IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-10 E-ISSN: 2347-2693

Securing Vehicle Numbers using Artificial Neural Networks

E. Narwal[1*], S. Gill[2]

[1*] Department of Mathematics, Maharshi Dayanand University, Rohtak, India
[2] Department of Mathematics, Maharshi Dayanand University, Rohtak, India

*Corresponding Author: ekta_narwal@yahoo.com, Tel.: +91-9468266661

Available online at: www.ijcseonline.org
Received: 29/Aug/2017, Revised: 14/Sep/2017, Accepted: 26/Sep/2017, Published: 30/Oct/2017

***Abstract*—** In automatic gate entry system security of vehicle numbers stored in the computer system is a crucial issue because in some parking areas only few important vehicles are permitted. The numbers of permitted vehicles are stored in computer systems. Cryptography based security systems are used to secure these numbers, but in modern environment this type of secure data can also be hacked and altered by the unauthorized users. In order to solve these vulnerable problems, in this paper, we try to create a security mechanism by using Artificial Neural Network (ANN) to protect the data stored on a computer device against unauthorized access. In place of saving vehicle numbers in actual form or in form of alphanumeric data into a text file, we store them in the form of network parameters and these parameters are generated by the back propagation algorithm of ANN using neural network toolbox of MATLAB. This type of security approach is the newest form of cryptography and also cracking of these types of parameters is not possible till today.

***Keywords*—** Artificial Neural Network; Back Propagation; Cryptography; Automatic Gate Entry System**.**

I. INTRODUCTION

The security of information is the one of the biggest problem in the modern computer systems. In automatic gate entry systems all the information related to the vehicles which are allowed to enter the buildings or the V.I.P. entries are stored in the computer systems. So it is the prime task to secure that file in which these vehicle numbers are stored because if they were hacked then the hackers can get information about these V.I.P. entries. To secure that type of files from unauthorized access the encryption techniques are used.

Encryption is the process of converting data into some other forms to make it sniffing-proof. Here we present an encryption system using back propagation algorithm of artificial neural network. In place of saving vehicle numbers into the computer system we save them in the form of weights and these weights are created during the learning process of artificial neural network. In an artificial neural network whenever we try to train the network with some input and target values some random weights are generated by the network. If some unauthorized users will hack these weights he will not be able to generate the original data from these weights. [1] This type of technique can be used in saving private keys used to secure messages during vehicular communication.

1.1 Artificial Neural Network

Artificial neural network (ANN) is based on the neurons, which in turn called the processing units of the network. These neurons communicate with each other through signals and the connections between neurons have some weights associated with them. There are basically three types of neural network architectures, in our research, we used multi-layer feed forward network using back propagation model. Here, the input layer contains 10 neurons with 2 hidden layers. Each neuron is related to the first character of the vehicle number. So we trained our network with 9 vehicle numbers and each vehicle number contains 10 characters and each character is converted into 8-bit pattern. So each number is converted into 80 bit pattern. The input and output values of the network are represented as I_i and O_k for ith neurons in the input layer and kth neuron in the output layer respectively. [2]

Section- I contains the introduction part, which involves brief description of the problem and the cryptography approach with ANN. Section- II contains the simulation process that we are going to use in our design. Section- III contains whole experimental setup of our problem solution with input, output patterns and algorithm. Section- IV contains the results and observations from the experiment and the last Section- V concludes the whole result.

II. THE PROPOSED SIMULATION

The basic network architecture is a multi-layer feed forward network, based on model of Back Propagation. The neurons of one layer are fully connected with the neurons of another layer and the input patterns of each unit are the sum of output patterns of the previous layer multiplied by weight matrix.

Fig.1 shows this type of network architecture. The network must be trained the known set of input and expected output values. After training we get network parameters like network output and error values and also we get weight matrix. These weight values are produced during the training process by reducing the error values through back propagation model and this is the basic idea behind our experiment.

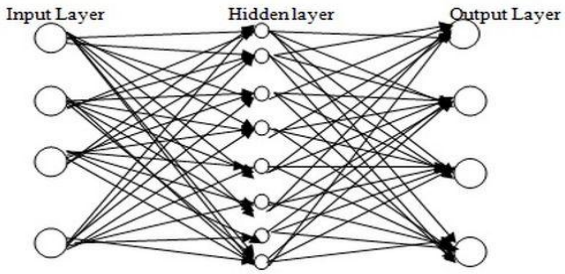

Fig. 1 Architecture of Multi-Layer feed forward Neural Network [3]

III. EXPERIMENTAL DESIGN

The experiment has training model Back Propagation Network, which is a supervised learning model containing three layers: Input layer, Hidden layer and Output layer. Vehicle numbers are used as the training patterns. The network has one input layer having 10 neurons with two hidden layers having 30 neurons, each , there is one output layer having 10 neurons corresponding to 10 neurons in the input layer and in this network model each node of input and output layer represents 9 columns each contains 8 bits pattern. Table I shows the vehicle numbers used in our research. Each vehicle number consists of 10 alphanumeric characters and each character is changed into 8-bit binary number. Table-1 also shows the training patterns. Minimum error exists in the network is 0.001 and the initial weights are between 0 and 1.

