International Journal of Computer Science and Engineering (IJCSE)
ISSN 2278-9960
Vol. 2, Issue 1, Feb 2013, 1-8
© IASET

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

AN EFFECTIVE APPROACH TO AUTHENTICATE TEXTUAL AND GRAPHICAL PASSWORD USING MLP NEURAL NETWORK

D. DHIVYA[1], S. PRIYA[2] & V. ELAMATHI[3]

[1]Assistant Professor, Department of CSE, Narasu's Sarathy Institute of Technology, Salem, India

[2]Assistant Professor, Department of CSE, Salem College of Engineering and Technology, Salem, India

[3]Assistant Professor, Department of MCA, Narasu's Sarathy Institute of Technology, Salem, India

ABSTRACT

Security has been an important issue to enable secures remote access to corporate networks, enhance their online services, and open new opportunities for e-commerce is bringing ever-growing attention to the importance of securing user access and validating identities. Password authentication is a common approach to the system security and it s also a very important procedure to gain access to user resources. In this paper multilayer perceptron network is trained to store the passwords instead of using verification table in traditional method. This proposed method is for password authentication using alphanumeric password and graphical password. This study proposes a model provides better accuracy, and quicker response time to registration and password changes.

KEYWORDS: Password Authentication, Multilayer Perceptron Neural Network, Textual Password, Graphical Password

INTRODUCTION

Recently, computer security has become an important issue. More and more systems have added control to the access process for avoiding illegitimate users reading sensitive information. Password authentication is one of the mechanisms that is widely used to authenticate a legitimate user.

The password authentication system is a pattern classification system based on an artificial neural network. The users only remember user identity and password numbers to log in to various servers. Users can freely choose their password.

Furthermore, the system is not required to maintain a verification table and can withstand the replay attack [4].

The main limitation in using the traditional password authentication method is that, a server must maintain a password table that stores each user's ID and password.

Therefore, the server requires extra memory space to store the password table. However, this method is dangerous. The password information table could be read or altered by an intruder. An intruder can also append a new ID and password into the table. Password table is protected using hash functions later and instead of password table [3] verification table containing hashed password (encrypted) will be stored in the server.

Alphanumeric password is derived from a Character Set. There are so many types of Character sets depending upon the application where we need authentication.

One of the well known Character Set is the American Standard Code for Information Interchange (ASCII). It is a character encoding scheme based on the ordering of the English alphabet. A common attack against password authenticated systems is the dictionary attack.

An attacker can write a program that, imitating a legitimate user, repeatedly tries different passwords, say from a dictionary, until it gets the correct password. Graphical password presents an alternative defense against dictionary attacks [7].

Graphical password [7] schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text, psychological studies supports such assumption. Neural networks can learn to map input onto output data. Neural networks are computational models inspired by the principles of how the human brain works. Typically neural networks are used for problems like classification, prediction, pattern recognition, approximation, and association [2].

The Multilayer Perceptron [5] is an example of an artificial neural network that is used extensively for the solution of a number of different problems, including pattern recognition and interpolation.

An MLP consists of multiple layers of nodes in a directed graph, with each layer fully connected to the next one. Except for the input nodes, each node is a neuron (or processing element) with a nonlinear activation function. The number of neurons in the input layer depends on the number of possible inputs we have, while the number of neurons in the output layer depends on the number of desired outputs.

The number of hidden layers and how many neurons in each hidden layer cannot be well defined in advance, and could change per network configuration and type of data. In general the addition of a hidden layer could allow the network to learn more complex patterns, but at the same time decreases its performance.

In this paper, we propose an efficient password authentication scheme based on a Multilayer Perception a neural network. This system identifies the legitimate user in real time using a pattern recognition technique and is applicable to multiserver network architecture.

PROPOSED MODEL

The proposed method for password authentication is used to obtain maximum accuracy of results generated by multi layer perceptron neural network. It train the data usernames as input and password as output.

When a particular user submits his login credentials we have given his username as input to network and we checked whether the output of network and specified password are equal or not, if both are equal the user is an authorized person.

The process can be divided into three phases

- The registration phase
- The login phase
- The authentication phase

The procedures for password authentication are shown in figure 1.

The Registration Phase

In the registration phase, the user must first register with the server. The steps of the registration phase are as follows.

- Allow the new user U to choose a login password P freely.
- The neural network is constructed with the training pattern of the new user. The network architecture consists of three layers: the input layer, the hidden layer and the output layer. The input units are the password characters and the value. The password characters can be a textual or graphical image.

