ISSN:0975-9646
D.Raghu et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, 2765-2772

Neural Network Based Authentication and Verification for Web Based Key Stroke Dynamics

Prof. D. RAGHU, CH. RAJA JACOB, Y.V.K.D.BHAVANI

CSE Dept., Nova College of Engineering & Technology,
Jangareddigudem, Andhra Pradesh, INDIA

***ABSTRACT*-Web based authentication provide remote authentication and security control mechanism. Password typing is the most widely used identity verification method in World Wide Web based Electronic Commerce (EC). Due to its simplicity, it is vulnerable to imposter attacks. Keystroke dynamics and password checking can be combined to result in a more secure verification system. We proposed an association of ideas of neural network that is trained with the timing vectors of the owner's keystroke dynamics and then used to discriminate between the owner and an imposter. This paper presents a novel application of neural nets to user identity authentication on computer-access security system. A three-layered back propagation neural network with a flexible number of input nodes was used to discriminate valid users and impostors according to each individual's password keystroke pattern. Keystroke latency is measured for each user and forms the patterns of keyboard dynamics. System verification performance was improved by setting convergence criteria RMSE (Root Mean Square Error) to a smaller threshold value during training procedure. The resulting system gave 1.1% FAR (False Alarm Rate) in rejecting valid users and zero IPR (Impostor Pass Rate) in accepting no impostors. An imposter typing the correct password can be detected with very high accuracy using the proposed approach. This approach can be effectively implemented by a Java applet and used in the World Wide Web. A suitable network structure for this application was also discussed. Furthermore, the implementation of this approach requires no special hardware and is easy to be integrated with most computer systems.**

KEYWORDS: **web, authentication, Neural Network(NN), FAR, IPR, EC, biometric, MLP, HTTP, applet,www,SSL.Finger Print, Palm print, hand shape,Iris etc.**

1. INTRODUCTION:

Web based system: At present developments the world wide web (WWW) and Electronic Commerce has emerged as the implementation platform of choice thanks to its simplicity and low cost. As more and more business is done online, the need for secure web-based transactions is constantly increasing. Passwords and user ID are no longer considered secure enough for transacting business over the internet. The strong web-based authentication is required for financial transactions.

Since the WWW was developed as a means of sharing information among computers scattered around the world, it tends to lack sophisticated security methods. Thus, it is not suitable for certain commercial transactions that require a secure communication channel. Superior security measures need to be developed to further an even wider acceptance of the WWW as an EC (E Commerce) platform. Web based authentication is equally important in protecting network integrity, preventing hackers from getting in, and combating identity theft.

User authentication is a particular aspect of security relevant to EC. It is concerned with verifying claimed identity. Several methods have been proposed for use on the WWW, such as user IDs and passwords, IP addresses, and message digest authentication. Additional ideas such as channel-based, content-based and message-based methods all use hypertext transfer protocol (HTTP). Although the password approach is the most widely used, as well as being the simplest and least expensive tool, it has loopholes because people tend to choose as passwords such easy-to-guess words and/or numbers as the names of family members, birthdays, phone numbers, addresses, etc. The result is a security failure. Some other means should be devised which replaces or consolidates the password approach.

One approach that is both inexpensive and simple takes advantage of the uniqueness of keystroke dynamics. When a user types a word, for instance a password, the keystroke dynamics can be characterized by a "timing vector", consisting of the duration of keystrokes and the time interval between them. A word of n characters followed by "Return" results in a timing vector of dimension $2n+1$.

In this paper, we proposed an association of ideas of neural network model that reduces error rates significantly. Timing vectors from an owner were collected and used to build a neural network model that outperformed a conventional Nearest Neighbor (k-NN) approach. Although experiments involving many more owners are required for practical use of this approach, the preliminary results are the best ever reported to the authors' knowledge. It is possible to implement this approach in the WWW environment using Java applets.

II. NEURAL NETWORK ARCHITECTURE

Neural Networks (NNs) are programs designed to solve any problem by trying to mimic structure and function of our nervous system. Neural networks are based on simulated neurons which are joined together in a variety of ways to form networks neural network resembles the human brain in the following two ways: -

1. A neural network acquires knowledge through learning.
2. A neural network's knowledge is stored within the interconnection strengths known as synaptic weight.

Neural network are typically organized in layers. Layers are made up of a number of interconnected 'nodes', which contain an 'activation function'. 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.

