IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Issue-9 E-ISSN: 2347-2693

Password Authentication in Wireless Networking using Neural Network Techniques

Menal Dahiya

Maharaja Surajmal Institute, Janakpuri, Delhi, India

Available online at: www.ijcseonline.org

Received: 12/Aug/2016 Revised: 21/Aug/2016 Accepted: 10/Sept/2016 Published: 30/Sep/2016

Abstract— There are various mechanisms that provide security to the users and resources in Wireless Networking. Password authentication is one of the important procedure that enhance the security measures of the system. Drawbacks of traditional password authentication system like stolen, forgotten etc. are overcome by the technologies used for authentication mechanism like Neural Network approaches. In this paper, the two algorithms of Neural Network have been taken for conducting the experiment. Neural Network is an emerging field of Artificial Intelligence that works like a human brain. One is the Backpropagation algorithm which follows feed forward procedure and the second one is Hopfield Neural Network which works on auto associative properties of the network.

***Keywords*—Backpropagation algorithm; Hopfield Neural Network; Password authentication; Wireless Networking.**

I. INTRODUCTION

Earlier computer networks were only used by the university researchers, corporate employees for sending office information through e-mail or by sharing peripheral devices among the employees in the military and in government operations [1]. At that time no one realized the security of data because the use was limited and by limited persons in a given amount of time. So security did not get a lot of attention that time. But for the last few decades, the existence of computer network spread widely. Daily, millions of ordinary people use the network facilities for their convenience such as for banking, shopping, ticket booking, watching movies online, chatting, sending emails and for the use of social networking like facebook, twitter etc. They use each and every facility of internet without knowing the security aspects. Before the widespread use of the internet, the security of information or data for an organization was provided to the managers or other reliable post and administrative means. Gradually, with the advancement in computer the need for automated tools for protecting data and other information stored in the computer became an evident basically in sharing systems. The general name given by the researchers to a collection of tools that protect data from hackers is a computer security [2]. Security is a vast topic and it includes data security and network security. Security is concerned with making sure that unwanted people cannot access or modify message intended for other recipients and unauthorized people are not trying to access the services [3]. Network security is a concept to protect data transmission over a wired or wireless network. Therefore, it is necessary to use some cryptographic methods or some other means of protection to enhance the security. Network security considers authorization of access of data in a network. Every user assigns an Id and corresponding password that allows them to access information without any problem. This Id is the identity of its authorized usage.

Authentication is a two way process in which user confirms his or her identity to the computer system [4]. Authentication schemes are mostly based on passwords, smart cards and biometrics. Authentication ensures that the services and system resources are used by the authentic person. This paper follows the sequence of, section II describes the two different neural network approach used for the authentication of password in wireless technology. Hopfield Neural Network and Back Propagation Neural Network are the two algorithms which applied to the data to conduct the experiment. Section III describes the results and discussion followed by a conclusion.

II. PROPOSED AUTHENTICATION SCHEMES USING NEURAL NETWORKS

This section, describes the proposed procedure of user login and authentication steps by using two Artificial Neural Network Techniques:

A. Using Back Propagation Neural Network Scheme: - We propose the authentication mechanism that used Back Propagation Neural Network in wireless networking. As wireless networking requires much security measures compared to wired networking. Back Propagation Neural Network is a Feed Forward Neural Network uses supervised learning algorithm for training. The basic architecture of BPNN consists of an input layer, hidden layer and output layer. Each neuron of the input layer is connected to the hidden layer which further connected to the output layer. A sample dataset will be prepared by collecting authentic and non-authentic users. Then data are to be trained using BPNN and after that trained network will be used for authentication [5,6,7]. For accessing the resources, user first login to the system with password. If the login process completes successfully, then the user is allowed to access the system. There are three main components of the authentication process: user registration phase, user login and user authentication phase. Generally, at first time when authorized user login, the system stores his/her personal information and afterwards, while a user would like to access he/she only needs to login with the correct combination of Id and password stored previously.

