MULTIVARIABLE SYSTEM SECURITY USING ANN IN THE LIBRARIES : DESIGNING AND DEVELOPMENT

Ranjana R K Aziz-ur-Rahman Makandar

Abstract

Owing to the developments in Science and technology, the new millennium has experienced severe impact of information and communication technology on each and every walk of life irrespective of business, industry, banking sectors, academic including information industry. With an urge on the part of Librarians to provide techno-based information services, the libraries have undergone sea of changes moving towards digital world. In this context, the virtual library needs to strengthen their networking architecture, security and proper maintenance. An attempt has been made to develop software using Artificial Neural Network for security management of Libraries serving in the networked environ using MATLAB. Further highlighted the importance of ANN and provided hierarchy of security using ANN technology and explained the methodology of security protection to the DBMS especially Library software working in different platforms.

Keywords : Library Networking, Artificial Neural Network, Feed Forward Architecture, Library Security.

1. Introduction

There has been tremendous impact of Information and Communication technology (ICT) on Library and Information Centers, which is affecting every facet of its activities and services. In this information rich society, the impact of ICT has been accepted by the Libraries and has been adopted in the routine activities and services. Further, adoption of Library software's in the Libraries with an objective to automate the in-house activities and extend techno-based information services has led to establishment of networking. Thus, the Library and Information centers are in the phase of networking the library activities and services with a view to improvise its services and meet the timely information needs of the user community in this Internet world.

Confidentiality is the concealment of information or resources. The need for keeping information secret arises from the use of computers in sensitive fields such as government and information industry. Access control mechanisms support confidentiality. One access control mechanism for preserving confidentiality is cryptography, which scrambles data to make it incompressible.

"A security policy is a statement of what is, and what is not allowed." A security mechanism is a method, tool, or procedure for enforcing a security policy. The heart of any security system is people. This is particularly true in computer security, which deals mainly with technological controls that can usually be bypassed by human intervention. For example, a computer system authenticates a user by asking that user for a secret code; if the correct secret code is supplied, the computer assumes that the user is authorized to use the system. If an authorized user tells another person his secret code, the unauthorized user can masquerade as the authorized user with significantly less likelihood of detection.

A neural network is a system composed of many simple processing elements operating in parallel whose function is determined by network structure, connection strengths and processing performed at computing elements or nodes [1]. Various types of neural networks are explained and demonstrated, applications of neural networks are described and a detailed historical background is provided. The connection between the artificial neuron and the biological (mammalian brain) neuron is also investigated and explained. Finally the mathematical models involved are presented to solve our present work.

The US Department of Defense has issued specific guidelines for password selection and management [2] Jermyn, Mayer, Monrose, Reiter, and Rubin use the graphical capabilities of many systems to generate passwords [3]. Passwords are an example of an authentication mechanism based on what people know; the user supplies a password, and computer validates it. If the password is the one associated with the user that user's identity is authenticated. If not, the password is rejected and the authentication fails.

Nothing prevails but maintenance becomes obligatory for the effective functioning of library system in the long run and as such proper maintenance and effective control over the databases in the library is of utmost significance. An attempt has been made to develop and design security system for networking, computer security on confidentiality and integrity.

2. Objectives of the Study

The present work emphasizes on the designing and developing of a multivariable system security using ANN in the libraries. The authentication to the system can be provided by the password. This is one of the means to provide security to the system. But this means has the following deficits:

1. Password becomes public.
2. Guessing of password is possible.
3. Password theft is possible.

Our paper proposes a unique and new solution to overcome this problem by using artificial neural network. The protection provided to the software/system is providing a unique unbreakable password facility with following features.

Several multi-variables are selected for providing more security to the system like:

1. To avoid the 'dictionary attack' of guessing the password by repeated trials and errors.
2. By increasing complexity of the password.
3. Passwords have the fundamental problem that they are reusable. There fore authentication is given in such a way that the transmitted password changes each time.
4. By allowing only limited trials.
5. By allowing letters, numbers and special characters of any length.
6. By restricting the time constraint to enter the password.