The first layer is the input layer and the last one, the output layer. The layers that are placed within these two are the middle or hidden layers. A neural network is a system that emulates the cognitive abilities of the brain by establishing recognition of particular inputs and producing the appropriate output. Neural networks are not "hard-wired" in particular way.

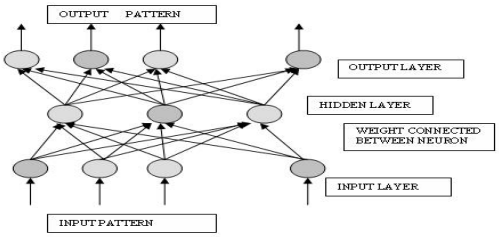

Fig-1: Representation of Neural Networks(NN)

They are trained using presented inputs to establish their own internal weights and relationships guided by feedback. They adapt on their own, they are usually adjusted, or trained so that a particular input leads to a specific target output .

III. SYSTEM SECURITY MEASURES

System security: The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users. The term computer system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively.

Now-a-days there are a lot of security systems that promises to provide excellent security to several types of systems, but in spite of that many of them fail to deliver when it comes to real time testing (burglary or crime events). For example in case of a house system secured by cryptography using password authentication technique, they do not assure foolproof security as at times they keep constraints like limiting the passwords to eight characters only, converting everything to lower case, etc. unfortunately this makes them more easy to be hacked. System security is usually maintained by system access control. User authentication is one way to achieve it.

The home security system using Neural Network which is suggested here is harder to be hacked. The Neural Network is used to train (learning) the identification parameters like User ID and password. Such a network acts as a brain in securing of passwords without constraints. One of the most well known types of neural network is the Multilayer Perceptrons Neural Network (MLPs).Such a perceptron network makes use of Back propagation Algorithm which is a supervised artificial neural network (ANN) .Using this system it is safe enough for the user to combine the door lock with the security system because it is hard for the intruder to hack the system and get the UserID and password. After the user enters the key, this system can be integrated as an authorization system before entering the house. Therefore, even if the key gets robbed, it would be difficult for strangers to access the door because it is hard to crack the owner's UserID and password.

IV. USER AUTHENTICATION APPROACHES

The ownership-based approaches are the oldest, but are vulnerable to loss or theft. The use of a password is the most popular approach in computer access security now thanks to simplicity, effectiveness, convenience and low cost. A user is expected to choose a hard-to-guess password and to change it frequently. The biometric-based approaches are free from loss, theft or memory problems. But they are not perfect, and involve two types of errors. False Accept Rate (FAR) denotes the rate that an imposter is allowed access. False Reject Rate (FRR) denotes the rate that the legitimate user is denied access. Various approaches can be quantitatively evaluated in terms of processing time, cost, and user acceptability as well as error rates as shown in Table II. The fingerprint method and the hand shape method suffer from similar problems.

This paper is structured as follows. First, various system security measures are described. Then the typing dynamics based verification method is presented, followed by the results of previous research. The neural network based novelty detector is proposed, and then data collection and experimental results follow. After a Java applet implementation on the WWW is described, a summary and discussion of ongoing and future research issues conclude this paper.

TABLE -I: USER AUTHETICATION APPROACHES

Approach	Examples
Ownership-based	Key, Card
Knowledge-based	Password, PIN
Biometric-based	(static) Fingerprint, Hand Shape, Retinal Pattern

IV.1. Strong User Authentication

So, how do we improve Web-based user-authentication systems without compromising usability and ubiquity, when the Internet is accessed mostly through a browser that has limited access to the client environment and hardware devices? The most common solution approaches that are used today involve, in more generalized terms, various forms of enhanced shared-secret and/or multifactor authentication.

Multifactor authentication refers to a compound implementation of two or more classes of human-authentication factors:

- **Something known to only the user**—Knowledge-based (for example, password, pass phrase, shared secrets, account details and transaction history, PIN, CAPTCHA, and so on).
- **Something held by only the user**—Possession-based (for example, security token, smart card, shared soft tokens, mobile device, and so on).
- **Something inherent to only the user**—Biological or behavior biometric traits (for example, facial recognition, fingerprint, voice recognition, keystroke dynamics, signature, and so on).