Table-1 Set of Input and Target Values Used in the Network

Training Patterns		
Vehicle Numbers	Input Patterns	Output Patterns
HR12DE1433	01001101-01001000-00110001-00110010-01000100-01000101-00110001-00110100-00110011-00110011	01001101-01001000-00110001-00110010-01000100-01000101-00110001-00110100-00110011-00110011
HR 01AB1234	01001101-01001000-00110000-00110001-01000001-01000010-00110001-00110010-00110011-00110100	01001101-01001000-00110000-00110001-01000001-01000010-00110001-00110010-00110011-00110100
HR4CAF4943	01000100-01001100-00110100-01000011-01000001-01000110-00110100-00111001-00110100-00110011	01000100-01001100-00110100-01000011-01000001-01000110-00110100-00111001-00110100-00110011
HR02AC5566	01001101-01001000-00110000-00110010-01000001-01000011-00110101-00110101-00110110-00110110	01001101-01001000-00110000-00110010-01000001-01000011-00110101-00110101-00110110-00110110
HR11AD4242	01001011-01001100-00110001-00110001-01000001-01000100-00110100-00110010-00110100-00110010	01001011-01001100-00110001-00110001-01000001-01000100-00110100-00110010-00110100-00110010
HR01AE8017	01001011-01001100-00110001-00110001-01000001-01000100-00110100-00110010-00110100-00110010	01001011-01001100-00110001-00110001-01000001-01000100-00110100-00110010-00110100-00110010
HR26CH8421	01001101-01001000-00110000-00110001-01000001-01000101-00111000-00110000-00110001-00110111	01001101-01001000-00110000-00110001-01000001-01000101-00111000-00110000-00110001-00110111
HR11CK0001	01000100-01001100-00110001-001100010-1000011-01001011-00110000-00110000-00110000-00110001	01000100-01001100-00110001-001100010-1000011-01001011-00110000-00110000-00110000-00110001

HR99BJ6662	01001000-01010010-00111001-001110010-1000010-01001010-00110110-00110110-00110110-00110010	01001000-01010010-00111001-001110010-1000010-01001010-00110110-00110110-00110110-00110010

3.1 Basic algorithm followed in our experiment is as follows:

Step1: First read the vehicle numbers from the file.
Step2: Convert that vehicle number into binary form.
Step 3: Initialize these vehicle numbers as Input and target values in the feed forward neural network, also initialize some random weights between 0 and 1.
Step 4: For i=1, 2, -----n
Set activation of input unit I_i
Step 5: For j=1, 2, ------p

$$H_{in_j} = z_{oi} + \sum_{i=1}^{n} I_i \, z_{ij}$$

$$H_j = \frac{2}{(1 + \exp(-2 * H_{in_j}))} - 1$$

Step 6: k=1, 2, -------- m

$$O\_in_k = y_{ok} + \sum_{j=1}^{p} H_j \, y_{jk}$$

$O_k = O\_in_k$

IV. RESULTS AND OBSERVATIONS

The cryptographic keys are used to make the file more secure. The same key must be used to decrypt the data. This means that we have to either memorize the key or store it somewhere. For this we first processed the input pattern set and inserted the input pattern set in the network and trained the network using Back Propagation model. Then, calculated the activation values and output values using Gradient Descent method. Weights were adjusted so that the sample input pattern converges to the desired output pattern. At last weights were updated and recorded. The recorded weights are now used in place of the original data. The original file is now deleted from computer memory because original data are now memorized in the network and the weights obtained from the network are stored in place of that file.

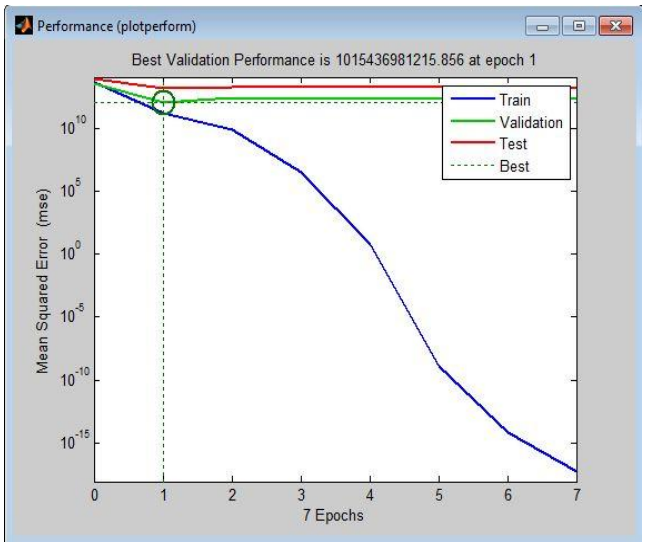

Fig. 2 Graph of Network Performance during Process of Memorizing Pattern

Table- 2 Memorized Vehicle numbers and Unknown Vehicle numbers

		Input	Output
Test Cases	HR02AC 5561	01001101-01001000-00110000-00110010-01000001-01000011-00110101-00110101-00110110-00110111 (Unknown Data)	1001098.1932-1001048.8944-109997.6991-110020.6425-1000000.8044-1000014.2225-109838.9269-142565.0404-110110.4985-110110.7994
	HR02AC 5566	01001101-01001000-00110000-00110010-01000001-01000011-00110101-00110101-00110110-00110110 (Known Data)	01001101-01001000-00110000-00110010-01000001-01000011-00110101-00110101-00110110-00110110

