User Authentication Using Neural Network in Smart Home Networks

Shahbaz Zahr Reyhani and Mehregan Mahdavi
Department of Electrical & Electronics Engineering, Guilan University, Rasht, Iran
{shahbaz, mahdavi}@guilan.ac.ir

Abstract

Security has been an important issue in the smart home applications. In home networks with distributed architectures that consist of a broad range of wired or wireless devices, it is likely that unauthorized access to some restricted data or devices may occur. Therefore, it becomes important to consider issues of security, authentication and access control. The authentication and authorization of users in smart environments are the key factors in the security of home networks. User authentication has been traditionally based on PIN, password, key, smart card or biometrics. Password-based authentication is widely used to identify legitimate users, because passwords are cheap, easy and reasonably accurate. In conventional password-based authentication methods, passwords store as a password or verification table. These methods use some encryption algorithms to prevent the passwords from being revealed, but they are still vulnerable. In this paper, we train 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.

1. Introduction

User authentication is very important in a networked smart environment. Authentication schemes are mostly based on passwords, smart cards and biometrics [1]. Currently, a vast majority of systems use passwords as the means of authentication. Passwords are very convenient for the users, easier and inexpensive to implement and consequently very popular in smart homes that use a computer to authenticate local or remote users. Whereas more secure authentication schemes have suggested, e.g., using smartcards or biometrics, none of them have been widely used in the consumer market [2].

Although, the password-based authentication is very convenient, but has some drawbacks because users have obviously tendency to choose relatively short and simple passwords that they can remember. Thus, they are very much susceptible to exhaustive search or dictionary attacks [3, 4].

In simple password-based authentication scheme, the system keeps each legitimate user’s ID, UID, and the corresponding password, PWD, in a table (Figure 1a). Since an intruder may be able to read or alter passwords, the password table in the system may present a potential threat to the security of the network, so this table should be kept secured.

In other password-based authentication approach, the system uses a verification table [3, 5]. In this scheme, the passwords are encrypted by one-way hash functions [6, 7, 8] or encryption algorithms [9] and then are stored as some patterns in the table (Figure 1b). The verification table need not be kept secured, because an intruder cannot decipher the original passwords from what is stored in the table [10]. Nevertheless, this technique has some shortcomings. An intruder is still able to append a forged pattern to the verification table or replace someone's encrypted password.

There is an alternative approach to these schemes that uses a Multilayer Perceptron (MLP) neural network to overcome the security problem of the verification table [11]. In this approach, a neural network is trained with back-propagation (BP) algorithm to store the user IDs and the corresponding encrypted passwords. In this method, the system stores the weights of the trained neural network instead of the verification table. As a result security of the system is increased. Although, this scheme offers more security compared to previous schemes, but still has minor weaknesses. The training time of its neural network is very long and the outputs of the neural network are not exact.

In this paper, we propose our scheme that is similar to the one proposed by Lin et al. [11], but is based on Radial Basis Function (RBF) neural network. Our proposed scheme uses an RBF network to overcome the drawbacks of the method presented by Lin.

The remainder of this paper is organized as follows: Section 2 explains our proposed method. We present our experimental results in Section 3. Finally, some conclusions are presented in Section 4.

2. The Proposed Authentication Scheme

In this section, we explain the details of our proposed method and show how an RBF neural network can be used to effectively authenticate users.

