, the process is aborted. As a result of this the server receives only bits of characters but not an entire set of string. When the server happened to receive only part of the password, it alerts the system while decrypting the received string as it mismatches at certain nodes. The user is sent an alert message by the node which received a different character than the real character it is supposed to receive. Neural networks can be used in this way for providing the stronger encryption and decryption technique. The architecture of the proposed method is shown in figure 2. The neural networks in this architecture store the encrypted message in contiguous blocks of memory. The development of artificial neural networks comes from simulating intelligent tasks which are performed by human brain and they are most widely used by the soft computing techniques that have the capability to capture and model complex input/output relationships of any system [18].

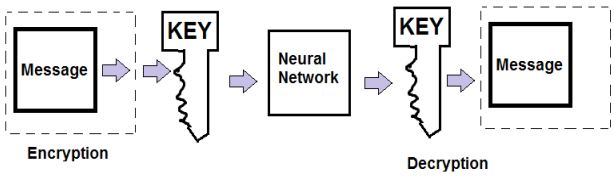

Fig 2. Architecture of Proposed Model

Cryptography is the exchange of information among the users without leakage or loses of information to others [19]. An Artificial Neural Network (ANN) is an information processing paradigm that is inspired by the way biological nervous systems, such as the brain, process information [20]. The primary task for implementing the proposed encryption and decryption model is to construct the model and then coding the constructed model. While constructing the model, first the flow diagram is constructed based on the minimum requirements as shown in figure 3. When the user enters a password and message, they are encrypted using the proposed model above. After encryption, the encrypted ciphers of password and messages are transmitted to the server. The decryption program near the server will decrypt the ciphers received and then passes it to the server. In the proposed model, Apache server is used for password verification and the model is coded in the server using PHP script. The password authentication system is a pattern classification system based on artificial neural network [21].

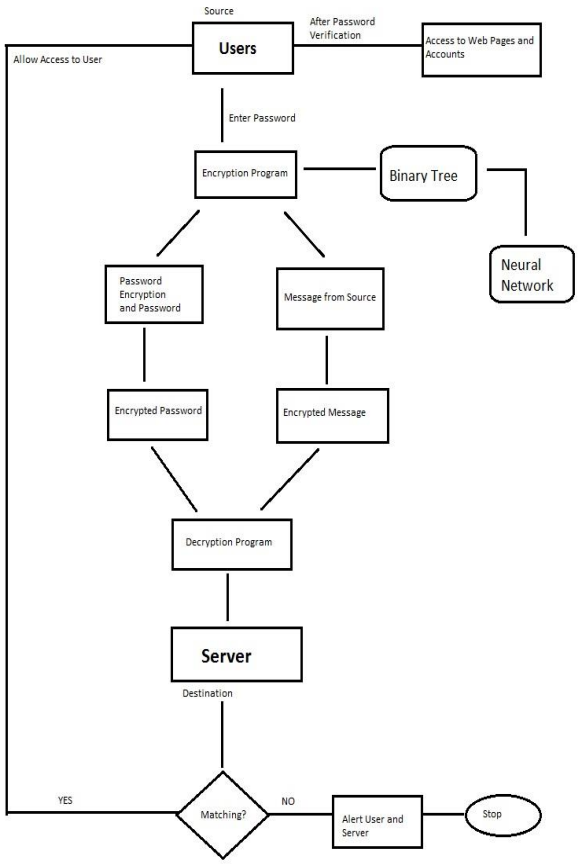

Fig 3. Flow Diagram of Proposed Model

2.2 Algorithm

The algorithm for the proposed encryption and decryption architecture in figure 2 can be used for various applications. The algorithm is given below.

1. Take an input string from user as the password and convert the given string into respective ASCII values.
2. Convert the given array of ASCII values into a matrix.
3. Construct a key matrix of the same order as the order of the matrix containing the ASCII values.
4. Multiply the key matrix with the matrix containing ASCII values and insert the resultant values in the binary tree as proposed.
5. Parse the values in the tree and construct a new matrix with the parsed values from the tree.
6. Input the values from the new array as an input to the feed forward neural network.
7. Perform the respective operations as proposed in the neural network and provide the results if the encryption is properly performed without any breach.

8. Provide the access to the user if there is no breach in the system.
9. If there is a breach in the network then alert the user and the server about the breach and block the access immediately until a response is received from either the user or the server.
10. After the access of account and the data end the encryption between the user system and the server.