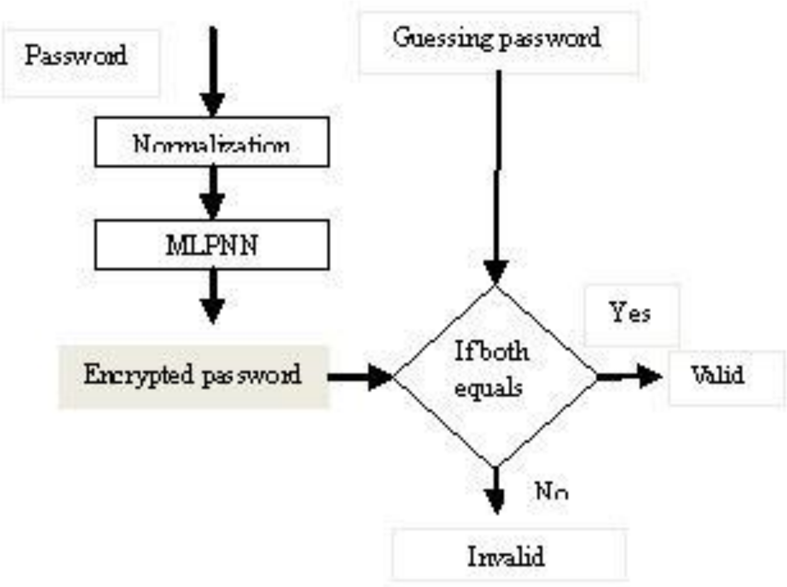


Figure 1: The Procedures for Password Authentication

The Login Phase

In this phase, assume that a legitimate user wants to login to server. The user can choose a password in textual or graphical image. If it is a image user can easily recall it to login.

The Authentication Phase

In the authentication phase the server performs the following tasks to authenticate the user's login request.

- The password is decrypted and the normalized data will be stored in verification table.
- Normalized data will forward to MLPNN and encrypted.
- If the encrypted data will be matched to the user login password then the output is valid.

A NEW AUTHENTICATION MODEL USING MULTILAYER PERCEPTRON NEURAL NETWORK

In network the output of neurons (unit) in one layer will be passed as input to the next layer and this process continues until the output layer units get an input from previous layers. Finally these output units yield an output. The output of network depends on Input, Connection strengths (Weight values), and Output function used in each layer. If we modify any of the above the output of the network will be changed. By taking this fact as an advantage we can perform encryption so that no attacker can decrypt it easily.

Here if 'P' is a row matrix representing input and 'W' is a matrix representing weights of the network then a MLP network produces cipher text in the following way.

$$C_i = \sum_{i=0}^{n} P_i W_{ij}$$

Method

- Define an own character set for alphanumeric data including special characters or we can use ASCII/GRAYCODE/EBCDIC/UNICOD.
- Normalize each character in to probabilistic values in the range [0, 1]

$$C_N = \frac{Ct - Cmin}{Cmax - Cmin}$$

where , C_t = Character taken,

C_{max}= maximum value of character set,

C_{min} = minimum value of character set

- a) The Normalized password data is supplied as input to a MLP neural network with one or more hidden layers. This produces encoded password in real values within the range [0, 1].

  b) Denormalize encoded data in to character notation (for memorization and backup).
- a) Guessing password data is given as input for MLP neural network with one or more hidden layers to produce decrypted data.

  b) If it is matched the password is authenticated, otherwise it is invalid.
- for de normalization use

  $C_t = C_N (C_{max} – C_{min})$

EXPERIMENTATION

Any organization which wants to use this novel password authentication technique can define their own Character Set by changing the order of the characters in the Character Set and giving their own maximum and minimum values for the Character Set.

If the organization wants to use existing character sets like ASCII, UNICODE etc., still they can use our technique and in order to increase security they can change the order of characters, even they can change constant assigned to each character.

Table 1: Example for Character Set

Character	ASCII
A	65
B	66
C	67
D	68
:	:

In the normalization we will convert each unique number assigned to a character in to probabilistic value.

Table 2: Normalized Character Set

Character	Probabilistic
A	0
B	0.04
C	0.08
D	0.12
:	:

Here we will convert the password into its corresponding probabilistic values and we can use those values as input to the neural network.

Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text; psychological studies supports such assumption [6]

Before giving the image as password the image should be converted in to its RGB values and these values will be normalized using our normalization function. we can't give image directly as input to the neural network. So image will be converted into matrix (or text).

After converting image into a matrix consisting of set of numbers we can give it to the neural network as input and we can train it using username and image matrix as a training sample.

