www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 2 February 2015, Page No. 10438-10444

Enhancing Data Security in Neural Network Computing Using Biometrics

C.R.Kavitha [1]
[1]Assistant Professor Senior,
Sri Lakshmi Narasimha College of Sciences,
Andhra Pradesh, India
kavithavellore@gmail.com

Abstract: Neural Network most probably known as "Artificial Neural Network (ANN)" is an information processing model, that is analogous to the way the biological nervous systems processes information. Neural networks can be used to extract patterns and detect trends that are too complex to notice by either humans or other computer techniques. In today's network world, maintaining the security of information or physical property is becoming both increasingly important and difficult. From time to time we hear about the crimes of Credit Card Fraud, Computer break in by hackers or security breach in a company or government buildings. In most of these crimes, the criminals were taking advantages of a fundamental flaw in the conventional access control systems. The systems do not grant access to " Who we are ", but give details about " What we have ", such as ID cards, keys, passwords, PIN numbers, or mother's and maiden name. None of these mean are not really define us but rather they merely authenticate us. It goes without saying that if someone steals, duplicates, or acquire these identity then, he or she will be able to access our data or our personal property anytime they want. Recently, developed technology became available to allow verification of "true" individual identity. This technology is based on a field called "BIOMETRICS" with Neural Networks.

Keywords: *Neural Network, Biometrics, Public Key Infrastructure, Cryptography.*

1. INTRODUCTION

Where does intelligence come into view? There are two important ways to answer this difficulty from the point of computational view. One is based on *'Symbolism'* and other is based on '*Connectionism'*. The former approach models intelligence using symbols, the later using connections and associated weights. In contrast to symbolic approach, the neural network approach adopts the brain metaphor, which suggest that intelligence come into view through a large number of processing elements connected together, each performing simple computation. The long term-knowledge of neural network is encoded as a set of weights on connection between units. For this reason, the neural network architecture has been dubbed the connectionist. Analytical neural modeling has usually been pursued in connection with psychological theories and neurophysiological research. The theoretical basis of neural networks was developed in 1943 by the neurophysiologist *Warren McCulloch* of the University of Illinois and the mathematician *Walter Pitts* of the University of Chicago. In 1954 *Belmont Farley* and *Wesley Clark* of the Massachusetts Institute of Technology succeeded in running the first simple neural network.

2. NEURAL NETWORK COMPUTING

Neural Networks are processing devices that are modeled based on the neuronal structure of the mammalian cerebral cortex. A large Artificial Neural Network might have hundreds or thousands of processor units, whereas a mammalian brain has billions/Trillions of neurons. The neural network contains a large number of simple neurons like processing elements and a large number of weighted connected between the elements. The weight on the connections encodes the knowledge of a network. The simplest definition of a neural network was provided by the inventor of one of the first Neurocomputers, *Dr.Robert Hecht-Nielsen* defined as: '*a computing system made up of a number of simple, highly interconnected processing elements, which process information by their dynamic state response to external inputs'*. The intelligence of a neuron network emerges from the collective behavior of neurons, even though each individual neuron works slowly, they can quickly find a solution by working in parallel. The brain naturally associates one thing with another. Thus, the brain-style computation points out a new direction for building an intelligence system, now there are more than one dozen of well-known Neural Network models have been built, such as Back-propagation net, ART, Hopfield net, Boltzman machine etc.,

2.1. The Neural Network Computation Model

The constructions of neural networks are typically organized by Layers. The Layers are of three types: The *Input Layer, Output Layer and Hidden Layer*. These Layers are made up of numbers of interconnected 'Nodes' which contain an Activation function/Activation Range . Patterns are presented to the network via the 'input layer', which communicates to one or more 'hidden layers' where the actual processing is done via a system of weighted 'connections'. The hidden layers then link to an 'output layer' where the answer is output as shown in the following figure.

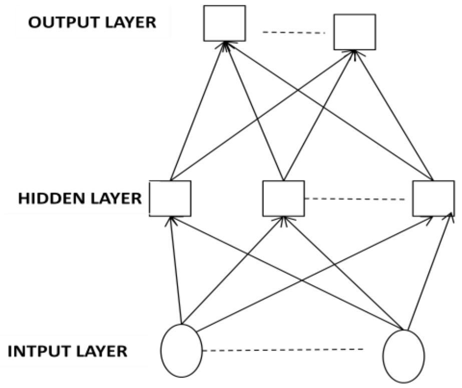

Figure 1: Neural Network Computational Model

2.2 .Computational Advantages offered by Neural Networks

(i) *Knowledge acquisition under noise and uncertainty:* Neural Networks can perform generalization, abstraction, and extraction of statistical properties.

