

International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 5, May 2016, pg.563 – 566

User Authentication Mechanism Based on Neural Networks

Menal Dahiya

Department of Computer Science, Maharaja Surajmal Institute, New Delhi

menaldahiya@gmail.com

Abstract: *In today's wireless communication system, building security between the two parties within the network is the most challenging concept. Many forms of encryption and decryption algorithms are available but they need different public private keys which are hard to remove and need more processing power. Password-based authentication mechanism is used broadly to identify authorize users, because this method is cheap, easy and quite accurate. This paper suggests that Neural Networks will provide solution to this problem. A neural network is trained to store the passwords instead of using verification table. Here, in this paper the keys which are used to secure the network are stored in the form of network parameter and other neuronal functions which are difficult to break.*

Keywords: *Authentication, Decryption, Encryption, Neural Network, Wireless Communication*

1. INTRODUCTION

Authentication is a process of establish identity between two devices or two parties. Old methods of authentication are based on physical characteristics of human being. Sometimes such methods are not sufficient then authentication protocols are capable of authenticating connecting party and authenticating itself to connecting party [1]. Password is the most famous authentication form used by the users. Security has become one of the most concerned issues in today's technological world. Commonly used password authentication method is the traditional approach based on passwords, PIN, smart cards and biometric devices etc [2]. While it is a very convenient and inexpensive procedure of authentication but it has some drawbacks also. Since in traditional method password table is stored in plain text format and can be easily seen by network administrator [3-4]. So, password table should be kept secured.

User can overcome from these type of problems by encrypting the (user Id, password) pairs before storing them in memory and then decrypting them. Reyhani & Mahadavi[5] have proposed neural networks in smart home networks for user authentication. This proposed method can be used to store the user profiles and access controls in smart home networks. They used a Radial Basis Function (RBF) neural network trained it to store encrypted passwords and it could be used to replace the password table stored in the authentication system. Wang and Wang [6] used Hopfield Neural Network for password authentication. In such password based authentication approach, system uses the verification table in which encrypted passwords are stored [6-7]. Passwords may be encrypted by one-way hash functions or any other encryption algorithms. Another way to swamped with the security problem is to use an Artificial Neural Network (ANN) which learns the (User Id, password) pair and generates the matching signal representing the user registration [8-9]. Artificial Neural

Networks is computational model that mimic the biological neural networks in the brain. This can be achieved by training ANN. Here, in this paper we apply Back Propagation Algorithm in the training phase. This approach is advantageous as it does not require the matching (User Id, password) to be stored on the external storage but requires network parameters to be stored. These network parameters are difficult to trace without knowing the exact internal organization of the network. Section 2, briefly describes Neural Network concept. In section 3, proposed methodology based on Back Propagation Algorithm will discussed. Then section 4, carried out the result of the proposed algorithm and finally section 5 will conclude this paper.

2. NEURAL NETWORK

A Neural Network is consist of set of parallel and distributed processing units called neurons. These neurons are connected by unidirectional or bidirectional links in an ordered fashion i.e.in layers. Three kinds of layers are present in Neural Network architecture, input layer consists of n number of inputs to the network and each input is multiply by a weight associated with this input. The product of input and weight are summed and feed into a network through a transfer function to generate the output. Artificial Neural Network has some attractive features that make it popular such as learning ability and one way property:

Learning ability: ANN has the possibility to gain knowledge through learning and one way property is the second most important feature of ANN. This property is used to authenticate data's integrity. Output can be easily generated from the given input although it is impossible to compute input from output.

Neural Network designing is based upon network topology, network transfer functions and network learning algorithms [9].

a) *Network Topology*

It is the most important criteria in building a successful network model. Deciding the training parameters of the neural network is not a easy task, e.g. number of hidden layers, number of neurons in each hidden layer, types of activation function, concept of over fitting and under fitting, interconnection within the layer. Two important neural network topologies are Feed Forward topology and Recurrent topology. In feed forward topology, the nodes are arranged in layers through unidirectional paths. The output flows in forward direction and does not allow feedback flow of information. In recurrent topology, the flow of information between the nodes is bidirectional.

b) *Network Transfer Function*

The transfer functions and activation functions play an important role in learning algorithms and influence the complexity and performance of neural network. There are various transfer functions such as linear, sigmoid, polynomial etc.

c) *Network Learning Algorithm*

There are three types of network learning algorithms: supervised, unsupervised and Reinforcement. In supervised learning the output is known priori and output result is compared with desired result. The gradient descent rule uses the error to adjust the weights between the actual output and target data. In unsupervised learning, there is no external source to provide the network, a set of training data is presented to the system and then the weights are adjusted through some sort of competition among the node of output layer [11]. In the third type of learning the network connections are modified according feedback information provided to the network by its environment.

3. METHODOLOGY

Neural Networks are used as an encryption and decryption in cryptography [12]. Topology of each neural network is based on their training sets. Generally encryption method is done on the input data and the decryption method is done on the output string of digits. If we use neural network for the network security means for encryption and decryption, their keys have adapted neural network parameters: their architecture and their configurations [12].

