IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 01-05
www.iosrjournals.org

Enhancing Authentication in Wireless Devices Using Neural Network

Menal[1], Dr. Sumeet Gill[2]

[1]*(menaldahiya@gmail.com, Department of Computer Science, Maharaja Surajmal Institute, Janakpuri, New Delhi, India)*

[2]*(drsumeetgill@gmail.com, Assistant Professor (CS), Department of Mathematics, Maharashi Dayanand University, Rohtak, Haryana, India)*

Abstract: *Security has been a crucial issue in the field of Wireless technology. One of the key points in the security is how to identify the authentication of the user. Authentication has been based on passwords or PIN etc. Password based authentication mechanism is very convenient and mostly adaptable in the Wireless devices. In conventional password based method, one way hash or any encryption algorithm is used to prevent the password but they are still vulnerable. In this paper we proposed a method based on Artificial Neural Network and use Back Propagation algorithm that can solve the security problems and enhance the security in Wireless devices.*

Keywords - *Artificial Neural Network, Authentication, Back Propagation algorithm, Wireless Technology*

I. INTRODUCTION

It is often seen that malicious people are trying to hack personnel information to harm someone intentionally. Today, security is the compulsory need for data operations. In every field trading, commerce, banking, business organization and information exchanges need security and reliability. Security problem is very much engrossed in wireless devices. Due to the excessive usage of wireless devices their security is the major issue. The unauthorized access can be prevented by user authentication. Authentication is a process of verifying the identity of communicating client stations which are involved through a protocol. User authentication is very necessary and beneficial in networked environment and it is important for wired and as well as for wireless devices. There are numerous security methods in today's era that are used for protecting the valuable information and resources that are attached to your system.

Conventionally, user authentication is mainly divided into –knowledge based, Token based and biometric based. Knowledge based authentication contains password and PIN codes. The Token based authentication relies on something one has and is characterized by possession whereas biometric based authentication is related to behavioral and physiological characteristics. Among these, password based security method is widely used because of its simplicity, applicability and cost effectiveness but obviously there is a lack of security in it, some drawbacks of conventional password appears like stolen the password, weak password etc.

Wireless technology ranges from complex systems to simple devices such as cell phones, i-pods, laptops, wireless headphones, PDAs, smart phones etc. also uses this authentication mechanism. These devices communicate and transfer information through some manner called protocol. The main wireless protocols that are explored in the field of wireless technology are: IEEE 802.11 covering wireless Ethernet; 802.15 dealing with wireless personal area networks (WPAN), including Bluetooth technology; and 802.16 for broadband wireless access.

Artificial Neural Network is a field that is inspired by the way the biological nervous system works. It contains large numbers of interconnected processing elements (neurons).

ANNs, like people, learn by examples. An ANN is configured for a specific application, such as pattern recognition or data classification, through a learning process.[1].

II. THE PROPOSED AUTHENTICATION SYSTEM

According to the learning ability, Artificial Neural Network has been used in Artificial Intelligence [2], neural network can be used to model nonlinear statistical data, which can model complex relationship between inputs and outputs.

The plan here is to use neural network to generate and memorize the identification parameters. The Back-Propagation Network (BPN) is one of the most well known types of neural network.

A. Neural network

The basic network architecture in this paper is a multilayer feed forward network using back propagation model. The input and output values of the network are represented as x_i and s_h for ith neurons in input layer and hth neuron in output layer, and w_{ih} is the weight that connects input of ith neuron to the output of hth neuron.**[3]**

The output values are given by the relation,

$$s_h = f\left[y_1^h\right]$$

in which y_1^h is the activation vector of any layer j and is given by:

$$y_1^h = \sum_{j=1}^{I} w_{ih} x_i$$

The error expression introduced for a single perceptron is generalized to include all squared errors for the outputs j=1,2,……..J for a specific pattern p=1,2,3,…..P that is at the input and gives the output error.

$$E^p = \frac{1}{2}\sum_{j=1}^{J}\left(d_j - y_j\right)^2$$

where, d is the desired output vector $[d_1 d_2 d_3 .... d_J]^t$

Now the weight adjustment is given as:

$$\Delta w_{hj} = -\eta \frac{\partial E^p}{\partial w_{hj}}$$

Where, η is the Back Propagation learning rate

This expression is adjusted as:

$$\frac{\partial E^p}{\partial w_{hj}} = \frac{\partial E^p}{\partial y_j^h} \cdot \frac{\partial y_1^h}{\partial w_{hj}} = \frac{\partial E^p}{\partial y_j^h} .\left[s_h\left(y_1^h\right)\right] = \frac{\partial E^P}{\partial s_j\left(y_1^h\right)} \cdot \frac{\partial s_j\left(y_j^h\right)}{\partial y_j^h}\left[s_h\left(y^h\right)\right]$$