3. Artificial Neural Network (ANN)

Biologists have studied biological neural networks for many years. The human brain is such a network. Discovering how the brain works has been an ongoing effort that started more than 2000 years ago. An information about the function the brain was accumulated, a new technology emerged as the quest for an

“Artificial Neural Network” started. The brain processes information super quickly and super accurately. It can be trained to recognize patterns and to identify incomplete patterns.

For example, even in a noisy football stadium with many thousands of people, we can still recognize a friend from a far or distinguish voice from the noise. So here we surely wish the duplicate the brain and create a brain like machine. Hence, if we manage to build a machine, an Artificial Neural Network that emulate the human brain, even at only 0.1% of its performance.

While designing ANN we should be concerned with the following :

1. Network topology
2. Number of layers in the network
3. Number of neurons or nodes
4. Learning algorithm to be adopted
5. Network performance
6. Degree of adaptability of the ANN (i.e. to what extent the ANN is able to adapt to itself after training).

A Neural network’s ability to perform computations is based on the hope that we can reproduce some of the flexibility and power of the human brain by artificial means. Network computation is performed by a dense mesh of computing nodes and connections. They operate collectively and simultaneously on most on most or all data inputs. The basic processing elements of neural networks are called artificial neurons, or simply neurons. Often we simply call them nodes. Neurons perform as summing and nonlinear mapping junctions. In some cases they can be considered as threshold units that fire when their total input exceeds certain bias levels. Neurons usually operate in parallel and are configured in regular architectures. They are often organized in layers, and feedback connections both within the layer and toward adjacent layers are allowed. Each connection strength is expressed by numerical value called ‘weight’, which can be modified.

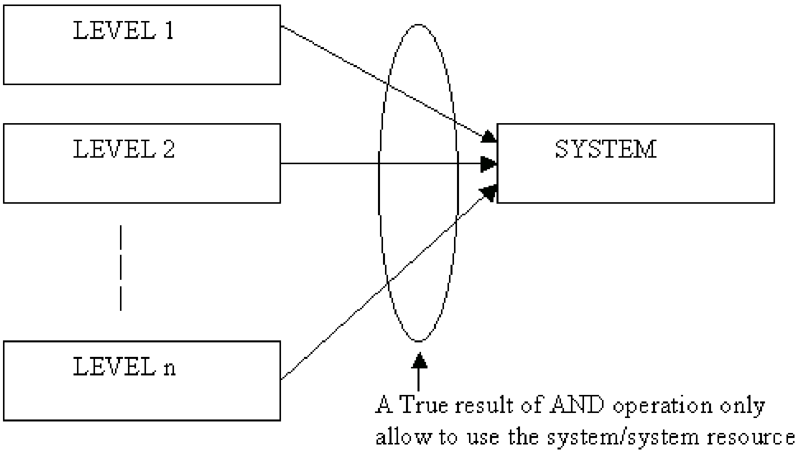
There are several technologies that are available for protecting the system, and provide security to the systems. Out of available technologies ANN is found to be the best because of the following reasons and is opted in the present work.

Neural network architectures are strikingly different from traditional single-processor computers. Traditional Von Neumann machines have a single CPU that performs all of its computations in sequence [4]. A typical CPU is capable of a hundred or more basic commands, including additions, subtractions, loads, and shifts. The commands are executed one at a time, at successive steps of a time clock. In contrast, a neural network processing unit may do only one, or, at most, a few calculations. A summation function is performed on its inputs and incremental changes are made to parameters associated with interconnections. This simple structure nevertheless provides a neural network with the capabilities to classify and recognize patterns, to perform pattern mapping, and to be useful as a computing tool [5].

The processing power of a neural network is measured mainly be the number of interconnection updates per second. In contrast, Von Neumann machines are benchmarked by the number of instructions that are performed per second, in sequence, by a single processor. Neural networks, during their learning phase, adjust parameters associated with the interconnections between neurons. Thus, the rate of learning is dependent on the rate of interconnection updates [6].

