A Review of Artificial Neural Network for Secure Access Authorization

MS. Khushboo R. Gupta.
M.E. 2^{nd} yr,PRMCEAM, Badnera,
Amravati University.

Prof. P. A. Khodke.
Dept. of Computer Science & Engg. PRMCEAM
Badnera, Amravati University.

Abstract

In the past decade, there has been a rapid development in internetworking and computing. So, information security is crucial in the field of information systems. Traditionally, authentication to access accounts, files and other valuables is based on passwords, PIN, physical keys, smartcards, any expensive biometric devices etc. Recent studies are performed for secure access authorization by using Artificial Neural Networks (ANN). Artificial Neural Networks (ANN) is computational model that mimic the biological neural networks in the brain. In this paper, we are discussing various approaches of ANN for secure access authorization. The use of ANN for secure Access authorization provides the benefit to eliminate the disadvantages of maintaining the conventional verification/password table and this makes the system much more secure[6] [12] [13] [15].

Keywords: *Artificial Neural Network (ANN), Information security, authentication.*

1. Introduction

The purpose of this paper is to introduce Artificial Neural Network (ANN) in the field of information security and to propose an easy to implement Neural Networks based approach for authentication. With the rapid increase of all types of information systems and the explosive use of the Internet majorly for business and educational information exchanges, protecting information and information systems from unauthorized access, information theft, and information interruption or destruction has been necessary nowadays. Therefore, to prevent an illegal user from interrupting the computer system, a user needs to provide an identity to a system as a proof of being legitimate user before he/she logs into the system. So far, there are many access control techniques to identify the legitimacy of login user such as passwords, PIN, smartcards, any expensive biometric devices like fingerprint etc.

Among many of these access control techniques, password based authentication has been widely used for long time and is still one of the most convenient and inexpensive mechanisms of today but has some drawbacks also because users have tendency to chose relatively short and simple passwords that they can remember or even strong passwords can be stolen. Thus, they are susceptible to various attacks. A common password authentication approach uses password and verification tables in which system keeps each authorized user's username/user Id and the corresponding password. When a user wants to login, he/she enters their User Id and password and the system then checks in the password table for a matching pair (User Id and password). If a match is found, the user is granted to login to the system otherwise the user is denied access. The major weakness of such an implementation is the possibility to steal saved (User Id, password) pair. Since an intruder may be able to read or alter passwords, storing information in password tables in the system may be a potential threat to the security of the network. So, password table should be kept secured.

We can avoid such problems by encrypting the (user Id, password) pairs before saving them in storage and then decrypting them. In such password based authentication approach, system uses the verification table in which encrypted passwords are stored. Passwords may be encrypted by one-way hash functions or any other encryption algorithms. Verification tables need not to be secured because an intruder cannot interpret the original passwords unless the encryption scheme's key is compromised. This technique has some more shortcomings like an intruder is still be to append a forged pattern to the verification table or replace someone's encrypted password. So the security of this technique can only be as strong as the encryption algorithm, authentication codes it relies on.

Another way to deal with these is to use an Artificial Neural Network (ANN) which learns the (User Id, password) pair and generates the matching signal representing the user registration [6]. This can be achieved by training ANN. In the training phase, the learned (User Id, password) pair is integrated into the neural network's weights. The benefit of this approach is that it does not require the matching (User Id, password) to be stored on the external storage but requires network weights to be stored. Even if these weights gets steal, it will be of not much use because without knowing the internal organization of the network and exact order of weights and which neural link they belong to, the process of retracting (User Id, password) is very much difficult.

In section 2, we review previous work on this subject. In section 3, we briefly discuss Artificial Neural Networks (ANN) features suitable for secure authorization along with the drawbacks of existing password based authentication approach. Then in section 4, we will discuss different authentication methods based on ANN. And finally section 5 will conclude this paper.

2. Related Work

In **2007, Reyhani & Mahadavi,**[12] have proposed neural networks in smart home networks for user authentication. Smart home networks [1] with distributed architectures consist of a broad range of wired or wireless devices, it is likely that unauthorized access to some restricted data or devices may occur. In this paper, authors have trained a neural network to store encrypted passwords and use it instead of the password or verification table.

This proposed method can solve the security problems in some authentication system and can be used to store the user profiles and access controls in smart home networks. They used a Radial Basis Function (RBF) neural network and hash the (User Id, passwords) with a one-way hash function and then encrypt them. The authors propose that RBF trains much faster than with back-propagation learning as RBF networks allows the selection of parameters for the hidden layer without the need for their optimization.

