SMSCC: Smarter and More Secure Credit Card Using Neural Networks in Zero Knowledge Protocol

Dr. Abeer Tariq

Abeer282003@yahoo.com
University of Technology - Computer Sciences Department

Abstract: *This paper aims to execute the concept of zero-knowledge that's used in web applications using feed forward neural networks (FFNN). Neural networks have been used in our proposal instead of any other Artificial Intelligence method like genetic algorithms, swarm intelligence algorithms, and machine learning in order to enhance the zero-knowledge method for its randomness and high-level authenticity. The new suggested method has been compared with the traditional method in terms of confidentiality, authenticity, accuracy and speed. It has been noted that the new suggested method is more authenticated and secure than its counterpart in web applications especially ones that require the use of credit cards, which demands a very strong protection between the client and the server in order*

to gain the client's confidence in these Websites and protect them from the piracy.

Keywords: Zero-Knowledge, artificial neural networks, client-server technology.

Introduction

Our time is characterized by the exchange of data, some of which is very sensitive, and the knowledge of such information could have important consequences to our future. The importance of knowing a credit card number or a password to access a secret database must be considered. Information exchange between two parties is essential in our world, and during this transfer, something bad could happen. For example, a third party could eavesdrop on the transmission, and then use the data in some malicious way for personal advantage. The so-called Mafia fraud consists of intercepting electronic payment messages, and then using that information to buy something very expensive [1].

Modern cryptography is based on the secrecy of the key. In Secret-Key Cryptosystems, two parties have to meet and agree on a common secret key before any communication can happen. In Public-key Cryptosystems, each party has a pair of keys, one published in a database available to everybody and the other kept secret. This scheme eliminates the need for a preliminary secure interaction between the two parties. The strength of this scheme rests on the limited computational resources available to each user, legitimate or malicious. The main idea in any public key cryptosystem is a difficult computational problem. The security is based on the fact that the private key can be computed from the public key only by solving this difficult problem. With the public key, a user could encrypt messages, and another could decrypt them with the private key. The owner of the private key would be the only one who could decrypt the messages, but anyone knowing the public key could send them in privacy [2].

Zero-knowledge protocols allow identification, key exchange and other basic cryptographic operations to be implemented without leaking any secret information during the conversation and with smaller computational requirements than using comparable public key protocols. Thus Zero-knowledge protocols seem very attractive especially in smart card and embedded applications [3].

Related work

Many researches were performed to enhance zero knowledge and other security models to exchange data over unsecure network some of these are:

1. L. J. Jun and Brandon apply a practical web/python implementation of Zero-Knowledge Authentication protocol without any prior knowledge of the concept of Zero-Knowledge Proof.

The Zero-Knowledge Proof is a concept used in many cryptography systems. It allows a party to prove that he/she knows something (i.e. credential), without having to send over the value of the credential. In this implementation, it will be used to prove the password of the user without sending over the actual password. The system also allows for no password hashes to be stored on the server. The purpose of the implementation is to make implementing the Zero-Knowledge Proof Authentication portable and easily customizable. This is achieved by using python based.[4]

2. S. K.. Udgata and S. L. Sabat address some of the special security threats and attacks in Wireless sensor networks WSNs. They propose a scheme for detection of distributed sensor cloning attack and use of zero knowledge protocol (ZKP) for verifying the authenticity of the sender sensor nodes. The cloning attack is addressed by attaching a unique fingerprint to each node, that depends on the set of neighboring nodes and itself. The fingerprint is attached with every message a sensor node sends. The ZKP is

used to ensure non transmission of crucial cryptographic information in the wireless network in order to avoid man-in-the middle (MITM) attack and replay attack. The paper presents a detailed analysis for various scenarios and also analyzes the performance and cryptographic strength [5].