2.3 Implementation

One of the requirements of the secured application is making information always accessible to users who need it and who have sufficient permissions to access it [22]. The many disadvantages of single static passwords include how easy they are to decipher [23]. The proposed method is implemented on the dataset containing over 20 messages and the corresponding ciphers for the messages that are resulted as the outputs are shown in table 1. When the server receives the ciphers it gives back the cipher to the decryption algorithm to get the real message user wanted to convey. The proposed method is implemented for three nodes using binary tree and the corresponding input and output of the implementation is shown in figure 4. The experimental analysis has shown some brilliant results when the proposed method is implemented for different types of messages and all the encrypted ciphers are properly transmitted over a network without any interception. In the implementation, first the user is asked to choose among the provided three options which are encrypt, decrypt and exit. When the user chooses the first option encrypt, the user is supposed to enter the password to be encrypted. The binary tree and neural network then processes the password and gives the output. The resulted output is the encrypted cipher. Then the server can choose the second option decrypt when it receives the encrypted cipher from the user. Then the decryption algorithm is run and the corresponding password is matched with the password stored in the server. When both the password entered by the user and the password stored in the database are matched, then the user is given access to the account. The complete neural network architecture is coded, both for encryption and decryption and the results are displayed in the table 1 with the screenshot of the implementation in figure 4. The program is executed and tested for more than 40 passwords and gave no errors. The results for 20 such password encryptions is given in table 1. Table 1 gives the three character passwords and their respective ciphers after encryption at the user end. These ciphers in the form of packets are transmitted through neural network to the server. The algorithm can also be coded in the scripting languages to provide the access to the web applications.

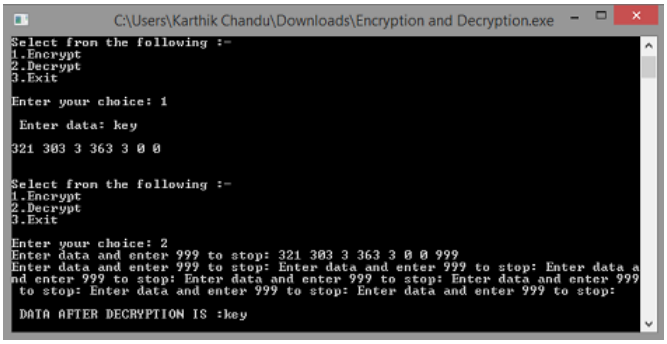

Fig 4. Implementation of Proposed Model

Table 1. Message and Corresponding Encryption Ciphers

Serial Number	Message	Cipher
1	KEY	321 303 3 363 3 0 0
2	RAM	342 291 3 327 3 0 0
3	BIT	294 315 3 348 3 0 0
4	BUS	294 351 3 345 3 0 0
5	GIF	309 315 3 306 3 0 0
6	FTP	306 348 3 336 3 0 0
7	LAN	324 291 3 330 3 0 0
8	LOG	324 333 3 309 3 0 0
9	MAQ	327 291 3 297 3 0 0
10	NET	330 303 3 348 3 0 0
11	ROM	342 333 3 327 3 0 0
12	SQL	345 339 3 324 3 0 0
13	WEB	357 303 3 294 3 0 0
14	WAN	357 291 3 330 3 0 0
15	ISP	315 345 3 336 3 0 0
16	HEX	312 303 3 360 3 0 0
17	BUG	294 351 3 309 3 0 0
18	ALT	291 324 3 348 3 0 0
19	CAD	297 291 3 300 3 0 0
20	DTP	300 8 3 336 3 0 0

3. Experimental Analysis and Comparison

Many password management apps offered on the market do not provide adequate level of security [24]. The experimental analysis shows that the messages and passwords can be encrypted and decrypted using the proposed method. As a comparison with the existing methods, the neural network encryption is built on C libraries with various optimization levels. The encrypted cipher is received by the program at the apache server at the server side and is decrypted for verification. When there is a breach in the path while transmitting the password and message, the system is alerting both the user and the server. Feed forward neural networks showed