This scheme can produce the corresponding encrypted password according to the entered username, and it could be used to replace the password table or verification table stored in the common authentication systems. The first advantage of their proposed method is that an intruder cannot add a forged username and password pair to the neural network. The second advantage of our proposed scheme is the simple computation operations to produce results. The third advantage is that training time of RBF neural network is very short instead of the training time of MLP-BP neural network in similar authentication system.

Ciaramella et al, 2006[4] has dealt with the access control problem. Authors have focused their attention on passwords: Password-based schemes provide a certain level of security as long as users choose good passwords, i.e., passwords that are hard to guess in a reasonable amount of time. In order to force the users make good choices, a proactive password checker can be implemented as a sub-module of the access control scheme. Such a checker, any time the user chooses/changes his own password, decides on the fly whether to accept or refuse the new password, depending on its guess ability.

By using neural networks and statistical techniques, authors develop an effective and efficient proactive password checkers. In this paper, authors discuss and analyze proactive password checker based on multilayer neural network. They evaluate the performance of several network topologies and of a combined approach comprising standard preprocessing techniques of the inputs and neural networks. They have applied SLP (single layer perceptron) and MLP (multi layer perceptron) networks to design the proactive password checkers.

Wang and Wang, 2008[13] has used a Hopfield network for password authentication to overcome the drawbacks of conventional approach to system security. In neural network approaches to password authentication, no verification table is needed; rather, encrypted neural network weights are stored within the system. This study proposes the use of a Hopfield neural network technique for password authentication. In comparison to existing layered neural network techniques, the proposed method provides better accuracy and quicker response time to registration and password changes.

Access authentication is crucial for computer security. The use of neural networks has been proposed to eliminate the defective features of the traditional verification table approach. However, the existing layered neural network method suffers several limitations such as the lengthy training time and the arbitration in authentication. This paper shows that a Hopfield Neural Network (HNN)-based authentication scheme can effectively be used for access authentication in the open computing environment. An HNN, with large capacity, can store authentication information using marginal training time. The authentication scheme incorporating the use of HNN can recall information for a legal user's ID and password instantly and accurately.

Lin, I., Ou, H. & Hwang, M. (2005) [8] has done some related work. They proposed a method that employs the BPN to recall the relationship of username and password. This method can easily produce the corresponding hashed password according to the input username, and it could be used to replace the password table or verification table stored in the system. Although the system still needs to store the parameters of the trained network, the stored parameters do not leak any sensitive information out.

Li, Lin, Hwang (2001) [7] have worked on a remote password authentication scheme for Multi-server Architecture Using Neural Networks. They have used a multilayer neural network with back-propagation training. Conventional remote password authentication schemes allow a serviceable server to authenticate the legitimacy of a remote login user. However, these schemes are not used for multi-server architecture environments. The password authentication system is a pattern classification system based on an artificial neural network. In this scheme, the users only remember user identity and password numbers to log in to various servers. Users can freely choose their password. Furthermore, the system does not require maintaining a verification table and can withstand the replay attack. The server only stores the weights of the classification network.

According this network, the server can authenticate the validity of the login user in real time. The main advantage of this scheme is that it is applicable to both multiuser and multi-server networks. The system users can freely choose their password and the servers are required to retain only the pair user ID and password. The user can login to various servers without repetitive registration with each server. The password authentication scheme can prevent the replay attack; the intruder cannot obtain a login password through the open network and replay the password to login to a server.

Capuano, N.; Marsella, M.; Miranda, S.; Salerno, S. [3], worked on user authentication with neural network. The purpose of their paper is to introduce Artificial Intelligence in the field of data-security and to propose an easy to implement Neural Networks based method for user authentication. In this paper, authors have illustrated their method for user authentication which tries to conjugate the easiness of implementation of knowledge-based password approach with the top degree of security offered by the biometric one that appraises a personal and non-transferable individual characteristic, such as the typing style. Typing style is an ideal indicator for the authentication because it seems to be unique for many users (also not experienced) and does not involve any additional hardware (except for a keyboard). Neural Nets were in fact used by authors to recognize users by their own typing style.

3. Artificial Neural Network (ANN) Features

There are number of features in ANN that are suitable for our security designs. ANN takes a completely different approach to solving a problem than that of conventional computing techniques. If we compared the conventional techniques with ANN then we can say that in conventional computing system use algorithm approach i.e. a system follows a set of instructions in order to solve a problem. Unless the system knows the exact instructions, it cannot solve a problem. While ANN process the information in a way similar to human brain. It has the ability to learn by example. However ANN and conventional computing are not in a competition but complement each other. So we can use a combination of these two approaches. Now let's see exactly what ANN is and why we are proposing to use it i.e. its benefits.