Basic Techniques Used in Proposal

There are two basic techniques used in our proposed system we will explain them according to using them in our proposal:

Zero-Knowledge Proof

Zero-Knowledge proof is a much popular concept utilized in many cryptography systems. In this concept, two parties are involved, the prover A and the verifier B. Using this technique, it allows prover A to show that he has a credential (for example, a credit card number), without having to give B the exact number. The reason for the use of a Zero-Knowledge Proof in this situation for an authentication system is because it has the following properties [4]:

- **Completeness**: if the statement is true, the honest verifier (that is, one following the protocol properly) will be able to prove that the statement is true to an honest verifier everytime.
- **Soundness**: if the statement is false, it is not possible (with a very small chance) to fake the result to the verifier that the statement is true.
- **Zero-knowledge**: if the statement is true, the verifier will not know anything other than that the statement is true. Information about the details of the statement will not be revealed.

ZKA_wzk Logic Algorithm [4]

The ZKA_wzk logic, as mentioned will be based on the ZKPoK Sigma Protocol. The following is a step-by-step procedure of the protocol, using **SPK**1{(x) : $Y = g0^{x}$} (*a*).

Initialization:

1. Given group ***G***. Let *g0*, *g1* be random elements of ***G***.
2. Let the public key be *zkapk* ={***G***, *g0*}.

Registration Process:

1. User inputs *username* and *password*.
2. The user hashes the password with Hash function, *H* and calculates *x = H(password).*
3. The user then computes $Y = g0^x$
4. The user sends (username, Y) to the server
5. The server stores (*username*, *Y*) into the database.

Authentication Process:

1. The server generates a random one-time token *a* and stores it and sends it to the user.
2. The user inputs username and password
3. The user hashes the password with Hash function, *H* and calculates *x = H(password).*
4. The user then computes $Y = g0^x$
5. The user generates random rx ϵ ***G*** and calculates $T1=g0^{rx}$.
6. The user then calculates *c=H(Y,T1,a).*and *zx = rx – cx*
7. The user sends (*c*, *zx*) over to the server
8. The server calculates *T1=Ycg0 zx* and verifies that *c=H(Y,T1,a)*
9. If successful, user is authenticated.

Single-Layer Neural Network

A single-layer net has one layer of connection weight as shown in figure (1). Often, the units can be distinguished as input units, which receive signals from the outside world, and output units, from which the response of the net can be read. In the typical single-layer net shown in figure bellow the input units are fully connected to output units but are not connected to other input units and the output units are not connected to other output units. The set of equations relating inputs and outputs is given by [6]:

$$y_{js} = f_j\left(\sum_{i=0}^{I} w_{ji}x_{is}\right);\ j = 1,2,\ldots,J;\ s = 1,2,\ldots,S,$$

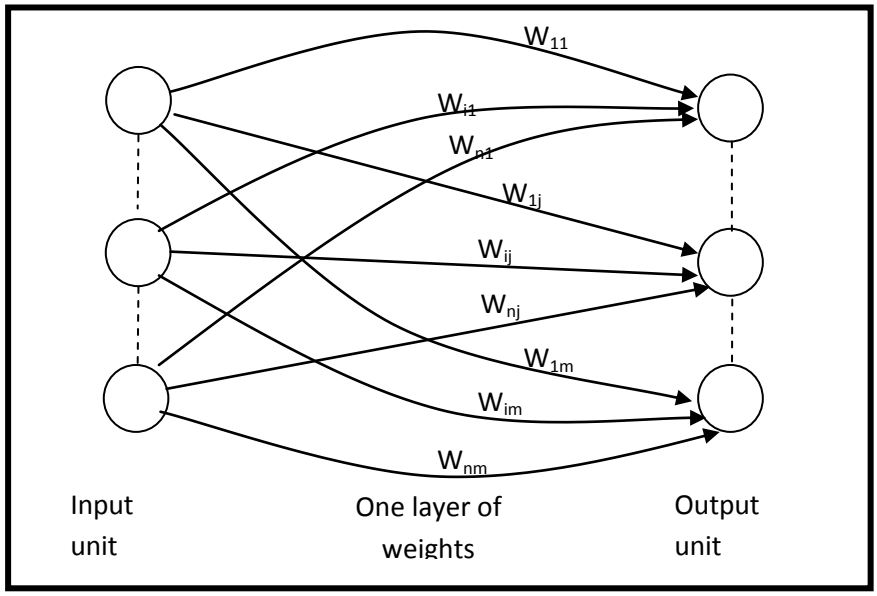

Figure (1) single layer neural network

Short characterization of feed forward networks [6]:

1. Typically, activation is fed forward from input to output for a single layer and through 'hidden layers' for multi layer, though much other architecture exist.
2. Mathematically, they implement static input-output mappings.
3. Most popular supervised training algorithm: back propagation algorithm.
4. Have proven useful in many practical applications as approximations of nonlinear functions and as pattern classificatory.