4. Hierarchy of Security Using ANN

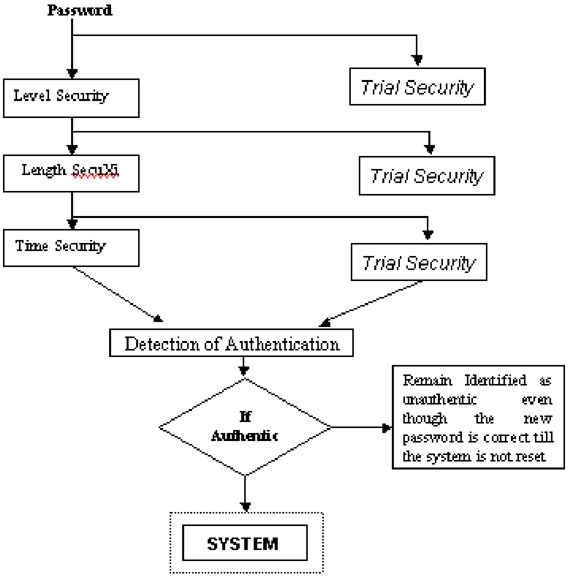
Authentication methods can be combined or multiple methods can be used to make the job of hackers impossible or difficult. By providing several levels of hierarchical setting the system it is possible to provide good security to the system or system resources.



A True result of AND operation only allow to use the system/system resource

Figure 1: Hierarchy of security using ANN

Levels of Security (Figure 2: Flow diagram representing Processing)


Password
Level Security
Trial Security
Length SecuXi
Trial Security
Time Security
Trial Security
Detection of Authentication
If Authentic
Remain Identified as unauthentic even though the new password is correct till the system is not reset
SYSTEM

5. Implementation of E-Security

The present work uses Neural network architectures depart from typical parallel processing architectures in some basic respects. First, the processors in a neural network are massively interconnected. As a result, there are more interconnections than there are processing units. In fact, the number of interconnections usually far exceeds the number of processing units. State-of-the-art parallel processing architectures typically have a smaller ratio of interconnections to processing units. Besides, parallel processing architectures tend to incorporate processing units that are comparable in complexity to those of Von Neumann machines. Neural network architectures depart from this organization scheme by containing simpler processing units, which are designed for summation of many inputs and adjustment of interconnection parameters.

The two primary attractions that come from the computational viewpoint of neural networks are learning and knowledge representation. A lot of researchers feel that machine learning techniques will give the best hope for eventually being able to perform difficult artificial intelligence tasks. Most neural networks learn from examples, just like children learn to recognize dogs from examples of dogs. Typically, a neural network is presented with a training set consisting of a group of examples from which the network can learn. These examples, known as training patterns, are represented as vectors, and can be taken from such sources as images, speech signals, sensor data, and diagnosis information. The most common training scenarios utilize supervised learning, during which the network is presented with an input pattern together with the target output for that pattern. The target output usually constitutes the correct answer, or correct classification for the input pattern. In response to these paired examples, the neural network adjusts the values of its internal weights. If training is successful, the internal parameters are then adjusted to the point where the network can produce the correct answers in response to each input pattern. Because they learn by example, neural networks have the potential for building computing systems that do not need to be programmed. This reflects a radically different approach to computing compared to traditional methods, which involve the development of computer programs. In a computer program, every step that the computer executes is specified in advance by the network. In contrast, neural nets begin with sample inputs and outputs, and learn to provide the correct outputs for each input. The neural network approach does not require human identification of features. It also doesn't require human development of algorithms or programs that are specific to the classification problem at hand.

Stable network and more security "You are almost not knowing what you are actually doing when using back propagation" it has pretty much success on practical applications and is relatively easy to apply.

It is for the training of layered (i.e., nodes are grouped in layers) feed forward (i.e., the arcs joining nodes are unidirectional, and there are no cycles) nets. Back-propagation needs a teacher that knows the correct output for any input ("supervised learning") and uses gradient descent on the error (as provided by the teacher) to train the weights. The activation function is (usually) a sigmoidal (i.e., bounded above and below, but differentiable) function of a weighted sum of the nodes inputs. The use of a gradient descent algorithm to train its weights makes it slow to train; but being a feedforward algorithm, it is quite rapid during the recall phase. By using backpropagation technique password get unbreakable output which will be possible because of the above explained functionality.

This Project takes care of checking of correct password and detection of unauthorized trials. Unauthorized trials can be detected by providing a limited number of trials, time delay in entering the password check. After unauthentication is detected reset code is to be given, to change the all passwords otherwise access is denied for the authorized user also.