Stronger user authentication was provided by using different approaches. One of that approaches is -

IV.II. Solution Approach:

Now, not all of the available strong-authentication options that are available today lend themselves well to the Web. Conventional multifactor authentication methods are effective for closed communities—such as employees and partners—but they are too costly, inconvenient, and logistically difficult. In this case, authentication solutions have to work primarily within the confines of the browser's security sandbox. Here, we discuss a solution approach that is relatively cost-effective to implement for online consumers, based on today's standards:

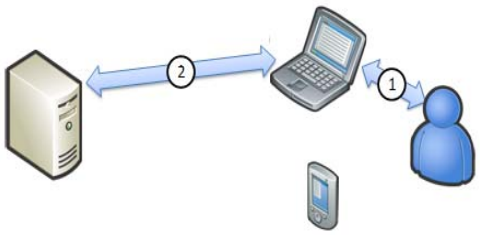

Fig- 2: Knowledge-based authentication

Knowledge-based authentication (KBA) typically is implemented as extensions to existing simple-password authentication. Knowledge-based credentials include chosen information, personal and historical information, on-hand information, deductive and derived responses, patterns, images, and so on. KBA is used also as an identity-verification method for self-service password-reset processes; but, when implemented effectively, they can be used as methods to complement primary authentication. This approach moderately improves authentication strength, as it is still single-factor (in-band within the browser) and prone to phishing attacks, but it might be sufficient for some Web sites.

V. Comparisons of Biometric Based Authentication Methods:

Biometrics (or biometric authentication) consists of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.

Biometric characteristics can be divided in two main classes:

- **Physiological** are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, Palm print, hand geometry, iris recognition which has largely replaced retina, and odour/scent.
- **Behavioral** are related to the behavior of a person. Examples include, but are not limited to typing rhythm, gait, and voice. Some researchers have coined the term **behaviometrics** for this class of biometrics.

V.I. Biological verification technology

Therefore on some occasion where the requirements for security are not so high, some simpler authentication such as password is used. In addition there are some authentication methods such as biological authentication.

Because of the importance of identity authentication, aside from the above men there are many other ways based on the user's biological characteristics such as face ID authentication, fingerprint ID authentication, Iris ID authentication, palm print ID authentication, voice ID authentication and manual signature ID authentication etc.

V.I.I. Fingerprint authentication method:

Fingerprint Authentication is one of the oldest biological authentications, which has been successfully applied to many areas. Finger print refers to the lines on the surface of a fingertip. The details of the finger print constitute the unique information of the fingerprint. A authentication procedure includes 3 parts: pattern extraction, finger print classification and match decision.

Pattern extraction means extracting details from the fingerprint image; the finger print images are classified to promote the authentication speed. Match determines if two fingerprints come from the same finger.

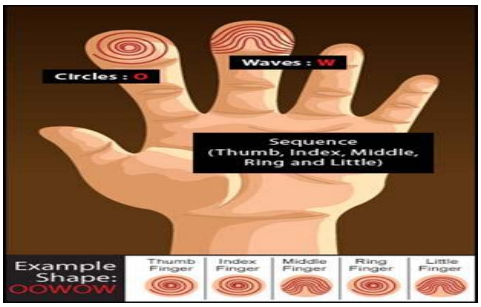

Fig-3: Finger print authentication

V.I.II Iris authentication:

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of the irides of an individual's eyes, whose complex random patterns are unique and can be seen from some distance.

Iris is the ring area between pupil and sclera. Compared with other biological authentication, Iris authentication is highly unique, stable, anti-fake and useable. The procedure of iris authentication includes: iris location, iris alignment, pattern expression and match decision. Iris location extracts iris form the whole image; iris alignment determines the corresponding relation between the structures of two images; pattern expression captures the unique spatial characters of the iris;

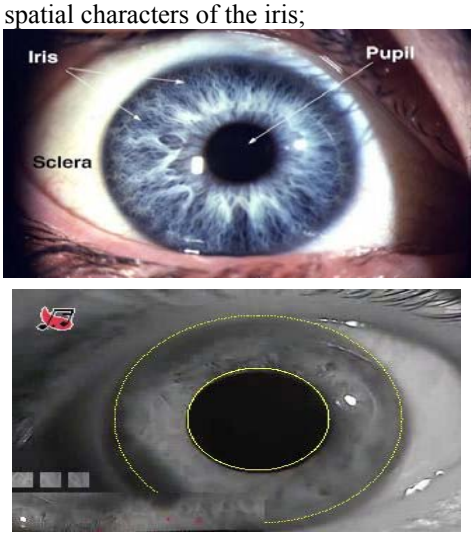

Fig-4: Iris recognition system based on pattern matching

V.I.III. Hand shape authentication:

Hand shape authentication is the speediest one in biological authentication since it is comparatively easy to measure the shape of hand and extract the image of hand shape. However, characteristics of hand shape do not have high uniqueness, and cannot be used alone for authentication as a result. Typical characteristics of hand shape include the length and width of fingers, thickness of palm, ration of length- to-width of finger etc.