Since $\frac{\partial S_j\left(y_i^h\right)}{\partial y_j^h} = \dot{S}_j(y_j^h)$

Hence the weight adjustment is now denoted as:

$$\Delta w_{ih} = -\eta \frac{\partial E^P}{\partial s_j\left(y_j^h\right)} .\dot{S}_j(y_j^h).s_h\left(y_j^h\right) = -\eta \sum_{j=1}^{J}\left(d_j - y_j\right).\dot{S}_j(y_j^h).s_h\left(y_j^h\right)$$

The final adjusted weight is given by:

$$\Delta w_{hj}(t+1) = w_{hj}(t) + \eta \sum_{j=1}^{J}\left(d_j - y_j\right).\dot{S}_j(y_j^h).s_h\left(y_j^h\right)$$

$$\Delta w_{ih} = \eta \sum_{j=1}^{N}\left(d_j - y_j\right) y_j^p .w_{hj} .\dot{S}_h(y_h^j).x_i^j$$

B. Authentication Process

For accessing the resources user login the system with password. Password may have various type of information like strings, characters or any alpha numeric data.There are three main components of the authentication process: input parameters, authentication algorithm and output values. In figure 1, we show the simple authentication method that uses the password as a input and any encryption algorithm that encrypts the password and store it and further compare it when someone login the system.

In password-based authentication approach, the passwords are encrypted by one-way hash functions [4, 5] or encryption algorithms [6] and then are stored as some patterns. Nevertheless, this technique has some shortcomings. An intruder is still able to append a forged pattern or replace someone's encrypted password.

There is an alternative approach to these schemes that uses neural network to overcome the security problem. In this approach, a neural network is trained with back-propagation (BP) algorithm to store the user encrypted passwords. In this method, the system stores the weights of the trained neural network and when system memorize these weights and store it in the form of encrypted file. We eliminate this encrypted file and as a result security of the system is increased. Although, this scheme offers more security compared to previous schemes. Figure 2 shows this explanation briefly.

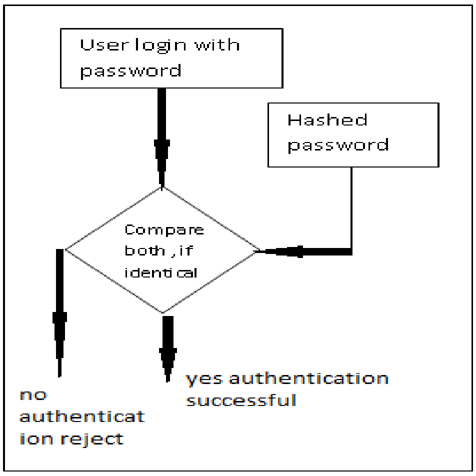
User login with password
Hashed password
Compare both , if identi cal
no authenticat ion reject
yes authentication successful

Fig 1. Simple authentication method

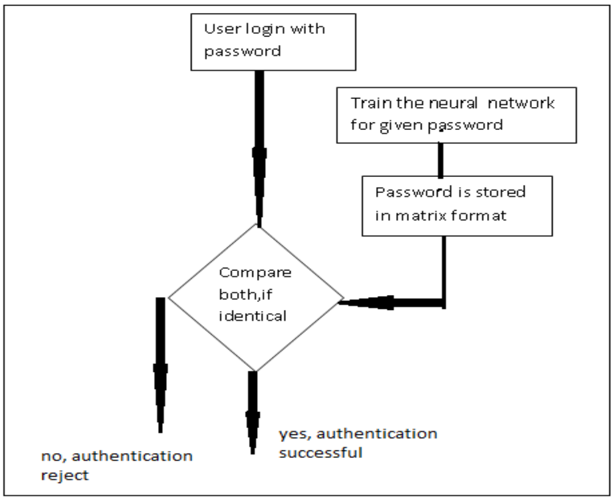
User login with password
Train the neural network for given password
Password is stored in matrix format
Compare both,if identical
no, authentication reject
yes, authentication successful

Fig 2. Proposed authentication method

In our proposed scheme, the neural network is initially trained using password. This trained network is then used to authenticate the validity of the user. So, the password is used as input of the neural network and the corresponding password as the desired output. Before, training the neural network, the system needs to normalize the ASCII codes of the characters.