In user registration phase different users choose their login id and passwords which are sent to the administrator. These login ids serve as a training set for the Back Propagation Neural Network. The input is the username and the corresponding password is the output. The Password is the combination of numbers and alphabets, so first we convert them into ASCII code and then into binary before training the BPNN. After the conversion hash function is applied to both on the user id and password. The administrator takes hashed username as the inputs and the corresponding hashed passwords as the expected output to train the BPNN [8]. When system trained successfully or completed the training phase, the system stores the network weights. In login phase, when a user wants to log into the system, the user has to input both user id and password, the client site automatically generates the encoded username and password. And finally the server receives the encoded combination. In user authentication phase, the stored trained hashed password is compared with the password provided by the user. If their matches, the login user is recognized as an authentic person otherwise rejected. Login and authentication phase of proposed algorithm is described in figure 1.

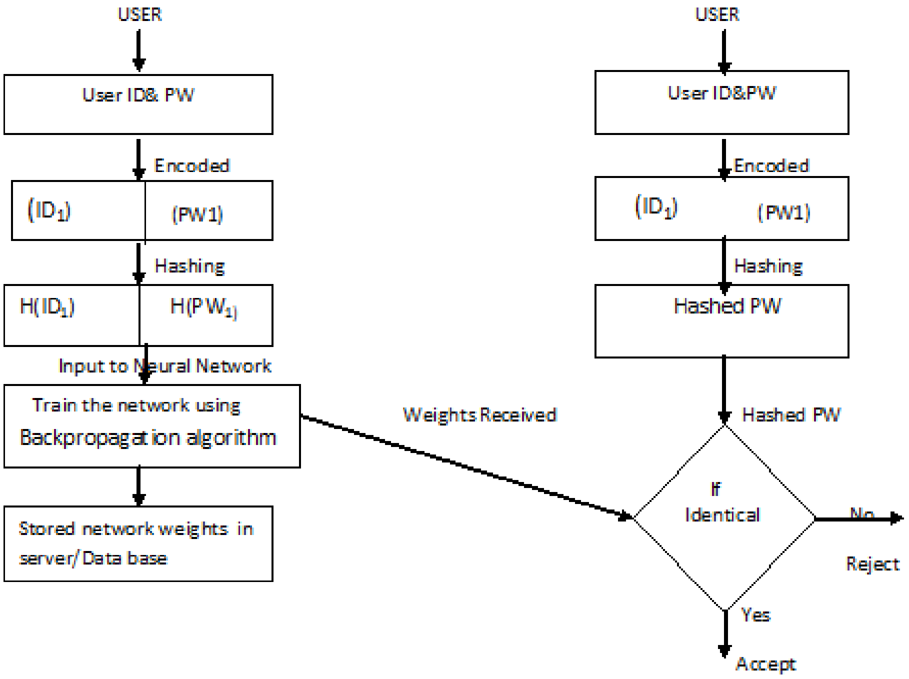

Figure 1. Login and Authentication Phase in Back Propagation Neural Network

B. Using Hopfield Neural Network Scheme: - Proposed mechanism of password authentication is based on a Hopfield neural network, which basically works upon recalling the stored pattern. Pattern recognition or recalling is the matching of giving input patterns with the already stored pattern. If the pattern matches with the already stored pattern, then pattern has been seen before or authenticate input. For improving the performance of HPNN, we must increase the information capacity and make the patterns sparsely encoded. If the patterns consist of a large number of nodes, it is easy for the network to recall the performance. The original patterns sparsely coded in accordance with the number of nodes in HPNN [9,10]. For e.g. 4-bit patterns (1 0 1 0) would be sparsely coded as 7-bit patterns such as (0 $\underline{1}$ 0 $\underline{0}$ $\underline{1}$ $\underline{0}$ 0), the underlined bits are used to increase the sparseness of the patterns. Maximum distance separable codes can be used to ensure the maximal sparseness of the resulting patterns.