2.1. The neural network mode

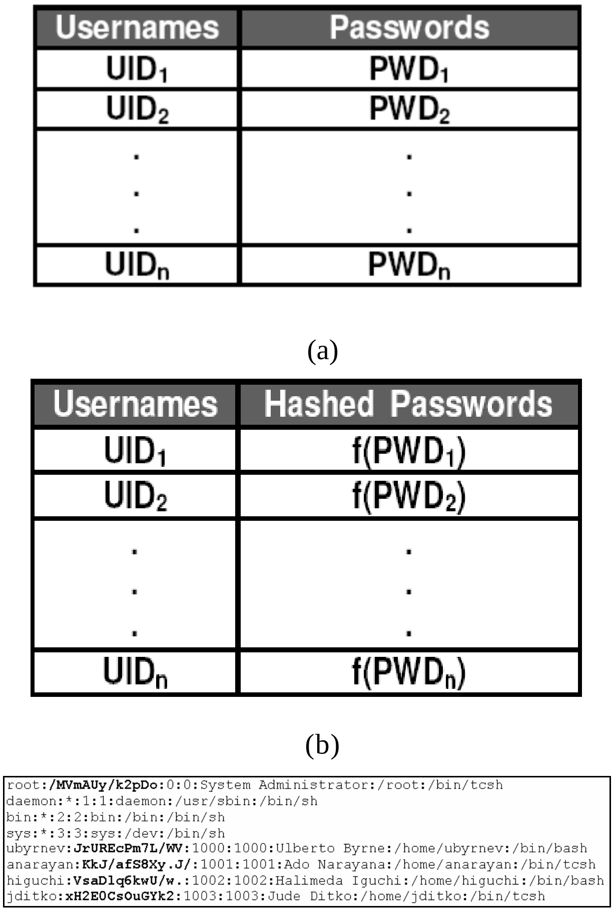
The proposed authentication system uses an RBF network. RBF networks are feed-forward neural networks trained using a supervised learning algorithm. They are typically configured with a single hidden layer of units whose activation function is selected from a class of functions called basis functions. While similar to back propagation network in many respects, RBF networks have several advantages. They usually train much faster than back propagation networks. RBF neural networks have been traditionally associated with a simple architecture of three layers [12, 13]. Each layer is fully connected to the following one and the hidden layer is composed of a number of nodes with radial activation functions called radial basis functions. Each of the input components feeds forward to the radial functions. The outputs of these functions are linearly combined with weights into the network output (Figure 2). Each radial function has a local response since their output only depends on the distance of the input from a center point. Each hidden layer unit computes an activation function which usually uses the following Gaussian function:

$$\varphi_i = e^{\left(-\frac{\|u - c_i\|}{2\sigma_i^2}\right)} \quad , i=1, 2,\ldots, l \qquad (1)$$

where u is the input vector and ϕ_ι is the output of the i-th unit. We call c_i and σ_i the center and the width of the i-th unit in the middle layer, respectively. ||.|| denotes the Euclidean distance. Each output layer unit computes a linear weighted sum of the outputs of the middle layer as follows:

$$x_j = \sum_{i=0}^{n} \varphi_i w_{ij} \qquad , j=1, 2,\ldots, m \tag{2}$$

where x_j is output of the j-th unit in the output layer. w_{ij} is the weight between the i-th middle layer neuron and the j-th output layer unit. More details about the training algorithm of RBF neural networks can be found in [14]



Usernames	Passwords
UID_1	PWD_1
UID_2	PWD_2
. . .	. . .
UID_n	PWD_n

(a)

Usernames	Hashed Passwords
UID_1	$f(PWD_1)$
UID_2	$f(PWD_2)$
. . .	. . .
UID_n	$f(PWD_n)$

(b)

```
root:/MVmAUy/k2pDo:0:0:System Administrator:/root:/bin/tcsh
daemon:*:1:1:daemon:/usr/sbin:/bin/sh
bin:*:2:2:bin:/bin:/bin/sh
sys:*:3:3:sys:/dev:/bin/sh
ubyrnev:JrUREcPm7L/WV:1000:1000:Ulberto Byrne:/home/ubyrnev:/bin/bash
anarayan:KkJ/afS8Xy.J/:1001:1001:Ado Narayana:/home/anarayan:/bin/tcsh
higuchi:VsaDlq6kwU/w.:1002:1002:Halimeda Iguchi:/home/higuchi:/bin/bash
jditko:xH2EOCsOuGYk2:1003:1003:Jude Ditko:/home/jditko:/bin/tcsh
```

(c)

Figure 1. (a) The password table, (b) the verification table, (c) the example of the usernames and encrypted passwords in some operating systems, the passwords are shown as bold face.