III. EXPERIMENTAL RESULTS

In our authentication system, we use the information of a wireless device i.e. a mobile phone. The user chooses the password which can be either in characters, in numeric or in both, shown in table 1.Here, the training model (BPNN) is a supervised learning model. The model consists of three layers: input layer, hidden layers and output layer. The training set of the experiment is shown in table1. Password is consisting of two characters and it transformed each character into 8-bit binary code. Therefore, the BPN architecture had 16 input units in the input layer, 8 processing units in the hidden layer and 16 output units in the output layer.

Unique mapping of a given password can achieve by giving the training of neural network with taking password as an input. [1] Once training completed up to specified error value, the final output of network is the final mapped valued of the password.

Wireless Device	Password	Hashed Password
Mobile phone	a9	

Table 1. Wireless Device and its password

a. Training using neural networks

Parameter	**Value**
Neurons in Input Layer	16
Number of Hidden Layers	2
Neurons in Hidden Layer	8
Neurons in Output Layer	16
Total no. of Epochs	10
Minimum Error Exist in the Network	0.001
Initial Weights and biased term values	Values between 0 and 1

Table 2. Parameters used for Training of Network using Back Propagation Model

According to specified description of neural network and its utilization of authentication, the following experiment has done: Training of the system was carried out for input pattern set-[a9] means 0110000100111001. For estimating the encryption pattern of link keys, we first need to define the functional dependency between the encrypted link keys in the form of weights in the neural network.

Weights of layer 1 from input:-

2.3908	3.4473
2.7223	2.8964
-2.6394	-2.9597
6.9529	-1.2193
1.1054	3.797
-3.825	-0.37657
-2.4295	3.0533
2.6009	-7.1802

Weights between hidden layer output layer:-

4.0333	4.7747	-3.5301	0.25939
-6.9442	-3.3935	-4.7295	2.4726
0.28991	0.36352	-0.4841	0.8384
2.7581	0.087158	1.5486	-2.6495

b. Training Performance

The performance of the proposed method would be turned good because the trained BPN makes its output approached the expected output as close as possible.

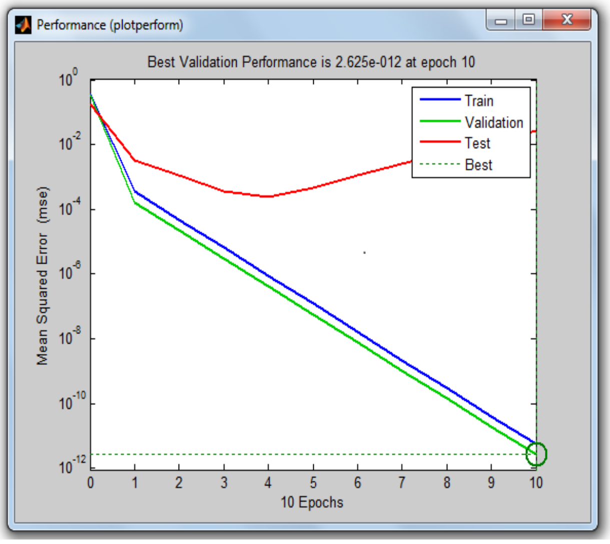

Fig 3. Graph for Network performance during Back Propagation Neural Network

IV. CONCLUSION

Simple password based Authentication system is the traditional computer network process. In contrast, our Authentication system uses neural network to recall the user's password. System stores the parameter of trained in the matrix format and for intruders it will be difficult to regenerate the inputs of the password as they are converted into weight values. This method gives new hope of development to password based security system.

V. FUTURE WORK

As the extension of this method, we use the information of two or more wireless devices and check the validity of this proposed authentication method on group of wireless devices.

REFERENCES

Journal Papers:

[1] M. K. Singh, "Password Based a Generalize Robust Security System design using Neural Network", IJCSI International Journal of Computer Science Issues, Vol.4, No. 2, 2009

[2] Bezdek j.c. “On the relationship between neural netwoks,pattern recognition and intelligence”, The international journal of approximate reasoning, 6(2): pp85-107,1992

[3] S.N Sivanandan ,S.Sumathi and S.N Deepa, Introduction to Neural Networks using MATLAB 6.0.

[4] I. B. Damgard, “A design principle for hash functions”, Advances in Cryptology, CRYPTO’89, pp. 416–427, 1989.

[5] R. C. Merkle, “One way hash function and DES”, Advances in Cryptology-CRYPTO’89, pp. 428–446, 1989.

[6] ISO/IEC 9797, “Data cryptographic techniques- Data integrity mechanism using a cryptographiccheck function employing a block cipher algorithm, Internal Organization for Standardization”