V.I.IV.Palm print authentication:

Compared with fingerprint, palm print authentication is much more obvious than those of fingerprint. Furthermore, the main characteristics of palm print are more stable and classifiable than those of finger print; therefore palm print authentication should be a method of ID authentication with high potential of development. Current palm print authentication basically utilizes major lines and palmers creases.

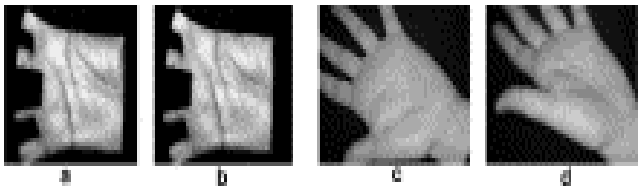

Fig-5: Sample palm print images. Image (a) and image (b) belong to the PolyU database. They are captured from the same palm. Image (c) and image (d) belong to the CASIA database. They are also captured from the same palm.

TABLE -II: COMPARISONS OF BIOMETRIC-BASED USER AUTHENTICATION METHODS

Authentication	FAR	FAR	Time	Cost	User
Fingerprint	0.001	0.5	4	4,000	Low
Hand Shape	1	1 – 3	6	3,500	Medium
Retinal	0.0001	5	2	6,000	Low
Voice	0.1 - 2	0.25 –	3	1,000 –	High
Signature	3	0.7	5	700 –	High
FAR: False Acceptance Rate					

VI.PASSWORD CHARACTERISTICS AND ERROR MEASURES FROM RESPECTIVE MODELS

Passwords can be the weakest link in a server security deployment. You should always take great care when you select a password. A strong password has the following characteristics:

- Are at least 8 characters long.
- Combines letters, numbers, and symbol characters within the password.
- Is not found in a dictionary.
- Is not the name of a command.
- Is not the name of a person.
- Is not the name of a user.
- Is not the name of a computer.
- Is changed regularly.
- Is significantly different from previous passwords.

Microsoft SQL Server passwords can contain up to 128 characters, including letters, symbols, and digits. Because logins, user names, roles, and passwords are frequently used in Transact-SQL statements, certain symbols must be enclosed by double quotation marks (") or square brackets ([ ]). Use these delimiters in Transact-SQL statements when the SQL Server login, user, role, or password has the following characteristics:

- Contains or starts with a space character.
- Starts with the $ or @ character.

If used in an OLE DB or ODBC connection string, a login or password must not contain the following characters: [] {}() , ; ? * ! @. These characters are used to either initialize a connection or separate connection values.

VI.I. Password complexity:

Password complexity policies are designed to deter brute force attacks by increasing the number of possible passwords. When password complexity policy is enforced, new passwords must meet the following guidelines:

- The password does not contain all or part of the account name of the user. Part of an account name is defined as three or more consecutive alphanumeric characters delimited on both ends by white space such as space, tab, and return, and any of the following characters: comma (,), period (.), hyphen (-), underscore (_), or number sign (#).
- The password is at least eight characters long.
- The password contains characters from three of the following four categories:
  - Latin uppercase letters (A through Z)
  - Latin lowercase letters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphanumeric characters such as: exclamation point (!), dollar sign ($), number sign (#), or percent (%).

Passwords can be up to 128 characters long. You should use passwords that are as long and complex as possible.

VI.II. Password Expiration:

Password expiration policies are used to manage the lifespan of a password. When SQL Server enforces password expiration policy, users are reminded to change old passwords, and accounts that have expired passwords are disabled.

VI.III. Policy Enforcement:

The enforcement of password policy can be configured separately for each SQL Server login. Use ALTER LOGIN(Transact-SQL) to configure the password policy options of a SQL Server login. The following rules apply to the configuration of password policy enforcement:

- When CHECK_POLICY is changed to ON, the following behaviors occur:
  - CHECK_EXPIRATION is also set to ON unless it is explicitly set to OFF.
  - The password history is initialized with the value of the current password hash.
- When CHECK_POLICY is changed to OFF, the following behaviors occur:
  - CHECK_EXPIRATION is also set to OFF.
  - The password history is cleared.
  - The value of lockout time is reset.