6. Selection of Learning Algorithm

Supervised learning is required for pattern matching and Generalised Data Rule (GDR) is used in so called Error Back Propagation Algorithm (EPBA) is the most popular of the supervised learning techniques used to train a feed forward multi-layered artificial neural network. The EBPA used gradient descent to achieve training by error correction, where network weights are adjusted to minimize error based on a measure of the difference between desired and actual feed forward neural network output. Desired input/ output behaviour is given in the training set where the input and the target values are predefined.

As the name “Error Back Propagation” itself suggests, the generated error signal at the network output is propagated backwards. The algorithm tries to minimize an error function, starting from the output layer towards the input layer, which is defined as the mean square of the generated error signal over the set of training data. We require error function to adjust the weights in a proper direction, as to provide maximum co-relation with respect to the inputs, so the network can converge towards a state that allows all the training patterns to be encoded, so this algorithm opted for training ANN in this project.

7. Test & Implementation

After getting the unique values from the user as a user identification, password and reset code, which are mapped by ANN corresponding to specified personal/system/Reset identification, the test trail is conducted by applying test string at different storage of security level as the system asked. After converting them into the binary format, ANN mapped the test string conversion in binary format, ANN mapped the test string to unique value corresponding to that of test string. A equality comparator checked the equality status of this test mapped value to the corresponding value which has been set at the same level of security. If the result of comparator is true then system goes for next test level of pattern identified, false result of comparator declare either unauthentication and seize the system for security purpose, or more for the next trail if the trail conduction is satisfied.

In order to train a neural network to perform some task, we must adjust the weights of each unit in such a way that the error between the desired output and the actual output is reduced. This process requires that the neural network compute the error derivative of the weights (**EW**). In other words, it must calculate how the error changes as each weight is increased or decreased slightly. The back propagation algorithm is the most widely used method for determining the **EW**. This can be easily converted into computerized form.

At the beginning all the inputs are stored in the form character strings, the same are converted into binary form as shown in the following example.

```
tv1=(dec2bin(double(tv1)))’;
```

where tv1 is a variable used to store user password and later it converts it into Binary format. Then we generate random weights by Gaussion Distribution.

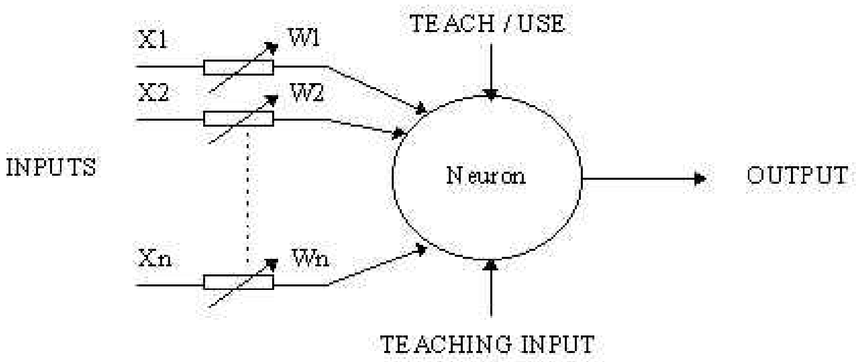


Figure 3: Training input through ANN.

In mathematical terms, the neuron fires if and only if; X1W1 + X2W2 + X3W3 + ... > T

The addition of input weights and of the threshold makes this neuron a very flexible and powerful one. The MCP neuron has the ability to adapt to a particular situation by changing its weights and/or threshold. Various algorithms exist that cause the neuron to 'adapt'; the most used ones are the Delta rule and the back error propagation. The former is used in feed-forward networks and the latter in feedback networks.

```
sum_x2 =x1* wh ;                % finding hidden node values %

x2=1./(1+exp(-sum_x2));         % pass sum value to sigmoid  %
```

Similarly we find output node values, then by calculating the error factors we go for next layer and then to the desired outputs.