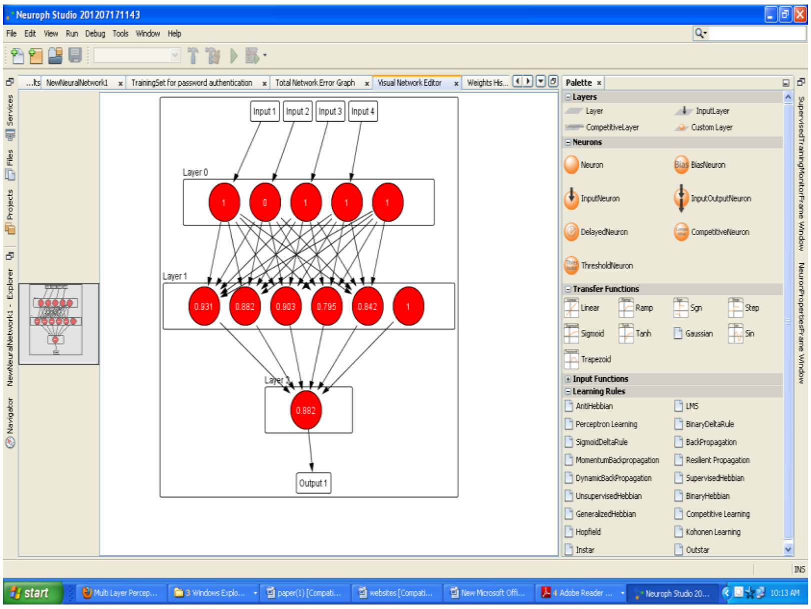
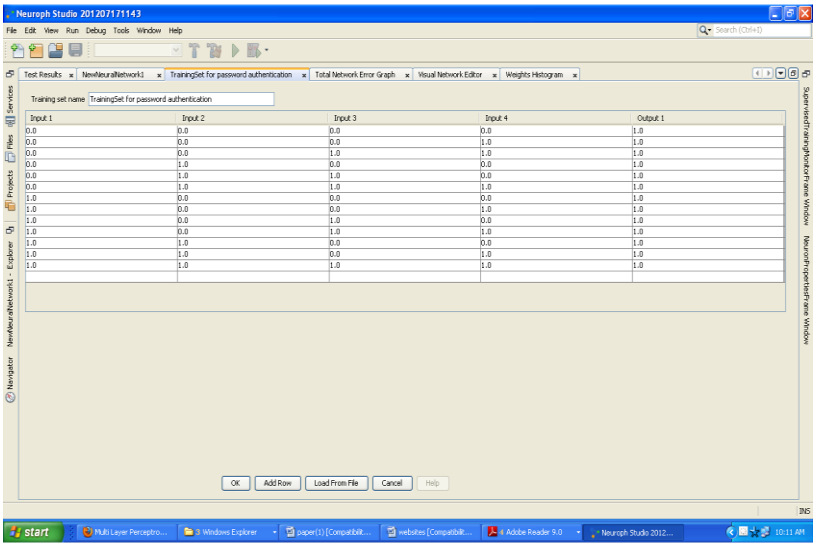


Figure 2: A Sample Multilayer Perceptron Model


Neuroph Studio 201207171143
File Edit View Run Debug Tools Window Help
Search (Ctrl+I)
Test Results
NewNeuralNetwork1
TrainingSet for password authentication
Total Network Error Graph
Visual Network Editor
Weights Histogram
OK
Add Row
Load From File
Cancel
Help
start
10:11 AM

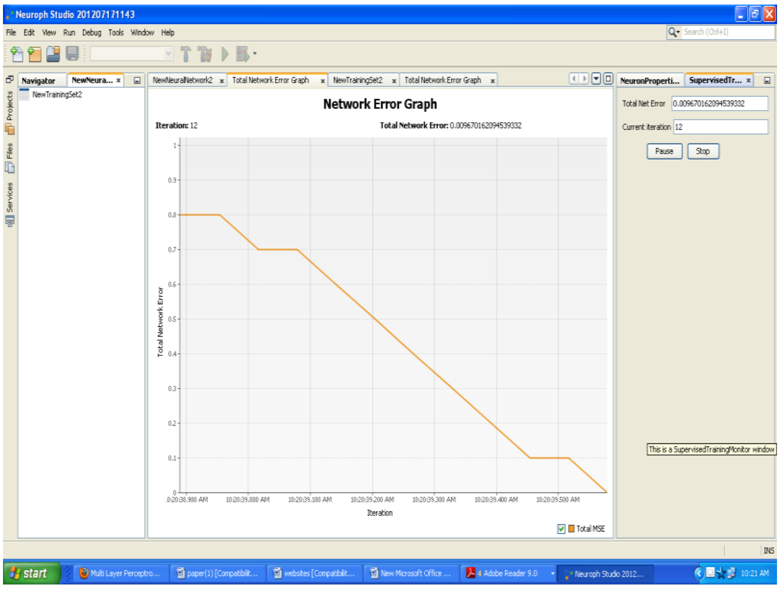
Training set name TrainingSet for password authentication