One of the advantages of RBF neural networks, compared to MLP networks, is the possibility of choosing suitable parameters for the units of hidden layer without having to perform a non-linear optimization of the network parameters. Hence, they are usually trained much faster than MLP networks. In our proposed scheme, the RBF neural network is initially trained using ID/password pairs. The trained network is then used to authenticate valid users.

2.2. The proposed scheme

Our user authentication scheme has two phases: the user registration phase and user authentication phase. First, authorized users have to register in the authentication system by giving their username and password. In second phase, i.e., the user authentication phase, the system validates the legitimacy of the users. The details of our authentication scheme are described as follows.

2.2.1. The user registration phase

In this phase, the system administrator obtains the training patterns from usernames and passwords to train the neural network. The registration process is described as follows.

1. Each user chooses a proper username and password and gives them to the system administrator.

2. The system applies a one-way hash function to the username and password and the result is used as the training pattern. So, the training pattern consists of hashed username, as the input of the neural network, and the corresponding hashed password, as the desired output of the neural network (Figure 3).

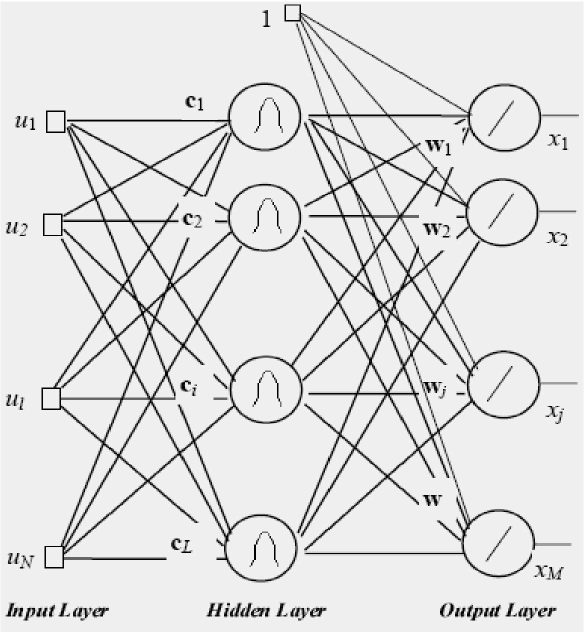


Figure 2. The structure of RBF neural network.

3. Before training the neural network, the system needs to normalize the ASCII codes of the characters of the training patterns.

4. The system administrator uses these training patterns for training the RBF network. After training process, the system administrator stores the RBF network weights in the system.

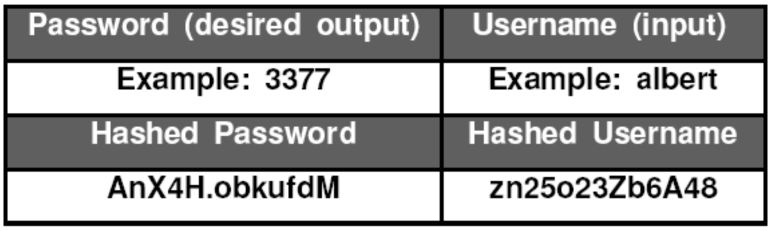
2.2.2. The user authentication phase

In this phase, the authentication system uses the trained RBF network and applies the same one-way hash function to authenticate the legality of the users. The authentication process is described as follows.

1. The system applies the same hash function on the entered username and password.

2. The system extracts an output through the trained neural network.

3. The system compares the output of the RBF network with the hashed password. If the results are equal, the user is recognized as an authorized user. Otherwise, the user is rejected as an illegal user (Figure 4).