Current web application login process

The most common login system used in web application currently is through the use of a form submission of a username and passwords enabled with SSL communication. In more secure systems, the password is hashed using a java script-based md5 hash before sending it over. Figure (2) illustrates traditional authentication system [4].

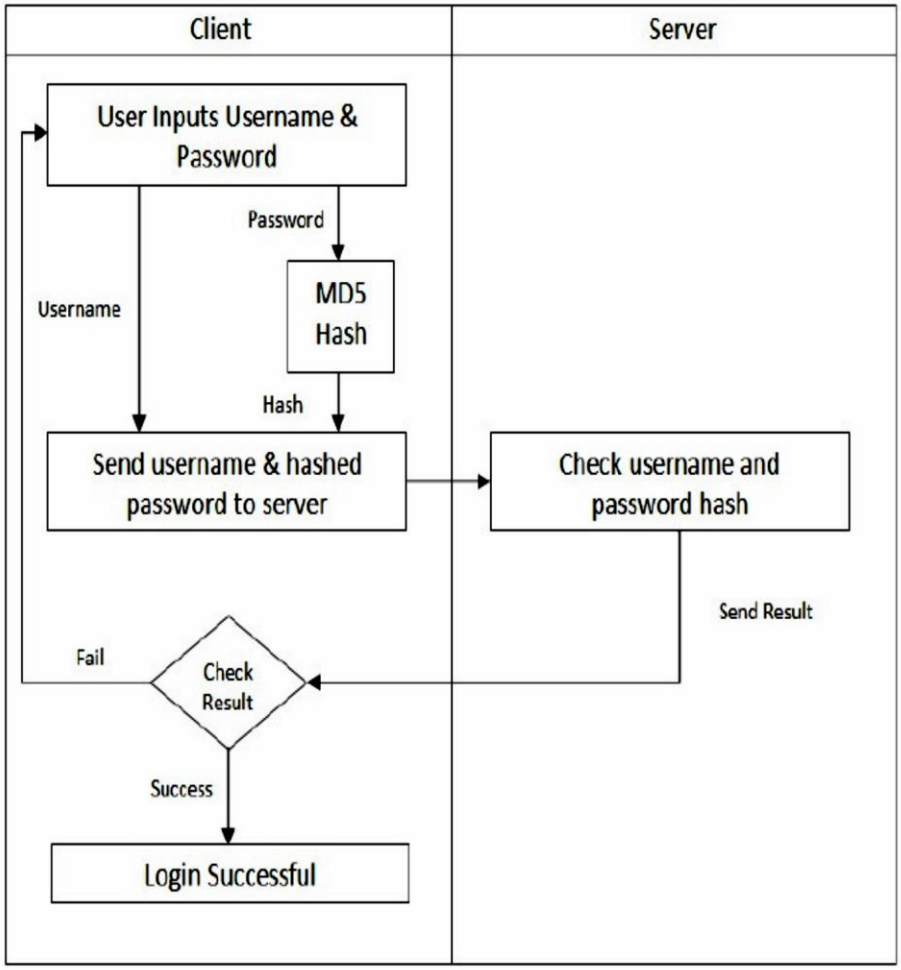

Figure (2) Traditional Authentication System

Proposal

The proposed system uses neural networks within the credit card system to increase reliability and that have not been used previously for any kind of credit cards (VISA Cards, Master Cards...etc) for the purpose of increasing security in the transfer of funds between the user(customer) and the server.

This section explains the logical design of the proposed system; it also explains in details the proposed system execution using the client –server technology in details.

The proposed system contains three main processes which are:

1. Login to the Website(using credit card username).
2. Registration (server side).
3. Authentication (both client and server sides).

The general algorithm of the proposed system:

Input: Credit card information (user name only)

Output: Login to the Website to transfer the funds.

Process:

Step1: the user send his/her (user name,(y, z)) to the server.