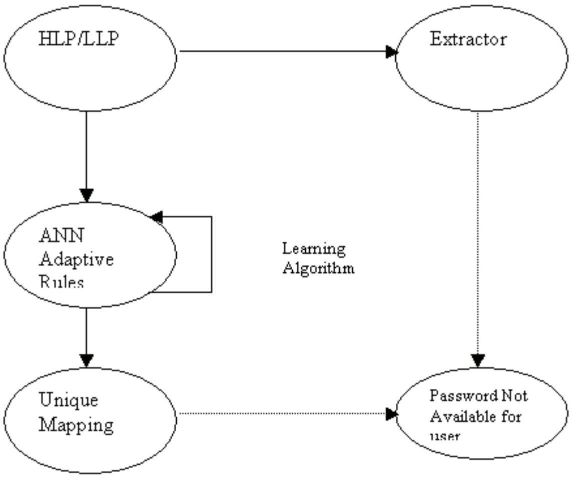


Figure 4: Security protection to the Library software's in the networked environ

8. Conclusion

A system has been developed for software security implementation purpose, which works efficiently for security purposes. Adaptive nature of architecture of ANN is used here efficiently. It is found to be more stable architecture to provide more security to the system. Thus, the role of ANN is very important in determining in this scope of this project, as it provides Non Linear Mathematical function, generates Random Number, provide variable architecture with respect to input, same fixed length output is produced for different length input, even same input also will give different outputs, by applying feed forward back propagation algorithm of ANN the project is developed.

It is a great boon to the Library networked managers to make use of this software for the protection of various DBMS and allied software's being used by libraries in this new millennium. This is up-to the library professionals to make the best of options available in the software in the best interest of the user community and to provide effective information services in the networked environ without disrupting the network architecture.

9. References

1. S.Jojodia and B.Kogan, "Transaction Processing in Multilevel-Secure databases using Replicated Architecture Proceedings of the 1990 Symposium on Research in Security and Privarcy, pp 360-368 (May 1990)
2. Department of Defense, Password Management Guideline, CSC-STD-002-85 (Apr.1985).
3. I. Jermyn,A. Mayer, F.Monrose, M.Reiter, and A.Rubin, "The Design and Analysis of Graphical Passwords Proceeding of the 8th USENIX Security Symposium, pp. 1-14(Aug.1999).
4. Vogel, William, "Minimally Connective, Auto-Associative, Neural Networks", Connection Science, Vol. 6 (January 1, 1994), pp 461.
5. Cross, et, Introduction to Neural Networks", Lancet, Vol. 346 (October 21, 1995), pp 1075.
6. Vogel, William, "Minimally Connective, Auto-Associative, Neural Networks", Connection Science, Vol. 6 (January 1, 1994), pp 461.
7. Rumelhart, D. E. and McClelland, J. L. (1986): Parallel Distributed Processing: Explorations in the Microstructure of Cognition (volume 1, pp 318-362). The MIT Press. (this is the classic one) or one of the dozens of other books or articles on backpropagation.
8. Simon Hykin(1994), "Neural Networks: A Comprehensive Foundaption , New York: Macmillan.
9. Jacek M. Zurda, "Introduction to Artificial Neural System, Jaico Publications, 3rd edition, 1999.
10. Maureen Caudil and Charles Buttler "Naturally Intelligent Systems MIT Press, Cambridge MA, 1990.
11. Daved E. Rumelhard and James L. McClelland, "Paraller Distributed Processing, Vol,:1, MIT Press, Cambridge, MA, 1986.
12. A. Fiorentino and N.Gueoguieva, "Supervised learning based on Multilayer feed forward potential function approach
13. Fundamentals of Artificial Neural Networks, Mohammad, H, Hassoun, Prentice-Hallof India, 1999.
14. Neural Networks And Fuzzy Systems, Bart Kosko, Prentice-Hall of India, 2000

About Author

Ms. Ranjana R K is a research scholar pursuing M.Tech in Computer Science at Khaja Bande Nawaj College of Engineering at Gulbarga with sound academic record of having obtained rank certificate at B.E (Computer Science). Research area of interest are Security through Neural Network, Linux, Networking etc.
E-Mail :

Sh. Aziz-Ur-Rahman Makandar presently working as Assistant Professor in the Department of Computer Science and Engineering at Khaja Bande Nawaj College of Engineering at Gulbarga with teaching experience of 8 years. He has published several research papers at national and international level. His research area lies on image processing.
E-Mail :