Artificial Neural Networks (ANNs) are models inspired by natural nervous system (brain) that are capable of machine learning and pattern recognition etc. Neural Networks are typically organized in layers. These layers are presented as systems of interconnected as "neurons" (artificial nodes) that compute values from inputs by feeding information through the network. Neural Networks have been used to solve a wide variety of tasks that are hard to solve using ordinary programming.

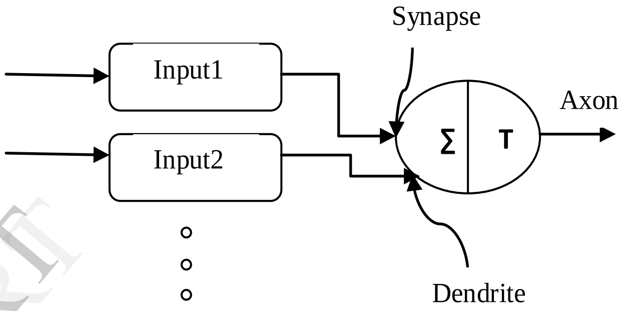

Figure1. Structure of Artificial neuron

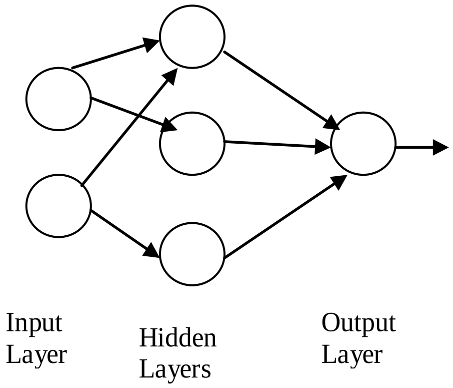

Figure2. Simple Artificial Neural Network

Many types of artificial neural networks (ANN) exits such as Feed-Forward Neural Networks, Radial Basis function (RBF) networks, Kohonen self-organizing network, Recurrent Neural network, Modular Neural Networks, etc[6].

Why Artificial Neural Network (ANN)? To answer this question we can list the number of features of ANN as below:

- **Learning ability** – As mentioned earlier ANN has the possibility to acquire knowledge through learning. This feature of ANN has attracted the most interest in ANN. Given a specific task to solve and a class of function, ANN can use a set of observations to solve the problem in an optimal sense.

Generally, according to the corresponding task, the learning ability can be categorized into two main types, i.e. supervised learning and unsupervised learning. In supervised learning, the inputs and outputs are known priori, so ANN learns by applying a cost function to generate the desired output for each given input. While in unsupervised learning, it is not known to priori that what the generated output should be for the given input combinations. So in this type of learning ANN learns itself by self-organizing the data and its properties.

- **One way property** – This one way property means that output can be easily computed from the given input while it is difficult or nearly impossible to compute input from output. This property is often required by the functions that are used to authenticate data's integrity.
- In Neural Network approaches to password authentication, no password or verification table is required; instead neural network weights are stored in the system.
- In ANN, only simple addition and multiplication are needed to produce the results compared to exponential computing required as in public key cryptography techniques.

4. Secure Access Authorization based on ANN

In this paper, we are mainly discussing various Artificial Neural Network (ANN) based approaches to achieve secure access authorization for the application where there are high risks of probing. So for this purpose, as mentioned earlier, there are number of artificial neural networks available such as Feed-Forward Neural Networks, Radial Basis function (RBF) networks, Recurrent Neural network, etc [6].

Feed-Forward type of artificial neural network (ANN) is the simplest type of ANN. In the Feed-Forward artificial neural networks, there are no cycles and in this network signals flow only in one direction, forward, from input nodes through the hidden nodes (if any) to the output nodes while in case of recurrent neural networks, there are loops i.e. neurons are linked in the same or previous layers.

The Multi-layer perceptron (MLP) neural networks are the examples of Feed-Forward ANN. Hopfield network is an example of recurrent neural network. In case of recurrent networks, dynamic changes can occur in the network because of their feedback cycles.

Now for secure authorization, we would train the neural network. For this there are number of training methods available such as:

- Back Propagation Network (BPN)
- Resilient Back Propagation Network (RBPN)
- Radial Basis Function network (RBF)
- Hopfield Neural Network (HNN), etc.