Here in Table –2 we have seen that if we enter any test case from the given input set of vehicle number, then the output of the network will remain the same because the network is now remembered the vehicle number, but if we enter any new vehicle number then the output will not remain same. Fig.2 shows the graph of performance obtained during network training.

V. CONCLUSION

Network parameters are generated during the learning process. Now the actual file containing vehicle numbers is replaced by these parameters and then actual file is deleted. After this process, we can get a more secured set of data. So artificial neural network is a powerful tool with the help of which we can easily perform these types of cryptographic activities to make stored data more secure. The weights are still stored in the system, but still they will not leak any type of information to the unauthorized users. Better results can be obtained by using more algorithms of neural networks and also this type of cryptographic techniques can be used in many other fields like securing digital signatures and the private keys used for encryption and decryption of messages in various mechanisms.

References

[1] K. Topel, A. Rane, R. Rahate, S.M.Nalawade, *Encryption and Decryption using Artificial Neural Network*, International Advanced Research Journal in Science, Engineering and Technology, Vol. **2**, No. **4**, pp. **81-83**, **2015**.

[2] N. Agarwal, P. Agarwal , *Use of Artificial Neural Network in the Field of Security*, MIT International Journal of Computer Science & Information Technology, Vol. **3**, No. **1**, pp. **42–44, 2013**.

[3] A. S. N. Chakravarthy, P. S. Avadhani, *A Probabilistic Approach for Authenticating Text or Graphical Passwords Using Back Propagation*, IJCSNS International Journal of Computer Science and Network Security, Vol.**11,** No.**5**, pp. **242-251, 2011**.

[4] Khalil Shihab, *A Back Propagation Neural Network for Computer Network Security*, Journal of Computer Science, Vol. **2** No.**9**, pp. **710-715, 2006**.

[5] M. Udi ,*A simple scheme to make passwords based on one-way function much harder to crack*, Computer Security, Vol. **15**, No. **2**, pp. **171–176**, **1996**.

[6] G. Horng, *Password authentication without using password table*, Inform. Processing Lett., Vol. **55**, pp. **247–250**, **1995**.

[7] Robert Biddle, Sonia Chiasson, P.C. van Oorschot , *Graphical Passwords: Learning from the First Twelve Years, Technical Report TR-11-01*, School of Computer Science, Carleton University, **2011**.

[8] Wei-Chi Ku, *Weaknesses and Drawbacks of a Password Authentication Scheme Using Neural Networks for Multiserver Architecture*, IEEE Trans. On Neural Network, Vol. **16**, No. **4**, **2005**.

[9] M. S. Obaidat and D. T. Macchiarolo, *An on-line neural-network system for computer access security*, IEEE Trans. Ind. Electron., vol. **40**, pp**. 235–**242, **1993**.

[10] B. Damgard, *A design principle for hash functions, In Advances in Cryptology*, CRYPTO'89. pp. **416-427**, **1989**.

[11] A. Jr. Evans, W. Kantrowitz, and E.Weiss, *A user authentication scheme not requiring secrecy in the computer*, Communications of the ACM, vol.**17**, pp. **437-442**, **1974**.

[12] V. S. Dhaka, M. Rao, M. P. Singh, *Signature Verification on Bank Checks Using Hopfield Neural Network*, Karpagam Journal of Computer Science, ISSN-0973-2926, Vol.**3** No.**4**, pp. **1131-1140, 2009.**

[13] V. Singh, K. Mahajan, *VANET and its Security Issues- A Review*, International Journal of Computer Science and Engineering, Vol. **4**, Issue **10**, pp. **59- 64, 2016.**

Authors Profile

Dr Sumeet Gill has Bachelor and Master degrees in High Energy Physics and Computer Science. He is currently working as Assistant Professor in Department of Mathematics, Maharshi Dayanand University, Rohtak. He has awarded Ph.D. degree in 2010. He has published 45 international publications in various journals. He has 17 years of teaching experience and 12 years of Research Experience.

Ms. Ekta Narwal pursed Bachelor of Science in year 2008 and Master of Science in year 2010 from Maharshi Dayanand University, Rohtak. She is currently pursuing Ph.D. from Department of Computer Science and Application and currently working as Assistant Professor in Department of Mathematics, Maharshi Dayanand University, Rohtak since 2012. She has 6 years of teaching experience.