better results than back propagation neural networks. Back propagation neural networks take more run time and execution time than the feed forward neural networks. Any system that takes more execution time or run time gives time for hacker to breach the encrypted server and thus the system also takes time to alert the user and the server. Encryption and decryption should be a faster process for transmission of data without breach. Considering all these factors and results, feed forward neural network is a better architecture to use in encryption and decryption than back propagation neural networks. The messages are transferred precisely from unit to unit. In order to avoid problems expressing security in the presence of non-determinism, messages are scheduled probabilistically instead of non-deterministically [25]. The proposed method also possess simpler interconnections and simpler architecture with a strong encryption and decryption that cannot be breached. The learning methodologies can be adopted by the neural networks for updating and adjusting the weights between the connections every time which makes it a difficult task for hackers to know the key weight values and ensures security and stability of the password that is being transmitted between the user and the server. The applications of binary trees are primarily confined to computational techniques such as data storage and file compression. This method uses binary tree for encryption and decryption and shows the most stable way of securing the data during transmissions through encryption and decryption techniques. One concern using binary trees is that trees are not recursive data structures which make it a difficult task to code the algorithm. Normal encryption techniques show the dynamic behaviors which has high memory consumption when compared to the proposed method. In the experimental analysis, the length of the password that has to be encrypted is considered to be of n characters. The evaluation of performance for inserting the characters of the password into the binary search tree and neural network is done and the results are shown below in table 2. The corresponding graph of the time complexity for the proposed method is shown in figure 5.

Table 2. Time Complexities

Operation	Average Case
Insert Character	O(logn)
Delete Character	O(logn)
Accessing Characters	O(logn)

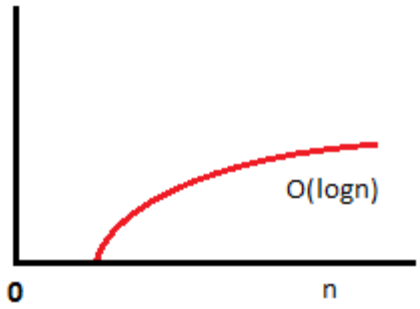

Fig 5. Time Complexity Graph

The proposed method is implementing using C++ programming language. The sourced code for the complete algorithm is simulated using Code-Blocks. Code-Blocks is a compiler that is used for compiling and analyzing the results for the proposed method. The feed forward network will roughly require between 1.5 to 3 megabyte of memory in order to store the weights values [26]. Table 3 shows the memory consumed by the existing encryption method using neural networks and the proposed method. The results showed that the proposed method takes very less memory than the existing methods. Since each and every node of the neural network is programmed to alert the user if there is any breach, the proposed method is less prone to attacks.

Table 3. Consumed Memory

Existing Method	Proposed Method
1.93 MB	988KB

4. Conclusion

The application of artificial intelligence and neural networks in security has a wide scope of future and a lot of research can be conducted on the same. The point where the connection originates and terminates should be noted such that the password is sent in packets contributing each packet for each node in the neural network. Each packet from the source contains one character of the password. So the packets are sent in the specific order that the encryption and decryption algorithm is coded. Here in the proposed method, it uses the logical binary tree order to pass the packets as mentioned above. The encryption and decryption algorithm can be used in various fields of computer science. The threats and attacks are increasing every day and with the increasing threats, there is a need for a strong encryption and decryption. In this paper a method is proposed to use an encryption and decryption for signing into accounts with passwords. In real the same

method can be used for transmission of messages from sender to receiver and this method can also be used for many other applications. The neural networks can be used for various applications and in this method the neural network is programmed to transmit the password and is using the logic gates and alert system functions. The proposed method used multilayer feed forward neural network topology and a further research can be conducted on using different types of neural networks. The functions can be altered and programmed for various other purposes. In the experiment implemented, the results were efficient and astonishing and the system alerts both the user and the server when there is any kind of breach of passwords and data. The paper only presents the idea and implementation but does not give the crucial details of the implementation of neural networks so the proposed encryption and decryption algorithm can be used for the real time applications. This paper also provides the alert functions, verify functions that are implemented. The existing method can be further implemented with many more added functions using neural networks. Programming the neural network for encryption and decryption is a challenge to the future applications.

References

[1] Arroyo D, Diaz J, Rodriguez FB, "Cryptanalysis of a one round chaos-based Substitution Permutation Network," Signal Processing, 93, 1358 – 1364, 2013.

[2] Xing-Yuan W, Jian-Feng Z, "Cryptanalysis on a parallel keyed hash function based on chaotic neural network," Neurocomputing, 73, 3224 – 3228, 2010.

[3] Nooshin B, Yousef F, Karim A, "A novel image encryption/decryption scheme based on chaotic neural networks," Engineering Applications of Artificial Intelligence, 25, 753 – 765, 2012.