Password (desired output)	Username (input)
Example: 3377	Example: albert
Hashed Password	Hashed Username
AnX4H.obkufdM	zn25o23Zb6A48

Figure 3. A sample training pattern

3. Experimental results

In our authentication system, we use the information of 200 sample users [11] to train the RBF neural network. Each username and password consists of eight characters. These usernames and passwords are hashed with a one-way hash function and are transformed to the encrypted words that are used as training patterns. Each of them consists of 13 characters and the ASCII code of each character in encrypted words is normalized. Therefore, the RBF network architecture has 13 input units in the input layer, 13 processing units in the hidden layer and 13 output units in the output layer. When the training of the RBF network is complete, the weight values of the neural network are stored in a 200 X 13 array. The array is then used to validate the legitimacy of the users in the user authentication phase. This authentication system was run on an Intel P4-2GHz PC with 256 MB size of RAM.

3.1. Accuracy and performance analysis

The authentication system has a good accuracy, as the trained RBF neural network generates outputs that are exactly identical to desired outputs. When a user enters a wrong username and password, the system inputs the hashed username to the trained RBF neural network and gets a hashed password that is not identical to the right password. Therefore, the user is rejected as an unauthorized user.

In the testing phase, we use the same training patterns to test the authentication system. In this phase, when we input the right username, the output of the system is the corresponding hashed password. The reason is that each username and password has been registered in the system and has been used to train the RBF neural network. If we randomly input an unauthorized username, the output from the RBF neural network is not equal to the existing hashed password. In other words, an unauthorized user would never be able to log into the network.

Our authentication system has a good performance in terms of the network training time and response time. The system spends a short time to train the RBF neural network. After the training process, the authentication system can be used to authenticate the identity of the user efficiently. Our authentication system, unlike some cryptographic systems, requires simple computing operations to produce the result

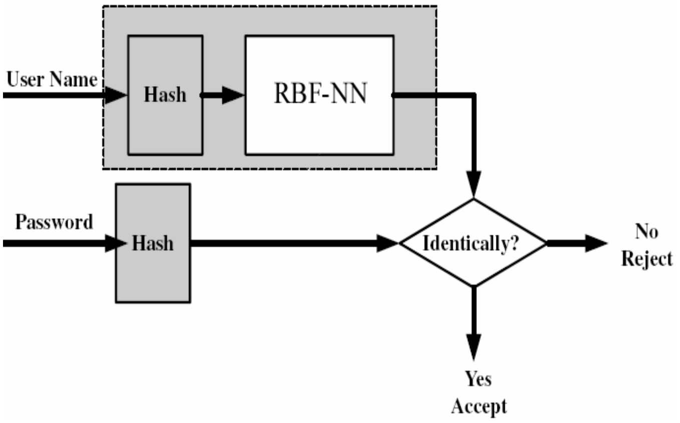


Figure 4. The user authentication phase in proposed system

The results are shown in Table 1. It compares the training times of MLP and RBF neural networks. As shown in the table, RBF network results in less training time than MLP network with BP learning algorithm. The output accuracy and response time of the trained MLP and RBF networks are also compared. According to the results output error in RBF network is very low and close to zero. The RBF network results in a response time equal to MLP network.

Table 1. The comparison of the network output error, training and response time of various methods

Method	Training time	Response time	Error
Verification table	-	< 1 sec.	0
MLP network	< 60 min.	< 1 sec.	< 3%
RBF network	< 2 sec.	< 1 sec.	≈0

3.2. Security analysis

In our authentication system, the usernames and passwords are encrypted to the patterns using one-way hash functions [7]. The security of our system is based on the difficulty of the patterns to the original usernames and passwords. Thus, an intruder cannot easily extract a password from the pattern even if he/she knows the weights of the trained neural network. Therefore, only the registered user would know both the correct username and the corresponding password

A disadvantage in our proposed authentication system is that an intruder may get the weights of the trained neural network and try all possible passwords to verify them until a match occurs. Such an attack is called a guess attack [10], and it has become a major threat to the security of some systems especially for the users who usually tend to select an easy-to-remember password [15]. An efficient way to prevent the guess attack is to select a strong password or use a method similar to the one offered in [10].