Some combinations of policy options are not supported:

- If MUST_CHANGE is specified, CHECK_EXPIRATION and CHECK_POLICY must be set to ON. Otherwise, the statement will fail.
- If CHECK_POLICY is set to OFF, CHECK_EXPIRATION cannot be set to ON. An ALTER LOGIN statement that has this combination of options will fail.

VI.IV Password strength

Password strength is a measure of the effectiveness of a password in resisting guessing and brute-force attacks. In its usual form, it estimates how many trials an attacker who does not have direct access to the password would need, on average, to guess it correctly. The strength of a password is a function of length, complexity, and unpredictability.

Using strong passwords lowers overall risk of a security breach, but strong passwords do not replace the need for other effective security controls. The effectiveness of a password of a given strength is strongly determined by the design and implementation of the authentication system software, particularly how frequently password guesses can be tested by an attacker and how securely information on user passwords is stored and transmitted. Risks are also posed by several means of breaching computer security which are unrelated to password strength. Such means include wiretapping, phishing, keystroke logging, social engineering, dumpster diving, side attacks and software vulnerabilities.

VI.V. Determining password strength

There are 2 factors to consider in determining password strength: the ease with which an attacker can check the validity of a guessed password, and the average number of guesses the attacker must make to find the correct password. The first factor is determined by how the password is stored and what it is used for, while the second factor is determined by how long the password is, what set of symbols it is drawn from and how it is created.

VI.V.I. Password guess validation

The most obvious way to test a guessed password is to attempt to use it to access the resource the password was meant to protect. However, this can be slow and many systems will delay or block access to an account after several wrong passwords are entered. On the other hand, systems that use passwords for authentication must store them in some form to check against entered values. Usually only a cryptographic hash of a password is stored instead of the password itself. If the hash is strong enough, it is very hard to reverse it, so an attacker that gets hold of the hash value cannot directly recover the password. However, if the cryptographic hash data files have been stolen, knowledge of the hash value lets the attacker quickly test guesses.

VI.V.II. Password creation

Passwords are created either automatically (using randomizing equipment) or by a human. The strength of randomly chosen passwords against a brute force attack can be calculated with precision. Commonly, passwords are initially created by asking a human to choose a password, sometimes guided by suggestions or restricted by a set of rules. This typically happens at the time of account creation for computer systems or Internet Web sites. In this case, only estimates of strength are possible, since humans tend to follow patterns in such tasks, and those patterns will always assist an attacker.

In addition, lists of commonly chosen passwords are widely available for use by password guessing programs. Any of the numerous online dictionaries for various languages is such a list. All items in such lists are considered weak, as are passwords that are simple modifications of them. Either can be quickly tried. For some decades, investigations of passwords on multi-user computer systems have shown that 40% or more are readily guessed using only computer programs, and more can be found when information about a particular user is taken into account during the attack.

V I I . TYPING DYNAMICS BASED USER VERIFICATION

When one types a phrase or a password on a keyboard, the typing dynamics or timing pattern can be measured and used for identity verification. More specifically, a timing vector consists of the keystroke duration times interleaved with the keystroke interval times. If one types a password of seven characters, a 13-dimensional timing vector results which consists of seven keystroke duration times and six keystroke interval times. Two more elements can be added to the vector if ENTER key information is considered. Figure 6 shows the timing vector when "ABCD" is typed. An actual example of 15-dimensional timing vector from a seven character-long password is [120,60,120,90,120,60,150,-60,120,-30,120,-60,120,120,90,60,150]. The time unit is in milliseconds. Negative interval time's result when the next key is pressed before a previous key is released.

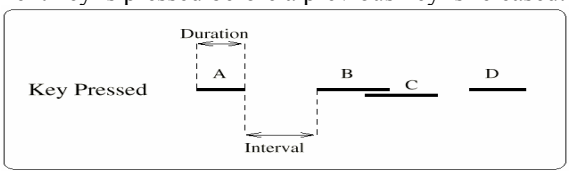

Figure -6: Timing vector corresponding to "ABCD"

It has been shown that an individual has characteristic and distinctive typing dynamics. A pattern classifier can be built which distinguishes an individual's typing dynamics from those of others (see Figure 6). Combined with a simple password scheme, the typing dynamics based identity verification provides an additional layer of protection with a negligible increase in cost and processing time.