The proposed authentication scheme includes login and authentication procedures. The user chooses the user Id (ID) and password (PW). The user Id and password are converted into n-bit binary numbers. These binary numbers are used to train the neural network. The neural network repeats the process again and again (iterations) until the network can remember the entire user Id and its corresponding password pairs. This password authentication scheme is based on Back Propagation Neural Network and it describes the verification of user Ids and passwords. The proposed model has N nodes and the output of each node is fed back to all the other nodes through symmetric weights. The threshold for present implementation is set to 0. During training phase the BPNN verifies the matching between input and output pair. If the weighted input sum is larger than threshold value output is set to 1 otherwise to 0. Figure 1 depicts the user authentication procedure using Back Propagation Algorithm. The authentication system has good accuracy, as the generated outputs are same as of

desired outputs. When a user enters a wrong combination of username and password, the system rejects that entry and declares that as an unauthorized user.

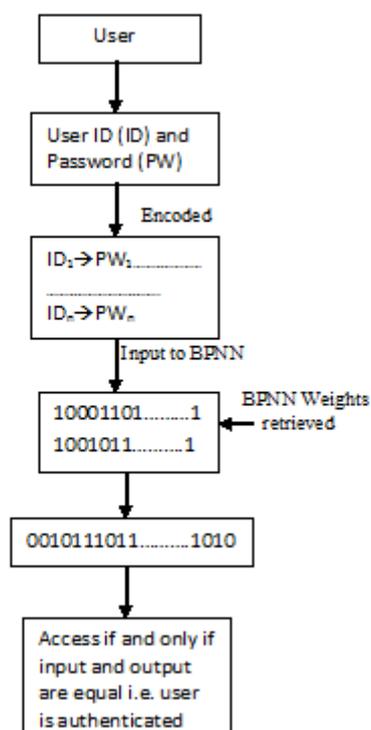


Fig 1. User Authentication using BPNN

4. RESULT

The studies are carried out on MATLAB simulation tool [13]. A PC with Intel-core i5 processor, 2.40GHz and 8GB RAM was used to conduct this simulation. The simulation is carried out for thirty users.

MATLAB Neural Network Toolbox was used for the implementation of the network. Using this tool one can define specifications like number of layers, number of neurons in each layer, activation functions of neurons in different layers, and number of training epochs. Then the training feature vectors and the corresponding desired outputs can be fed to the neural network to begin training. Error back-propagation algorithm was used for training.

The overall simulation results are summarized as follows.

- 1) The total time for the registration of 30 users was about 0.0005sec.
- 2) The trained BPNN was able to recall each legal user's ID and password accurately and instantly.
- 3) The trained BPNN was able to reject each illegal user's ID and passwords correctly.

5. CONCLUSION

The present work describes the usefulness and robustness of Back Propagation neural network based password authentication scheme. The proposed authentication scheme included two major procedures: log-in and user authorization. The network could recall all the authenticate users accurately and rejecting the unauthorized users. The implementation can be worked out for more users.

REFERENCES

- [1] Bin Hu, Qi Xie, Yang Li- Automatic verification of password based authentication protocols using smart card (2011).
- [2] B. Menkus, "Understanding the Use of passwords", Computers & Security, vol.7, pp. 132-136, 1988.
- [3] W. Yang, Shieh, S., "Password Authentication Schemes with Smart Cards," Computers & Security, vol. 18, pp. 727-733, 1999.
- [4] R. Morris, Thompson, K., "Password Security: A Case history," Communications of the ACM, vol. 22, pp. 594-597, 1979.
- [5] Reyhani, S. & Mahadavi, M. "User Authentication Using Neural Network In Smart Home Networks". *International Journal of smart Home*, Vol. 1, No. 2, (2007), Pp.147-154.

- [6] Wang, S. & Wang, H. "Password Authentication Using Hopfield Neural Networks". *IEEE Transactions On Systems, Man, And Cybernetics, Part C: Applications And Reviews*, Vol. 38, Np. 2, (March 2008), Pp. 265-268
- [7] Shihab, K.; "A Backpropagation Neural Network For Computer Network Security", *Journal Of computer Science 2 (9) : 710-715, 2006, ISSN 1549-3636 © 2006 SCIENCE PUBLICATIONS*
- [8] Fadi N. Sibai, Aasha Shehhi, Sheikha Shehhi, Buthanina Shehhi And Najlaa Salami , "Designing And Training Feed-Forward Artificial Neural Networks For Secure Access Authorization" *Http://Www.Intechopen.Com, 2009*
- [9] R. J. Schalkoff, *Artificial Neural Networks*, McGraw-Hill, 1997.
- [10] Chien cheng Yu, and Bin Da Liu, "A backpropagation algorithm with adaptive learning rate and momentum coefficient," *IEEE, 2002*.
- [11] H. Shruti, K. Manjunath, K.S. Patil "A Survey: Research Summary On Neural Networks", *IJRET e-ISSN: 2319-1163, Vol.3 , May 2014*.
- [12] Michal Janosek, Eva Volna, Martin Kotyrba, Vaclav Kocian, "Cryptography based on Neural Network" *Proceedings 26th European Conference on Modeling and Simulation, Year 2012. www.scs-europe.net/conf/ecms*
- [13] Howard Demuth, Mark Beale, "Neural Network Toolbox, version 4", The MathWorks, Year 2012.