In some authentication systems that use the verification table, an intruder can easily append a forged pair of username and password into the table. In our proposed system, each user's username and password is combined in the trained RBF neural network and adding a forged entry is very difficult. In this case, an intruder has to collect all usernames and passwords to retrain the neural network or change its weights in order to match the forged username with the excepted password.

4. Conclusions

Some authentication systems traditionally use a password table or verification table. In our authentication system, we employ the RBF neural network to recall the relationship of username and password. 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 our 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 [11].

Our proposed authentication system can be used in embedded systems and some applications that require low computational capability. After the network is trained, the applied data (usernames and passwords) are converted to the weight values that can not be interpreted by an intruder. So, this system can be used to securely store the passwords, user profiles, device profiles and access controls in smart home applications

5. References

[1] S. Bleha, M. S. Obaidat, "Dimensionality reduction and feature extraction applications in identifyi ng computer users", IEEE Trans Syst Man Cybern 21, pp. 452–456, 1991.

[2] V. Goyala, V. Kumara, M. Singha, A. Abrahamb, S. Sanyalc, "A new protocol to counter online di ctionary attacks", computers & security 25, pp. 114–120, 2006.

[3] R. Morris, K. Thompson, "Password security: a case history", Communications of the ACM Nove mber 22(11), pp. 594–7, 1979.

[4] D. V. Klein, "Foiling the cracker: a survey of, and improvements to password security", Proceedin gs of the second USENIX UNIX security workshop, pp. 5–14, 1990.

[5] A. Jr. Evans,W. Kantrowitz, E. Weiss, "A user authentication scheme not requiring secrecy in the c omputer", Commun ACM 17, pp. 437–442, 1974.

[6] I. B. Damgard, "A design principle for hash functions", Advances in Cryptology, CRYPTO'89, pp. 416–427, 1989.

[7] R. C. Merkle, "One way hash function and DES", Advances in Cryptology-CRYPTO'89, pp. 428–446, 1989.

[8] R. C. Merkle RC, "A fast software one-way hash function", J Cryptogr 3(1), pp. 43–58, 1990.

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

[10]U. Manber, “A simple scheme to make passwords based on one-way function much harder to crack”, Comput Security 15(2), pp. 171–176, 1996.

[11]IC Lin, HH Ou, MS Hwang, “A user authentication system using back-propagation network”, Neural Comput & Applic 14, pp. 243–249, 2005.

[12]D. Broomhead, D. Lowe, “Multivariable functional interpolation and adaptive networks”, Complex Systems 2, pp. 321-355, 1988.

[13]J. Moody and J. Darken, Fast learning in networks of locally-tuned processing units,” *Neural Computation*, vol. 1, pp. 281-294 , 1989.

[14]C. M. Bishop, “Neural networks for pattern recognition”, Clarendon Press, Oxford, 1995.

[15]D. L. Jobush, A. E. Oldehoeft, “A survey of password mechanisms: weakness and potential improvements”, Comput Security 8, pp. 587–604, 1989.

Authors

Shahbaz Zahr Reyhani

Received a B.S. degree in electrical and electronics engineering from Guilan University, 1992, and M.S. degree in electrical and electronics engineering from Shiraz University, Iran, 1997. He is lecturer in the Department of Electrical and Electronics Engineering, Guilan University, Iran. His research interests include neural networks, embedded systems, computer networks and computer network security.

Mehregan Mahdavi

Is Assistant Professor in the Department of Electrical and Electronics Engineering, Guilan University, Iran. His research interests are in the area of Web and database including Web caching, Web portals, Web Services, Web data integration, and data versioning. He has published some papers on these topics. His research area also includes identity and access management. He is a member of the IEEE.