VIII.PREVIOUS RESULTS

Here, we review typing dynamics based user verification methods that have been proposed in the past. All biometrics-based approaches have two types of errors; the false accept rate (FAR) and the false reject rate (FRR). Since one type of error can be reduced at the expense of the other, an appropriate middle point is usually used as a threshold based on the relative cost of the errors. A different choice of threshold results in different FAR and FRR values. In this paper, we employ a widely used error measure "FRR when FAR = 0", i.e. FRR when we set the threshold such that FAR becomes zero.

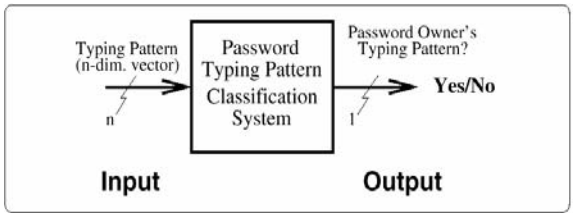

Fig -7: Typing Dynamics based Identity

In the past, a short character string such as a password was regarded as inadequate for user authentication . A long string of 537 characters, for example, had to be employed to achieve 5.0% FAR and 5.5% FRR . Only recently through the use of neural networks, a comparable performance of 12% to 21% was achieved using short strings such as real life names These error rates are still too high to be practically acceptable. In addition, the neural network was trained in advance not only with the owner's timing vectors but also with those of imposters. In real life situations, this is unacceptable because the owner's password has to be revealed to users at large.

In the late 80's, two US patents were granted for statistical approaches, but performance results are not available. A lower error rate of 2.5% was obtained when the user identification problem was solved. This problem involves finding out who, among several candidates, typed the password rather than determining whether the timing vector is that of the owner. The network had to be trained with the timing vectors of all candidates. Unfortunately, the result cannot be applied to the user authentication problem. Also, a 0% error rate was recently reported in user verification using 7 character-long login names . However, negative examples (i.e., intruder's typing patterns) as well as positive examples (i.e., owner's patterns) were used for training, and the training data set was much larger (6,300 positives and 112 negatives). Also, the training and test patterns were not chronologically separated.

IX. PASSWORD CHARACTERISTICS AND ERROR MEASURES FROM RESPECTIVE MODELS

Also shown in Table III are the error rates for the *k*-NN and MLP approaches. The error is the False Reject Rate (FRR) when the False Accept Rate (FAR) was reduced to zero. For *k*-NN, we tried 1, 2, and 3 as *k* values and obtained the best result with *k*=1, which is shown here. Each MLP contains the same number of hidden units as input units. All 21 MLPs were trained with a standard back propagation algorithm, with a learning rate of 0.1 and a momentum term of 0.3, for 500 epochs. The proposed MLP approach clearly outperformed the *k*-NN. A perfect authentication was achieved for 13 owners. The worst performance was from owners 12 and 13, with an error rate of 4.0%. The average error rate was 1.0%. The paired comparison hypothesis test was performed with

H_0 : an H_1 : μ_d *where random variable D denotes the difference of error rates .*

$\mu_d = d > 0$ *for two algorithms;i.e-eMLP,.*

e1-NN- e_{MLP}

Assuming both error values are from a normal distribution, follows a t-distribution with a degree of freedom of 20. Since then statistic value of 3.656 is t_0 0 h0 is rejected with a 99% confidence. In larger than 2.528= 1 ; conclusion the superiority of MLP approach's performance is statistically significant.