Step2: The server receives the information and stores it in a database

Step3: the server send (x) to the user.

Step4 (proposal): client and server sides apply feed forward neural network.

Step5: client and server both XOR's the output of the FFNN

Step6: the client sends the output of his/her calculation to the server.

Step7: the server checks the results (client and server results).

Step8: if both results are equal then authentication is successful.

Step9: apply registration to the Website.

End.

The basic steps of our proposed system between client and server are shown in figure (3).

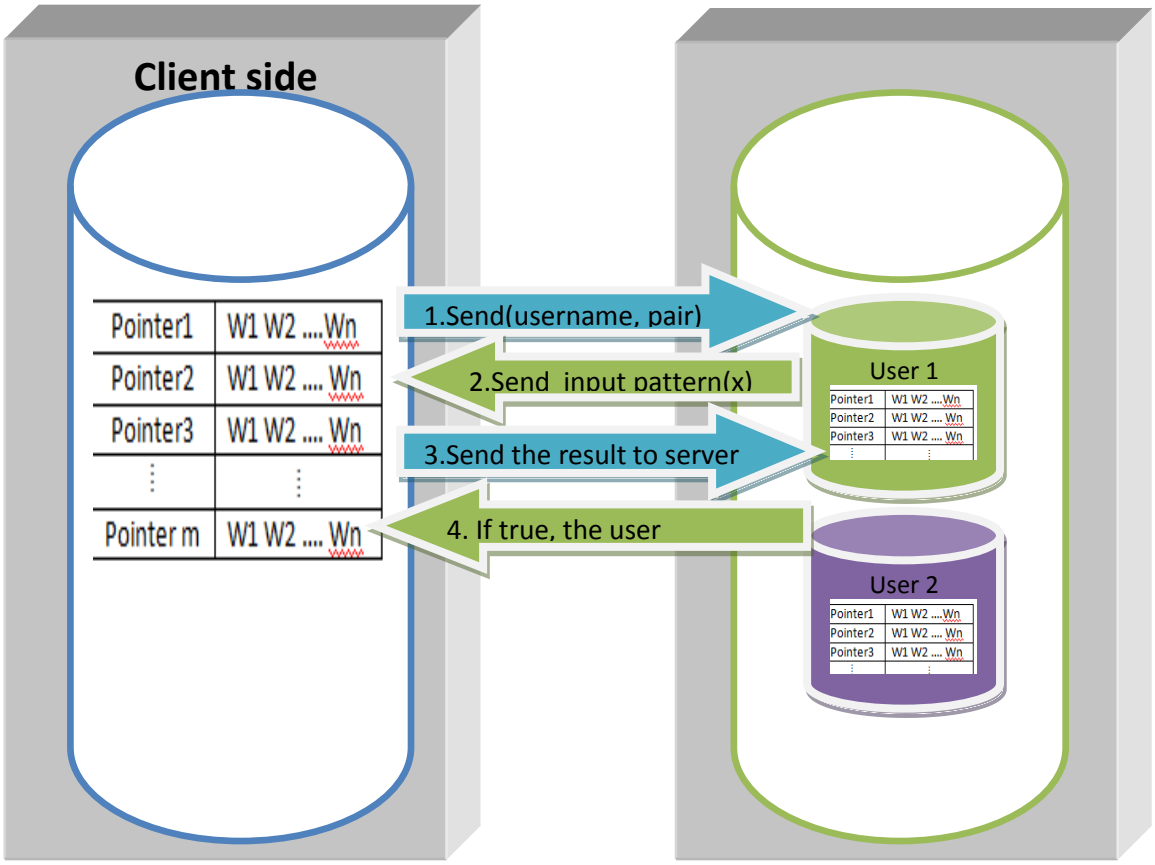

Figure (3) basic steps between client and server

Simulated Design

In this section, to explain the implementation of the proposed system we will focus on display the basic steps between client and server side.

Client side:

1. Has a large database containing single layer feed forward NN with a large number of weights ordered in arrays and the value of weights in these arrays differ from one array to another and must periodically updated in client and server side to increase authentication process.