Back Propagation is a common method used for training ANN. In simple words, it includes the backward propagation of errors. If we say technically, BPN is used to calculate the gradient of error of the network with respect to the network's modifiable weights. It is a supervised learning method. From a desired output, the network learns from many inputs similar to the way a child learns to identify things from number of examples. It requires a dataset of desired output for the given set of inputs, making up the training set. BPN is most useful for Feed-Forward type of Neural Networks.

The calculated gradient in BPN is generally used in a simple Gradient Descent Algorithm to find weights that minimize the error. But such Gradient Descent Algorithms are not suited with multilayer networks mainly because multilayer networks generally makes use of sigmoid or tan sigmoid activation functions and slope of these functions tends to approach zero for large inputs.

Now as the name suggests, the Resilient Back Propagation Network (RBPN) is a kind of Back Propagation (BPN) network. The Resilient Back Propagation Network (RBPN) considers only the sign of the gradient to determine the direction of weight update. The size of the weight change is manipulated by a separate update value. In RBPN, if the weight continues to change in the same direction for several iterations, the magnitude of weight change is increased.

5. Conclusion and Future Work

Research in the field of artificial neural networks (ANN) has been attracting attention increasingly in the recent years compared to other techniques. In this paper, we provide an overview of existing work; discuss the drawbacks of existing password authentications techniques. We have also discussed benefits of Artificial Neural Network (ANN) approach for secure access authorization over the existing password authentication. The use of

ANN for secure Access authorization provides the benefit to eliminate the disadvantages of maintaining the conventional verification/password table and this makes the system much more secure[6] [12] [13] [15]. Next, we provide an overview different technologies and methods available for ANN based authorization. As discussed in this paper ANN will provide an improved secure authorization. Implementation of this approach is under progress and is left for future work.

6. References

[1] Anil Naik (2010), ARTIFICIAL NEURAL NETWORK FOR HOME SECURITY SYSTEM (ANNHSS), *Yuva Engineers, Mumbai University.*

[2] Bishop, C. (1995) Neural Networks Pattern Recognition, Oxford University Press, UK.

[3] Capuano, N.; Marsella, M.; Miranda, S.; Salerno, S., User Authentication With Neural Networks. *W. Duch (Ed), Proceedings of the V International Conference on Engineering Applications of Neural Networks (EANN 99), 13-15 September, (1999), Warsaw, Poland, pp. 200-205, Wydawnictwo Adam Marszalek, 1999, ISBN 8371745125.*

[4] Ciaramella, A; D'Arco, P., De Santis, A., Galdi, G. & Tagliaferri, R. (2006). Neural Network Techniques for Proactive Password Checking. *IEEE Trans. On Dependable and secure Computing*, Vol. 3, No. 4, pp. 327-339.

[5] Eun-Jun Yoon, Kee-Young Yoo. A New Remote User Authentication Scheme Using Interacting Neural Network. *Journal of Security Engineering (2008).*

[6] Fadi N. Sibai, Aaesha Shehhi, Sheikha Shehhi, Buthanina Shehhi and Najlaa Salami (2009). Designing and Training Feed-Forward Artificial Neural Networks For Secure Access Authorization. *http://www.intechopen.com*

[7] Li, L.; Lin, I. & Hwang, M. (2001). A Remote Password authentication scheme for multiserver architecture using neural networks. *IEEE Transactions on Neural Networks*, Vol. 12, No. 6, (November 2001), pp. 1498-1504.

[8] Lin, I., Ou, H. & Hwang, M. (2005). A user authentication system using back-propagation network. *Neural Computing and Applications*, 14, (2005), pp. 243-249.

[9] Manoj Kumar Singh; PASSWORD BASED A GENERALIZE ROBUST SECURITY SYSTEM DESIGN USING NEURAL NETWORK, *IJCSI International Journal of Computer Science Issues, Vol. 4, No. 2, 2009*

[10] Ramasubramanian, P.; Kannan, A. (2004). Quickprop Neural Network Ensemble Forecasting Framework for a Database Intrusion Prediction System. *Neural Information Processing–Letters and Reviews*, Vol. 5, No. 1, October 2004.

[11] Rojas, R.; Neural Networks: A Systematic Introduction, *Springer-Verlag, Berlin*, 1996

[12] Reyhani, S. & Mahadavi, M. (2007). User Authentication Using Neural Network in Smart Home Networks. *International Journal of Smart Home*, Vol. 1, No. 2, (2007), pp.147-154.

[13] Wang, S. & Wang, H. (2008). 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.

[14] Wang, G.; Hao, J.; Ma, J.; Huang, L.; A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. *Expert Systems with Applications, 2010 – Elsevier.*

[15] 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.*