TABLE III
PASSWORD CHARACTERISTICS AND ERROR MEASURES FROM RESPECTIVE MODELS

Owner ID	Password	Number of Training Patterns	Discard Rate	FRR when FAR = 0	
				1-NN	MLP
1	loveis.	207	0.21	22.7	2.7
2	i love 3	330	0.15	30.7	0.0
3	autumnman	111	0.10	0.0	0.0
4	90200jdg	164	0.10	5.3	0.0
5	rla sua	101	0.18	8.0	1.3
6	dhfpql.	232	0.08	17.3	2.7
7	love wjd	101	0.19	54.7	0.0
8	dltjdgml	151	0.14	0.0	0.0
9	dusru427	365	0.27	0.0	0.0
10	manseiii	86	0.25	60.0	1.3
11	rhkdwo	205	0.20	18.7	0.0
12	beaupowe	76	0.24	9.3	4.0
13	tdwnsl1	108	0.18	17.3	4.0
14	yuhwa1kk	388	0.12	0.0	0.0
15	anehwksu	319	0.10	10.7	0.0
16	tjddmswjd	337	0.10	33.3	0.0
17	drizzle	299	0.10	9.3	1.3
18	dlfjs wp	342	0.06	1.3	0.0
19	c.s.93/ksy	200	0.22	17.3	2.7
20	dirdhfmw	309	0.33	89.3	0.0
21	ahrfus88	260	0.20	5.3	0.0
Avg.		223	0.17	19.5	1.0
Min.		76	0.06	0.0	0.0
Max.		388	0.33	89.3	4.0

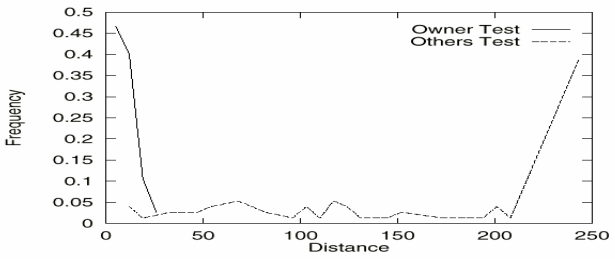

Fig 8. Histograms of average distance measure (1-NN). The better separated the owner and imposter populations are, the better the classification is.

When the proposed neural network approach is to be used in actual applications, a few issues have to be resolved. **First**, how one obtains training data in a real situation? Obviously, a separate data-collecting module has to be built. During the data collection period, right after a new password is registered, the proposed identity verification cannot be used. However, an ordinary level of security can be maintained with the conventional password security system. The length of the collection period can be dynamically determined by monitoring the

variability of typing patterns. This data collection overhead is common among all dynamic biometrics based approaches including the online signature based identity verification.

Second, for each password or user, a separate MLP has to be constructed. Also, whenever a user changes his or her password, a new MLP has to be built. The problem of finding the appropriate number of hidden units, or model selection, is not straightforward.

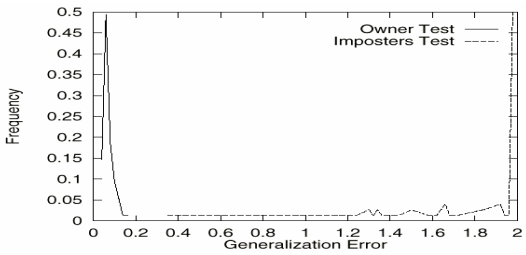

Fig 9. Histograms of generalization error (MLP). The better separated the owner and imposter populations are, the better the classification is.

Trial and error is usually employed. However, it is not much of a concern here since the auto associative MLP used here employed the same number of hidden units as input and output units for all 21 cases. It was automatically set, thus the network building cost can be minimized.

Third, the performance measure we used in the paper is FRR when FAR is set to zero.

X. WWW IMPLEMENTATION

Figure 10 shows a simplified diagram of how the proposed scheme can be implemented over a network in the WWW. There are three different ways to implement the typing dynamics, namely Plug-in, Active-X and Java applet. The Plug-in approach is expensive since actual implementation depends on the type of web browser and operating systems involved. The Active-X approach makes it possible to take advantage of already developed Component Object Model (COM) objects in Windows. The downside is that the resulting system operates only in a Windows environment. Finally, the Java applet approach is inexpensive since a single implementation works for different environments as long as a web browser (see Figure 7) supports Java Virtual Machine. Also, unlike the Plug-in approach, it is not necessary to install anything in a client machine in advance.