2. The user selects random two values (pair) which define two pointers each one of these pointers point to one dimensional array containing the weights.
3. The user sent (username, pair).
4. The user receive from the server the input pattern(x),convert to binary.
5. The user calculates input(x) to the selected neural networks (the pair) and store the result after three iteration of NN.
6. Convert each result to binary.
7. XOR the result of the first NN with the second one.
8. Send the result to the server.

Server side

1. In other hand the server also has the same huge database which resides in a very secret place.
2. Each user has its own fields in the database containing the same single layer feed forwards NN with the same large number of weights ordered in arrays and the value of weights in these arrays differ from one array to another
3. The server receives (username, pair)
4. The number of iteration is one iteration for each neural network
5. The server generates the input pattern randomly (x)and send it to the user
6. Convert input(x) to binary value.
7. The server begin calculate input(x)to the selected neural networks (the pair) and get the result after one iteration of NN.
8. Convert each result to binary.
9. XOR The result of the first single layer feed forward NN with the second one
10. The server receives the result from the client side.
11. Compare the result from the user with its result. If successful, user is authenticated.

A proposed system registration process is shown in figure (4) from both client side and severs side.

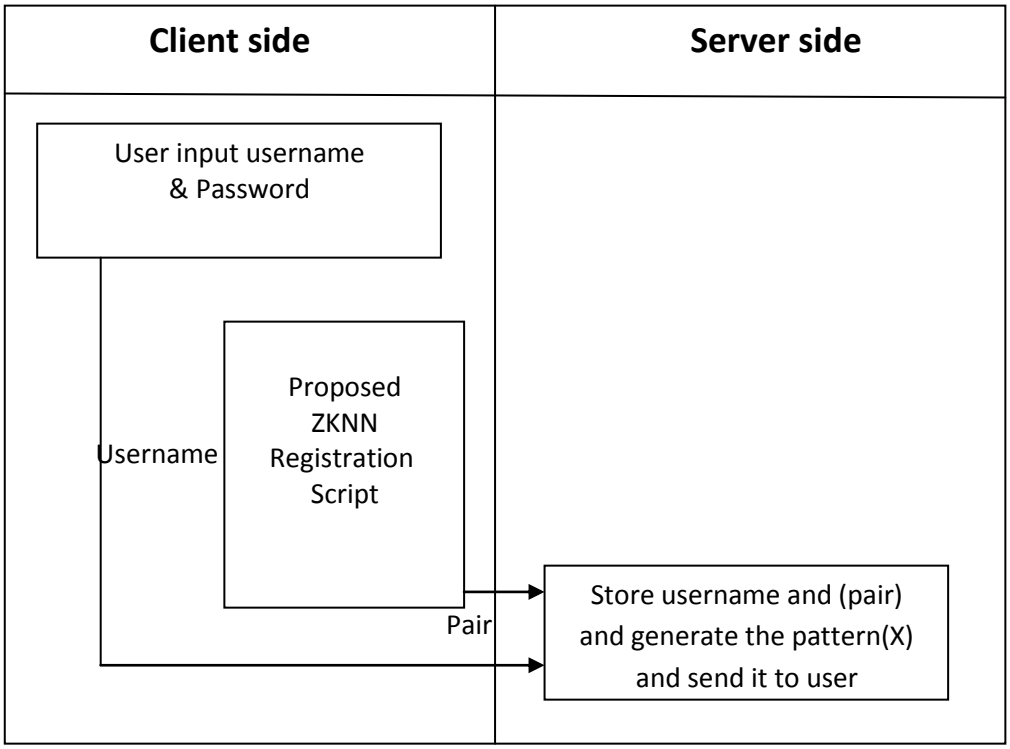

Figure (4) Proposed system registration process

Let's take a very simple example to illustrate the idea:

Suppose client1 want to buy some item from any E-Commerce Website:

1. Client1 must have a large database and this database resides in client and server side. Simple example to illustrate the proposed method: let client1 database contains (5) pointers and (6) weights for each pointer as shown below:

pointers	weights					
1	4.3	0.12	0.6	0.19	3.22	-0.31
2	-0.03	1.24	0.67	0.99	-0.11	0.44
3	0.41	-0.33	0.82	0.32	2.1	0.77
4	1.24	0.003	0.19	0.33	0.68	-1.9
5	-0.88	0.05	0.1.31	0.09	1.12	0.08