The authentication scheme includes three major phases—registration, login, authorization. In HPNN it is not possible to train the network by giving input data and generate a corresponding output pair [11,12]. So we take password as input to the network and the corresponding weight matrix is stored in the memory of the network. HPNN authentication gives better result with bipolar inputs instead of binary inputs. So, first convert characters into ASCII code, then in binary and then into bipolar values. Value of 1 is +1 and 0 is -1 in bipolar and convert them by using following formula (2x-1), where x is a binary digit. After conversion these bipolar units are used as a training sample. After training when they trained successfully server store these networks. Whenever user access the service from server, server matches the username and password with the already stored weight matrix. If they both are identical, then the user is authentic otherwise the system rejects it. Most users image as a password in that case we have to convert images into text because the image is not directly used as an input in a neural network. Login and authentication procedure is explained diagrammatically in the figure 2.

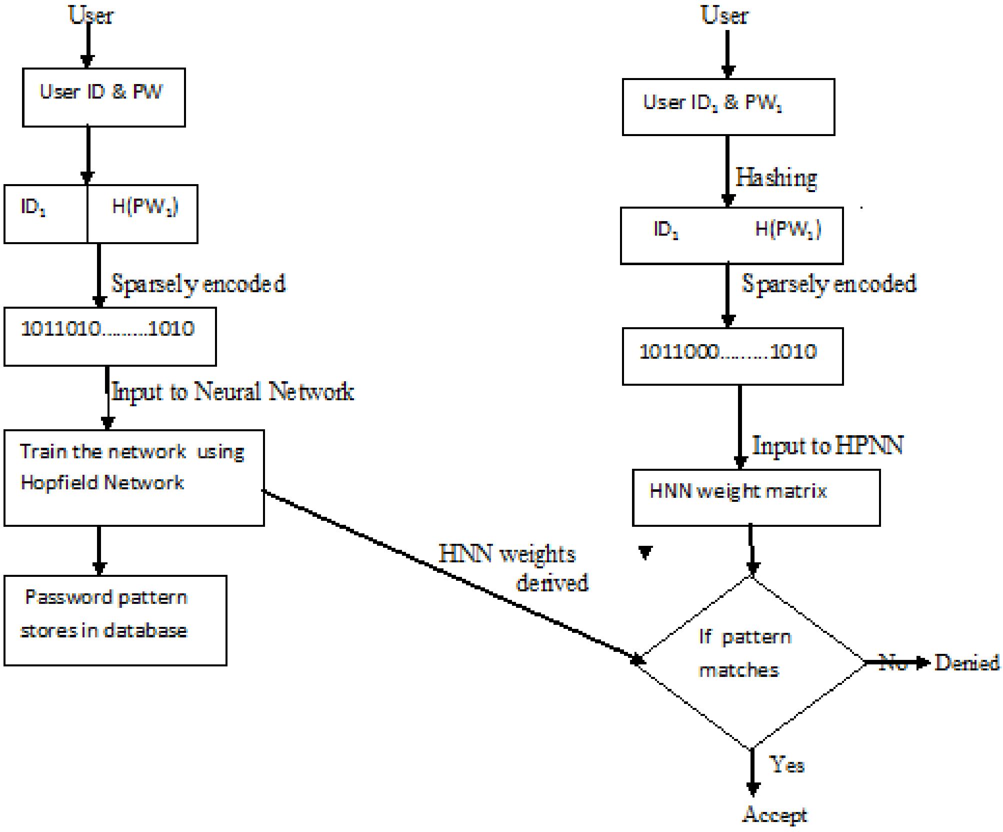

Figure 2. Login and Authentication Phase in Hopfield Neural Network

III. CONCLUSION

In traditional password based schemes, the server maintains a verification table for storing passwords which is not a fully secure mechanism. Using Neural Network techniques such as Back Propagation and Hopfield, server only stores the network parameters of the classification network. Both algorithms use different procedure for storing the password. Hopfield is an auto associative type of network, which recall the patterns correctly and can be effectively used in an environment. On the other hand, Back Propagation is a widely used Feed Forward Network.