(ii) *Flexible Knowledge representation:* Neural networks can create their own representation by self-organization.

(iii) *Efficient knowledge processing:* Neural nets can carry out computation in parallel. It is known as 'Parallel-distributed processing' or PDP (Rumelhart and McClelland 1986). Special hardware device have been manufactured which exploit this advantage. Training a neural network may be time-consuming, but once it is trained, it can operate very fast.

(iv) *Fault Tolerance:* Through distributed knowledge representation and redundant information encoding, the system performance degrade gracefully in response to faults.

3. NEURAL NETWORK DATA SECURITY

Authentication may be defined as "providing the right person with the right privileges the right access at the right time." In general, there are three approaches to authentication. In order of least secure and least convenient to most secure and most convenient, they are:

- Something you **have** - card, token, key.
- Something you **know**- PIN, password.
- Something you **are** - a biometric.

Any combination of these approaches further heightens security. Requiring all three for an application provides the highest form of security. The analysis concept of security will be differ from person to person as well as from industry to another industry. To setup a security system, we are in position to answer the following questions.

1. How secure is the data?
2. Who is accessing the data?
3. Where is the data?
4. What kind of accessing resources are allowed?
5. How much confidential will your data be?
6. How does Neural Network secure your data?

3.1. Common Mistake and Challenges in Neural Security

1. Failing to use cryptography when cryptographic security is a viable option. Everything should be encrypted by default.

2. Failing to use cryptographically secured protocols when you have a choice. Using FTP, Telnet or HTTP rather than a secured version of these plaintext protocols is simply negligent.

3. Sending sensitive data in unencrypted e-mail and sending passwords, pins or other account data in unencrypted e-mail exposes that data in multiple places.

4. The major challenging role of neural network is that the knowledge learned by a neural network is difficult to interpret.

3.2. Benefits of enhanced security in Neural Network Computing

1. A Neural Network can be viewed as suitable choice for the functional forms used for encryption and decryption operations.

2. A Neural Network is used to construct an efficient system by using a permanently changing key.

3. This type of network has to be trained so that the set of inputs produces the desired set of outputs.

4. Artificial Neural Networks can be used to implement very complex combinational as well as sequential circuits.

5. In data communication systems, data security is of prime concern. So, Artificial Neural Network can be used as a new method of encryption and decryption of data.

3.3. What the Biological Neural Networks are not

1. The Biological neural system do not apply principles of digital or logical circuit.

2. Neither the neurons, nor the synapses are bitable memory elements.

3. No machine instruction or control code occurs in computing.

4. The brain circuits don't implement recursive computation and are thus not algorithmic.

5. Even on the highest level, the nature of information processing is a different in the brain and in digital computers.

4. ENHANCING SECURITY BY COMBINING BIOMETRICS TO CRYPTOGRAPHY

In ancient Greek Bios standard for 'Life' and Metron standard for 'Measure', and the more expansive definition of biometrics is: the study of methods for uniquely recognizing humans, based upon one or more intrinsic physical or behavioral traits. As a category of authentication method it's used as discriminating factors and some personal characteristic such as Fingerprints, voice patterns, Signature, Typing styles and so on. Since such personal characteristics are virtually unique of the individual. The Biometrics is the most promising approach in the field of user identification. Differently from password, keys and cards, personal characteristic are a part of the individual. So they can't be lost, stolen, forgotten or transferred. A combination of this Biometrics and the design of algorithms for encryption and decryption, intended to ensure the secrecy and/or authenticity of message has immense scope of providing a higher security platform in various fields. The most important issue in cryptographic system is the key management. Therefore in order to combine biometrics with cryptography we have to relate to the issue of how to combine biometrics along with cryptographic keys.

The three important steps involved while combing biometrics with cryptography are:

1. Biometrics key release

In this mode, if the biometric matching is successful then only the user will be able to view the key.

2. Biometric key generation

In key generation mode, we require the key of a cryptographic system which is being derived from the biometric template hence providing a platform for the security systems as the unique biometrics results in a unique key which is based on some feature or transform extraction.

3. Biometrics key binding

Here, the system secures the user biometrics with the cryptographic key at the time of using it for the first time registration. The key would only be displayed if all the user details match perfectly with the cryptographic keys.

The key generation/binding mode is very much secured as compared to key release mode because key release mode involves the key release and user authentication as two separate and different parts rather than involving a dual mode exchange by the user as well as the cryptography. The conventional cryptography systems depends on the accuracy of the matching of the key and don't require any complex pattern recognition. The key matching process should be very accurate and could not tolerate even smallest of error. As the biometrics are known to be not absolutely accurate and is known to be quite variable, therefore researchers face the challenge of bridging the gap between fuzziness of biometrics matching and exactness of the cryptographic system with much higher accuracy rate.