Input 1	Input 2	Input 3	Input 4	Output 1
0.0	0.0	0.0	0.0	1.0
0.0	0.0	0.0	1.0	1.0
0.0	0.0	1.0	1.0	1.0
0.0	1.0	0.0	0.0	1.0
0.0	1.0	1.0	0.0	1.0
0.0	1.0	1.0	1.0	1.0
1.0	0.0	0.0	0.0	1.0
1.0	0.0	0.0	1.0	1.0
1.0	0.0	1.0	0.0	1.0
1.0	0.0	1.0	1.0	1.0
1.0	1.0	0.0	0.0	1.0
1.0	1.0	0.0	1.0	1.0
1.0	1.0	1.0	1.0	1.0

Figure 3: Training the Network Using MLP

Table 3: Performance of MLP

MLP	
Accuracy	
Correct Rate	Error Rate
83.02%	16.98%



Iteration: 12

Total Network Error: 0.009670162094539332

Total Net Error 0.009670162094539332

Current iteration 12

Figure 4: Shows the Total Network Error Graph for Multilayer Perceptron Neural Network. It shows the Improved Accuracy and Minimum Error Rate

CONCLUSIONS

In this paper, authentication using back propagation is implemented for both textual and graphical passwords. In the training process normalized input values were used for enhancing the password authentication. The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. In this scheme, the server does not store or maintain password or verification table. The server only stores the weights of the classification network. Model provides better accuracy, and quicker response time to registration and password changes. In future the password authentication can be provided to sound signal by signal recognition in neural network.

REFERENCES

1. Chakravarth, A.S.N., Prof. Avadhani, P.S., Krishna Prasad, P.E.S.N., Rajeev, N. and Rajasekhar reddy, D. July 2011. A novel approach for authenticating textual or graphical passwords using hop field neural network. Advanced Computing: An International Journal (ACIJ).

2. Prasad, B.D.C.N., Krishna Prasad, P.E.S.N. and Sagar Yeruva, December 2010. A Study on Associative Neural Memories. Horng, G. 1995. Password authentication without using password table.

3. Li-Hua Li, Iuon-Chang Lin, and Min-Shiang Hwang, November 2001. A Remote Password Authentication Scheme for Multiserver Architecture Using Neural Networks. IEEE Transactions On Neural Networks.

4. Sta_ordshire University Beaconside Sta, November 17, 2005. Multilayer Perceptron Tutorial Leonardo Noriega School of Computing.

5. Shouhong Wang and Hai Wang, March 2008. Password Authentication Using Hopfield Neural Networks. IEEE Transactions On Systems, Man, And Cybernetics.

6. Xiaoyuan Suo, Ying Zhu, and Scott Owen, G. December 5-9, 2005. Graphical Passwords: A Survey, Proceedings of 21st Annual Computer Security Applications Conference.

7. http://neuroph.sourceforge.net/tutorials/MultiLayerPerceptron.html

Ms.D.Dhivya is currently working as a Assistant Professor in the Department of Computer Science and Engineering in Narasu`s Sarathy Institute of Technology, Salem. She received her M.E degree in Computer Science and Engineering under Anna University of Technology, Coimbatore in May 2011. She received her B.E degree in Computer Science and Engineering, under Anna University Chennai in May 2009. Her research interest is in Data Mining, Neural Networks and Bioinformatics.

Ms.S.Priya is currently working as a Assistant Professor in the Department of Computer Science and Engineering in Salem College of Engineering and Technology, Salem. She received her M.E degree in Computer Science and Engineering under Anna University Chennai in May 2012. She received her B.E degree in Computer Science and Engineering, under Anna University Chennai in May 2009. Her research interest is in Wireless Networks and Neural Networks.

V.Elamathi is currently working as a Assistant Professor in the Department of Computer Applications in Narasu`s Sarathy Institute of Technology, Salem. She received her MCA degree in Computer Applicatios under Anna University, Coimbatore in May 2011. She received her B.Sc degree in Microbiology, under Periyar university, Salem in May 2008. Her research interest is in Wireless Networks, Bioinformatics and Neural Networks.