REFERENCES

[1] 802.11a: A Very-High-Speed, Highly Scalable Wireless LAN Standard, White Paper, www.proxim.com, 2002.

[2] L. Sachin, "Security in MANET: Vulnerabilities, Attacks and Solutions", International Journal of Multidisciplinary and current research, Volume.02, Page No (62-68), Jan-Feb 2014.

[3] Shivlal Mewada, Aarti Shrivastava, Pradeep Sharma, N Purohit and S.S. Gautam" Performance Analysis of Encryption Algorithm in Cloud Computing", International Journal of Computer Sciences and Engineering, Volume-03, Issue-03, pp (83-89), Jun -2014

[4] K. Sumedha, S. Ankur, "Network Security using Cryptographic Techniques", International Journal of Advanced Research in Computer Science and Software

Engineering, Volume.02, Issue-12, Page No (105-107), December 2012.

[5] C. Zhen-Guo, C. Tzu-an, C. Zhen-Hua, “Feed Forward Neural Networks Training: a Comparison Between Genetic Algorithm and Back-Propagation Learning Algorithm”, International Journal of Innovative Computing , Information and Control, Volume.07, Isuue-10, Page No (5839-5850), October 2011.

[6] Neha Shukla, Meena Arora, "Prediction of Diabetes Using Neural Network & Random Forest Tree", International Journal of Computer Sciences and Engineering, Volume-04, Issue-07, Page No (101-104), Jul -2016

[7] I. Mukhopadhyay, M. Chakraborty, S. Chakrabarti, T. Chatterjee, “ Back Propagation Neural Network Approach to Intrusion Detection”, IEEE International Conference on Recent Trends in Information Systems, pp (303-308), December 21th-23rd 2011, INSPEC Accession Number: 12542068.

[8] Dahiya. M, “Back Propagation Neural Network for Wireless Networking”, International Journal of Computer Science and Engineering, Volume.04, Issue-04, Page No (123-125), May 2016.

[9] ASN Chakravarthy, P S Avadhani, PESN Krishna Prasad, N. Rajeev, D. Rajasekhar Reddy, “A Novel Approach for Authenticating Textual or Graphical Passwords Using Hopfield Neural Network”, Advanced Computing: An International Journal (ACIJ), Volume.02, Issue-04, Page No (33-46), July 2011.

[10] Shouhong Wang and Hai Wang, “Password Authentication using Hopfield Neural Network”, IEEE Transactions on Systems, Man and Cybernetics- Part C: Applications and Reviews, Volume.38, Issue-02, Page No (265-268), March 2008.

[11] J.Suneetha and K.Sandhya Rani, "Recognition of Facial Expression Using AAM and Optimal Neural Networks", International Journal of Computer Sciences and Engineering, Volume-04, Issue-04, Page No (136-140), Apr -2016

[12] S. Humayun, Ye. Zhang, “ Hopfield Neural Networks- A Survey”, AIKED’07 Proceedings of the 6th conference on 6th WSEAS International Conference on Artificial Intelligence, Knowledge Engineering and Databases, Greece, pp (**125-130**), February 16th-19th **2007**, ISBN: 978-960-8457-59-**1.**

AUTHOR PROFILE

Ms Menal Dahiya is an Assistant Professor of Computer Science at Maharaja Surajmal Institute (Affiliated to GGSIP University, Dwarka) and a P.hD Research Scholar of Maharshi Dayanand University, Rohtak in the Department of Computer Science and Applications. She received her M.Phil in Computer Science from Chaudhary Devi Lal University, Sirsa, India in 2007. Before she had studied at Guru Jambheshwar University of Science and Technology (GJU), Hisar and Kurukshetra University, India. Her main research interest are Neural Network, Wireless Security and Wireless Communication. Several of her research papers have been published in International and National peer-reviewed journals indexed in Scopus, Copernicus and others.