4.1. Security Enhancement in Biometrics

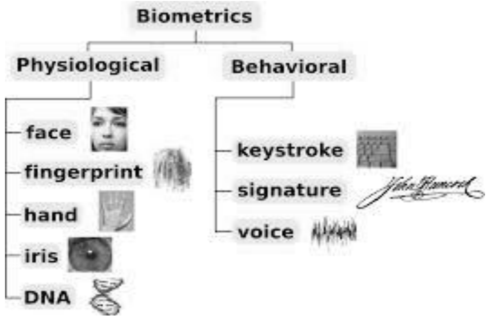

Figure 2: Types of Biometrics

4.1.1. Face Recognition

Biometric identification by scanning a person's face and matching it against a library of known faces; The principle exclusively is the analysis of the shape, positioning and pattern of facial features. It is highly complex technology and largely software based. Its primary advantage is that, it is hands free and a user identity is matched and confirmed by simply staring at the screen. Most face recognition systems either use Eigen faces or local feature analysis.

4.1.2. Fingerprint Recognition

Fingerprints have been recognized as a primary and accurate method of identification. Authentication matches a person's identity to their respective biometrics with one or more security technologies. The use of the ridge and valley (minutiae) found on the surface tips of a human finger to identify an individual. It uses the ridge endings on a person finger to form minutiae. The number and location vary from finger to finger as well as from person to person.

4.1.3. Hand/Finger Geometry

It is a Visual/Spatial Biometric. Geometric features of the hand such as the lengths of fingers and the width of the hand is used to identify an individual. Hand or finger geometry is an automated measurement of many dimensions of the hand and fingers. Neither of these methods takes actual prints of the palm or fingers. Spatial geometry is examined as the user puts his hand on the sensor's surface and uses guiding poles between the fingers to properly place the hand and initiate the reading. Finger geometry usually measures two or three fingers. Hand geometry is a well-developed technology that has been thoroughly field-tested and is easily accepted by users. Because hand and finger geometry have a low degree of distinctiveness, the technology is not well-suited for identification applications

4.1.4. Iris Recognition

It is based on the analysis of the iris of the eye, visible features (corona rings etc). It is regarded as the most safe, accurate biometrics technology and capable of performing 1-to-many matches without sacrificing the accuracy. It is a highly mature technology with a proven track record in number of applications. Iris scanning measures the iris pattern in the colored part of the eye, although the iris color has nothing to do with the biometric. Iris patterns are formed randomly. As a result, the iris patterns in a person's left and right eyes are different, and so are the iris patterns of identical twins. Iris scanning can be used quickly for both identification and verification applications because the iris is highly distinctive and robust.

4.1.5. DNA Matching

This is a Chemical Biometric, where the identification of an individual are identified using the analysis of segments from DNA.

4.1.6. Keystroke

Keystroke dynamics is an automated method of examining an individual's keystrokes on a keyboard. This technology examines such dynamics as speed and pressure, the total time taken to type particular words, and the time elapsed between hitting certain keys. This technology's algorithms are still being developed to improve robustness and distinctiveness. One potentially useful application that may emerge is computer access, where this biometric could be used to verify the computer user's identity continuously.

4.1.7. Signature Recognition

The authentication of an individual by the analysis of handwriting style, in particular the signature. There are two key types of digital handwritten signature authentication, Static and Dynamic. Static is most often a visual comparison between one scanned signature and another scanned signature, or a scanned signature against an ink signature. Technology is available to check two scanned signatures using advances algorithms. Dynamic signature verification is an automated method of measuring an individual's signature. This technology examines such dynamics as speed, direction, and pressure of writing; the time that the stylus is in and out of contact with the "paper," the total time taken to make the signature; and where the stylus is raised from and lowered onto the "paper."

4.1.8. Voice/Speaker Recognition

This is a Auditory Biometric Recognition. Voice or Speaker Recognition uses vocal characteristics to identify individuals using a pass-phrase. A telephone or microphone can serve as a sensor, which makes it a relatively cheap and easily deployable technology. Speaker verification is a 1:1 match where one speaker's voice is matched to one template (also called a "voice print" or "voice model"). Speaker verification is usually employed as a "gatekeeper" in order to provide access to a secure system (e.g.: telephone banking). These systems operate with the user knowledge and typically require their cooperation.