2. Select two pointers randomly. Let be (3,1)
3. send (client1 ,(3,1))
4. Server receive these values and generate random number (x), let be x=17
5. sever send (x=17) to client 1 convert it to (6) bits binary value, 17=010001
6. client and server begin calculate (y) for pointer 3 and pointer 1.
   y3 = (1*0.41)+(0*-0.33) + (0*0.82) + (0*0.32) + (1*2.1) + (0*0.77)
   = 0.41 + 2.1 = 2.51= 3 = 000011
   y1= (1*4.3) + (0*0.12) + (0*0.6) + (0*0.19) + (1*3.22) + (0*-0.31)
   = 4.3 + 3.22 = 7.52 = 8 = 001000
7. XOR y3 and y1(000011 XOR 001000)= **001011** send to server
8. Same calculation steps will done in server side and the result is = **001011**
9. The server receive the result from the client
10. Compare user name and the result with its (server) result
11. If true, then the server is authorized.

Implementation of our proposed System

The proposed system was applied on a dataset which containing a number of credit cards (user names and passwords) and compare it with traditional system.

1. Vector NN presents the proposed method.

2. Vector 1, Vector 2, Vector 3, Vector 4…..Vector 9 present the traditional method

The following table (1) and figure (5) illustrates the comparison between Traditional zero knowledge and Proposed method using NN over statistical measures to calculate the performance:

Table 1 describes the comparison between Traditional zero knowledge and Proposed method using FFNN Execution

	Traditional zero knowledge	**Proposed method using FFNN**
Vectors	**Vector1, Vector2, Vector3, Vector4**	**Vector NN**
Performance	**24%, 15%, 4%, 2%**	**90%**
Complexity	**20%, 3%, 15%, 0%**	**88%**
Security	**56%, 27%, 4%, 23%**	**86%**
Speed of Execution	**34%, 24%, 0%, 3%**	**85%(one iteration)**
Authentication	**42%, 11%, 10%, 0%**	**95%**
Accuracy	**45%, 19%, 5%, 5%**	**82%**

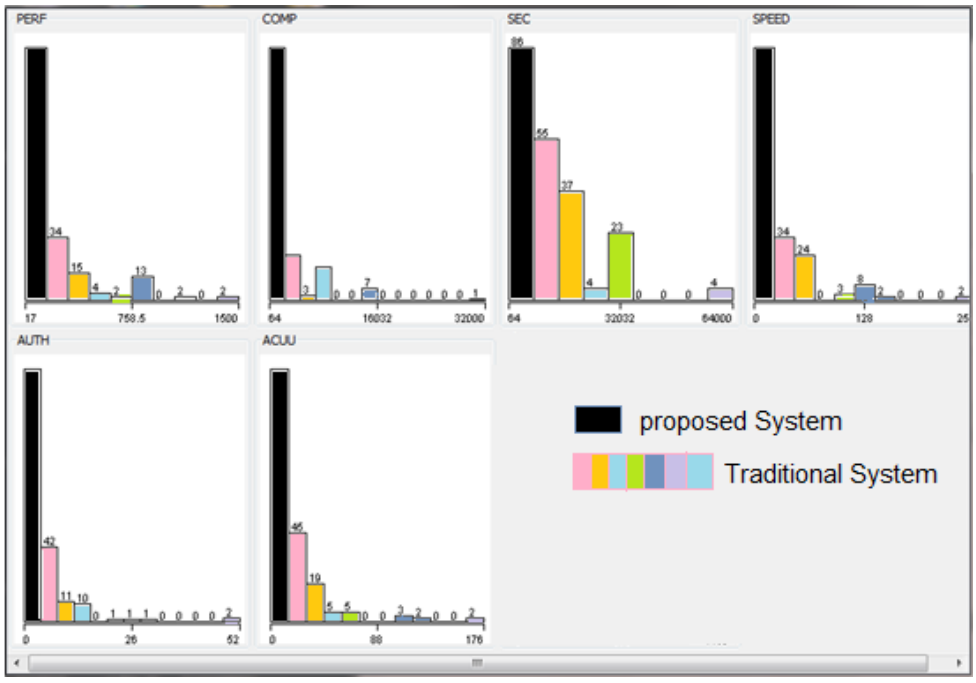

Figure (5): comparison according traditional statistical mean, variance, and standard deviations.