[4] Tai-Wen Y, Suchen C, "The semi-public encryption for visual cryptography using Q'tron neural networks," Journal of Network and Computer Applications, 30, 24 – 41, 2007.

[5] Christina A, Sherali Z, "Critical infrastructure protection requirements and challenges for the 21st century," Science Direct, 8, 53 – 66, 2015.

[6] Singh Y, Singh AC, "Neural Networks in Data Mining," Journal of Theoretical and Applied Information Technology, 2009.

[7] Khalil S. A Back, "Propagation Neural Network for Computer network Security," Journal of Computer Science, 9, 710 – 715, 2006.

[8] Agarwal N, Agarwal P, "Use of Artificial Neural Network in the field of Security," International Journal of Computer Science and Information Technology, 3, 42 – 44, 2013.

[9] Venkata Karthik Gullapalli, Rahul Brungi, "A Novel Methodology to Implement Optimization Algorithms in Machine Learning," International Journal of Computer Applications, Volume 112, No 4, 2015.

[10] Venkata Karthik Gullapalli, Rahul Brungi, Gopichand G, "Application of Perceptron Networks in Recommending Medical Diagnosis," International Journal of Computer Applications, Volume 113, No 4, 2015.

[11] R M Jogdand, Sahana S Bisalapur, "Design of an Efficient Neural Key Generation," International Journal of Artificial Intelligence & Applications, Volume 2, No 1, 2011.

[12] Eric S Imsand, Deon Garrett, John A. Hamilton, "IEEE: User Identification Using GUI Manipulation Patterns and Artificial Neural Networks."

[13] Henry A. Rowley, Shumeet Baluja, and Takeo Kanade, "Neural Network-Based Face Detection," 1998.

[14] I. Kanter, W. Kinzel, "The Theory of Neural Networks and Cryptography," 2013.

[15] J. Hertz, A. Krogh, and R. G. Palmer, "Introduction to the Theory of Neural Computation," Addison Wesley, Redwood City, 1991.

[16] A. Engel, and C. Van den Broeck, "Statistical Mechanics of Learning," Cambridge University Press, 2001.

[17] M. Opper and W. Kinzel, "Statistical Mechanics of Generalization," Models of Neural Networks III, ed. by E. Domany and J.L. van Hemmen and K. Schulten, 151–20, Springer Verlag, 1995.

[18] lker Dalkiran, Kenan Danisman, "Artificial Neural Network Based Chaotic Generator for Cryptology", Turk J Elec Eng & Comp Sci, Vol 18, No 2, 2010.

[19] Minal Chauhan, Rashmin Prajapati, "Image Encryption Using Chaotic Cryptosystems and Artificial Neural Network Cryptosystems: A Review", International Journal of Scientific & Engineering Research, Volume 5, Issue 5, 2014.

[20] Eva Volna, Martin Kotyrba, Vaclav Kocian, Michal Janosek, "Cryptography Based on Neural Network", 26th European Conference on Modelling and Simulation, 2012.

[21] Ashwini Galande, Dattatraya Londhe, Mangesh Balpaande, "Security in Voip Network Using Neural Network and Encryption Techniques", International Conference on Information and Network Technology, Volume 4, Singapore, 2011.

[22] Syed S. Rizvi, Aasia Riasat, Khaled M. Elleithy, "Combining Private and Public Key Encryption Techniques for Providing Extreme Secure Environment for an Academic Institution Application", International Journal of Network Security & Its Applications, Volume 2, No 1, 2010.

[23] E. Kalaikavitha, Juliana Gnanaselvi, "Secure Login Using Encrypted One Time Password (OTP) and Mobile Based Login Methodology", International Journal of Engineering and Science, Volume 2, Issue 10, 2013.

[24] Andrey Belenko, Dmitri Sklyarov, "Secure Password Managers and Military Grade Encryption on Smartphones", Elcosoft Co. Ltd.

[25] J. Mitchell, A. Ramanathan, A. Scedrov, and V. Teague, "A probabilistic polynomial-time calculus for analysis of cryptographic protocols", Electronic Notes in Theoretical Computer Science, 45, 2001.

[26] V. R. Kulkarni, Shaheen Mujawar and Sulabha Apte, "Hash Gunction Implementation Using Neural Networks", International Journal on Soft Computing, Volume 1, No 1, November, 2010.