4.1.9. Retina Recognition

Retinal scans measures the blood vessel patterns in the back of the eye. It is the pattern of blood vessels that emanate from the optic curve and disperse throughout the retina which depends on individuals. A retina scan cannot be faked as it is quite impossible to forge a human retina. It is highly accurate and has an error rate of 1 in 10,000,000.

The application of biometrics cannot be uniform for each and every level of people. For different level of people we need entirely different type of technology which would be the best for them. We can conclude that:

(i) For Defence sector as it contains very sensitive information which they cannot afford to leak we must deploy retina recognition as well as iris recognition at different levels of their hierarchy organization.

(ii) For Financial sector we must use the technology of face recognition as well as fingerprint recognition which could be more enhanced with the use of one time passwords for funds transfer, access to internet banking etc.

(iii) For privacy of the emails we can have powerful email encryptions as well as decryption tool which would insure data security and proper handling of sensitive information. At the login page passwords should be replaced with one time password for enhanced security.

4.2. Public Key Infrastructure (PKI)

The principal objective for developing PKI is to enable secure, convenient and efficient acquisition of public keys. Public key infrastructure as the set of hardware, software, people, policies and procedure needed to create, manage, store, distribute and revoke digital certificates based on asymmetric cryptography. It is used to secure data transmission and authentication system, secures privately exchanged data with the help of public keys and private keys which is obtained via a trusted authority. It uses encryption, digital signatures, digital certificates, decryption, certificate authorities, certificate revocation and storage.

4.2.1. Components of Public Key Infrastructure

1. ***Certification Authority (CA)***
   The CA issues the certificate and is responsible for identifying correctness of the identity of the person and verifies the certificate and digitally signs it. It also generates key pairs.

2. ***Revocation***
   When a system publishes certificates there should be a system to let the people know when these certificates are invalid. The challenge to this is that a distributed denial of service attack on the directory or database of stored certificates might create appearance of a fake certificate. The reason for revocation include private key compromise, change in affiliation, and name change.

3. ***Registration Authority(RA)***
   They are sued by the CA to perform necessary identity checks regarding the person or company to prevent from forgery. An optional component that can assume a number of administrative functions from the CA. The RA is often associated with the End Entity(Servers, Routers) registration process, but can assist in a number of other areas as well.

4. ***Certificate publishing method***
   It is the fundamental of PKI systems where certificates are published such as directories, databases, e-mails ect so that the user find it.

5. ***Certificate Management system***
   The management system through which certificates are published, renewed, temporary or permanently suspended or revoked.

Public Key Infrastructure (PKI) is the most evolved form but things could be implemented: PKI should be embedded in every system which would automatically encrypt the data for the sender and decrypt the data for the receiver with the help of public or private keys. The keys could be enhanced with introduction of biometrics between the encryption and decryption process which would make it a complex structure to break upon. The encryption algorithm could be more rigid and strong.

5. NEURAL NETWORK STANDARD

The term Neural Network was traditionally used to refer to a network or circuit of biological neurons. The modern usage of the term often refers to artificial neural networks. Which are composed of artificial neurons or nodes. Thus the term may refer to either Biological neural network, made up of real biological neurons or artificial neural networks, for solving Artificial intelligence problems. In order for neural network modes to be shared by different applications, a common language is necessary. Recently the Predictive Model Markup Language (PMML) has been proposed to address this need.

PMML is an XML-based language which provides a way for applications to be defined and share neural network models and other data mining models between complaint applications. PMML provides applications a vendor independent method of defining modes so that proprietary issues and incompatibilities are no longer a barrier to the exchange of modes between applications. It allows users to develop modes within one vendor's applications or use other vendor applications to visualize, analyze, evaluate.

A range of products are being offered to produce and consume PMML includes the following neural network products:

1. R : Produces PMML for neural nets and other machine learning models via package PMML.
2. SAS Enterprise Miner : Produces PMML for several mining models, including Neural Networks, Liner and Logistic regression, Decision Trees, and other Data Mining models.
3. SPSS: Produces PMML for Neural Networks as well as many other mining models.
4. Statistica: Produces PMML for Neural Networks, Data Mining models and traditional statistical models.