The table above included many important points such as:

- The performance of the proposed method is very good in comparison to the traditional method.
- The proposed method is more complex than its counterpart.
- The proposed method has the highest level of security.
- The speed of execution is lower than the traditional method if we are use the FFNN for one iteration only, otherwise; if we use the FFNN for ten iteration or more the speed will be mirrored.
- The authentication of the proposed method is higher than the traditional method.
- The accuracy of the proposed method is higher than the traditional method.

Conclusion and Future Works

This research reached the following points:

1. Web log is the intrinsic factor in securing web applications, since it present first step in security model of web.
2. Traditional methods with Zero-knowledge protocols very attractive since it secure and prevent leaking of information. But suffer from weak in critical points such as accuracy. Supporting Zero-knowledge protocols with ANN make it more accurate that due to ANN ability for training to avoid new events in login that may decrease accuracy of traditional Zero-knowledge.
3. Proposal increase computational power, ANN is a universal function approximated. The proof is not constructive regarding the number of neurons required or the settings of the weights.
4. Proposal increase complexity, artificial neural network models have a property called 'complexity', which roughly corresponds to the amount of information can be stored in the network, it's application, and ability to model any given function.

This shows that the proposed method is more powerful in terms of security and we suggest for future works to use other complex artificial intelligence methods.

References

1. Annarita Giani, **"Identification With Zero Knowledge Protocols"**, SANS Institute reading room, 2010.

2. Interactive Proofs & Zero Knowledge URL http://www.msri.org/publications/ln/msri/2000/crypto/dwork/3/index.html

3. Hannu A. Aronsson, **"Zero Knowledge Protocols and Small Systems",** Department of Computer Science, Helsinki University of Technology, 2007.

4. Lum Jia Jun, Brandon," **Implementing Zero-Knowledge Authentication with Zero Knowledge (ZKA_wzk)**", The Python Papers Monograph 2: 9 Proceedings PyCon Asia-Pacific, 2010.

5. Siba K. Udgata, Alefiah Mubeen and Samrat L. Sabat, **"Wireless Sensor Network Security model using Zero Knowledge Protocol",** Department of Computer & Information Sciences University of Hyderabad, IEEE ICC proceedings, 2011.

6. Enrique Castillo. **"A Very Fast Learning Method for Neural Networks Based on Sensitivity Analysis"**, Department of Applied Mathematics and Computational Sciences University of Cantabria and University of Castilla-La Mancha, Journal of Machine Learning Research 7 /1159–1182, Spain, 2006.

بطاقات الائتمان الأكثر ذكاء والأكثر أمنية باستخدام الشبكات العصبية وبروتوكول المعرفة الصفرية

م.د. عبير طارق
Abeer282003@yahoo.com
الجامعة التكنولوجية – قسم علوم الحاسوب

المستخلص:

يهدف هذا البحث الى تنفيذ مبدأ المعرفة الصفرية المستخدمة في تطبيقات الويب واستخدامها في الشبكات العصبية ذات التغذية الأمامية. تم استخدام الشبكات العصبية عوضا عن بقية طرق الذكاء الاصطناعي مثل الخوارزميات الجينية، خوارزميات التجمعات الذكية، والتعلم بالماكنة لغرض تحسين طريقة المعرفة الصفرية بسبب عشوائيتها وموثوقيتها العالية. الطريقة الجديدة المقترحة تم مقارنتها بالطريقة التقليدية من حيث الخصوصية، الموثوقية، الدقة والسرعة. ولقد تم ملاحظة ان الطريقة المقترحة اكثر موثوقية وسرية من نظيرتها في تطبيقات الويب وخاصة في التطبيقات التي تتطلب استخدام البطاقة الائتمانية والتي تطالب بحماية قوية جدا ما بين الخادم والعميل من أجل كسب ثقة العميل في هذه المواقع على شبكة الأنترنت وحمايتهم من القرصنة.

الكلمات الرئيسية: المعرفة الصفرية، الشبكات العصبية، تقنية الخادم والعميل