6. WHY USE NEURAL NETS

1. Artificial Neural Nets have a number of properties that make them an attractive alternative to traditional problem solving techniques. The main alternatives to using neural nets are to develop an algorithmic solution and to use an Expert system.
2. Algorithmic methods arise when there is sufficient information about the data and the underlying theory. By understanding the data and the theoretical relationship between the data, we can directly calculate unknown solutions from the problem space. Ordinary Von Neumann computers can be used to calculate these relationships quickly and efficiently from a numerical algorithm.
3. Expert system, by contrast is used in situations where there is insufficient data and theoretical background to create any kind of a reliable problem model. In these cases, the knowledge and rationale of human experts is codified into an expert system. Expert systems emulate the deduction processes of a human expert, by collecting information and traversing the solution space in a directed manner. Expert systems are typically able to perform very well in the absence of an accurate problem model and complete data. However, where sufficient data or an algorithmic solution is available, expert systems are a less than ideal choice.
4. Artificial neural nets are useful for situations where there is an abundance of data, but little underlying theory. The data, which typically arises through extensive experimentation may be non-linear, non-stationary, or chaotic, and so may not be easily modeled. Input-output spaces may be so complex that a reasonable traversal with an expert system is not a satisfactory option. Importantly, neural nets do not require any a priori assumptions about the problem space, not even information about statistical distribution. Though such assumptions are not required, it has been found that the addition of such a priori information as the statistical distribution of the input space can help to speed training. Many mathematical problem models tend to assume that data lies in a standard distribution pattern, such as Gaussian or Maxwell-Boltzmann distributions. Neural networks require no such assumption. During training, the neural network performs the necessary analytical work, which would require non-trivial effort on the part of the analyst if other methods were to be used.

7. ADVANTAGES AND DIS-ADVANTAGES OF NEURAL NETWORK

Advantages

(i) A Neural Network can perform a task that a liner program can't.

(ii) When an element of the Neural Network fails, it can continue without any problem by their parallel nature.

(iii) A Neural Network learns and does not need to be reprogrammed.

(iv) It can be implemented without any problem.

(v) It can be implemented in any applications.

Disadvantages

(i) The Neural Network needs training to operate.

(ii) The architecture of Neural Network is different from the architecture of microprocessors therefore needs to be emulated.

(iii) Requires high processing time for large Neural Networks.

8. CONCLUSION

This paper showed the introduction of Artificial Neural Network in data security context. Today, in data communication systems, data security is of prime concern, because building a secure channel is one of the most challenging areas in research and development. Cryptography enables the parties to communicate over an insecure channel so that an attacker cannot understand and decrypt the original message. Public Key cryptography is available in many forms but it requires huge time consumption, complexity and large computational power. An Artificial Neural Network can be the best way to overcome these problems. The connection between an Artificial Neural Networks and cryptography is providing a great help for the security concerns. So, Artificial Neural Network can be used as a new method for encrypting and decrypting the data.

9. REFERENCES

[1] Limin Fu, Neural Networking in Computer Intelligence, Tata McGraw Hill Edition, New Delhi, 2003. (book chapter style)

[2] Williams Stallings , Cryptography and Network Security, Pearson prentice Hall, New Delhi, 2007. (bool chapter style).

[3] Yuvraj Gupta, “Enhancing Data Security in Cloud Computing”, International Journal of Scientific & Engineering Research, Vol 3, 2012. (journal style).

[4] Navika Agarwal, Prachi Agarwal, “Use of Artificial Neural Network in the field of Security”, MIT International Journal of Computer science & Technology, pp.42-22, Vol 3, No.1, 2013.(journal style)

[5] Teuvo Kohonen, “An Introduction to Neural Computing”, Neural Networks, pp.3-16, Vol 1, 1988 (journal style)

[6] Nilmani, “Neural Network”, Jan.29,2010[Online]. Available:http://www.slideshare.net/nilmani14/neural-network-3019822 [Accessed: Oct. 25, 2014]. (General Internet site).

[7] wikibooks, “Artificial Neural Networks/Neural Network Basics”, Oct.24,2014 [Online]. Available:http://en.wikibooks.org/wiki/Artificial_Neural_Networks/Neural_Network_Basics Accessed: Oct. 25, 2014]. (General Internet site)

[8] MIS Biometrics Home, “ MIS Biometrics”,Apr. 4, 2008[Online].Available:http://misbiometrics.wikidot.com/ [Accessed: Oct. 24, 2014] (General Internet style)

[9] Biometrics Institute Limited, “Types of Biometrics”,2005[Online]. Available: http://www.biometricsinstitute.org/pages/types-of-biometrics.html [Accessed: Oct. 24,2014](General Internet style)

[10] “A Basic Introduction to Neural Networks”, Available: http://pages.cs.wisc.edu/~bolo/shipyard/neural/local.html [Accessed: Oct. 24, 2014] (General Internet style).

Author Profile

C.R.Kavitha received the B.Sc. (Chemsitry) in University of Madras in 1999 and MCA in Indira Gandhi National Open University in 2004. And Completed M.Phil in Thiruvalluvar University in 2008. She now working as a Assistant Professor in Sri Lakshmi |Narasimha College of Sciences,Andhra Pradesh, India.