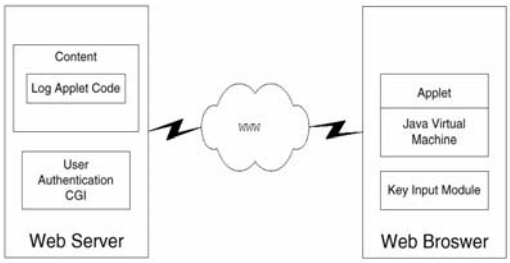

Figure -10: Client-server implementation structures in WWW

When the Java applet code is loaded by the web rowser security environment such as Secure Sockets Layers (SSL), it can use the additional package support to communicate with the CGI in the secure sockets layer because the standard Java package does not provide the SSL(Service Socket Layer). For these reasons, we have chosen the Java applet approach in this work. Comparison of the three methods is summarized in

Structures in WWW figure 11 security environments for the java applet approach

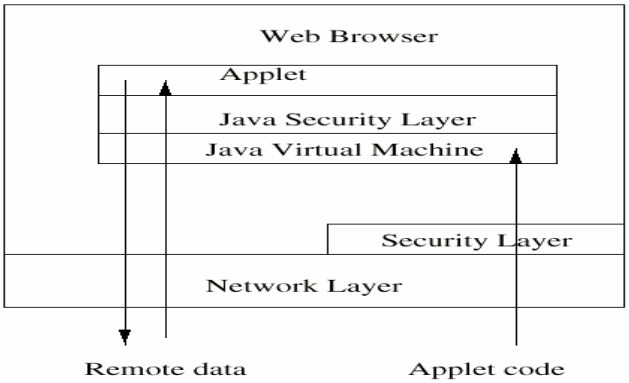

Figure -11:. Security environment for the Java applet approach

XI. COMPARISON OF PLUG-IN, ACTIVE-X, AND JAVA APPLET

Conceptually, the Java applet approach works as follows. When a client tries to access a homepage, for example, say a firm's on- line shop, located in a server, the user types the already registered user ID. Then the server sends the client a Java applet code that can measure the user's password keystroke timing vector. Once the Java applet running in the client system gathers the user's keystroke timing vector, it sends it back to the server. Then the autoassociative neural network located in the server can verify whether the user is the person he or she claims to be. Since the code is programmed in Java, any client system that has a Java browser can be connected to the server.

More specifically, the procedure can be described in four steps (see Figure 8). First, the Java applet byte code stored in the web server is downloaded onto the web browser. Second, the applet receives user ID and password information (characters and timing vectors) through TextField object and send them back to Common Gateway Interface (CGI) which is the authentication module in the web server. Third, if the password information is classified as authentic, a first page is sent back to the web browser along with a cookie. From then on, URL requests are issued through the cookie.

TABLE IV
COMPARISON OF PLUG-IN, ACTIVE-X, AND JAVA APPLET

	Plug-in	Active-X	Java
Platform	UNIX, Windows	Windows	UNIX,
Language	C/C++, Basic	MFC	Java
Cost	High	Medium	Low
Prior additional Installation	Yes	No	No

XII. CONCLUSION

An MLP-based novelty detector is proposed for user authentication using keystroke dynamics. An auto associative MLP is built from a set of timing vectors previously collected from the owner. When a new timing vector arrives, it is presented to the MLP, and output is computed. If the output is close enough to input, the input timing vector is classified as that of the owner. If not, it is classified as that of an imposter. The experimental results involving 21 skilled users show that the proposed approach is significantly more effective than the *k*-NN approach. For 13 owners, the MLP approach achieved perfect authentication. Among the rest, the worst performance was a 4% error rate. The overall average error rate was 1%. The preliminary result reported here is quite promising. The proposed approach was also implemented on the World Wide Web, proving that the scheme can be used for electronic commerce applications.

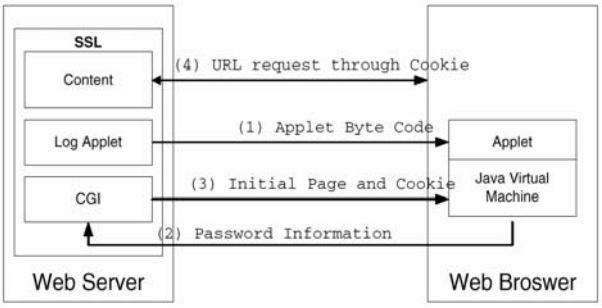

Fig 12:. Step-by-step WWW implementation procedure

Further investigation is necessary in the following areas: **First**, many more experiments involving human subjects must be conducted. Such issues as typing inexperience, learning effects, and fatigue must also be considered. **Second,** we must investigate how to make the number of necessary training patterns as small
as possible. Finally, a variety of preprocessing and feature extraction algorithms must be examined.

XIII.REFERENCES

[1] J. Garcia, "Personal identification apparatus", *Patent No. 4,621,334*. U.S. Patent and Trademark Office, Washington D.C. 20231, 1986.

[2] J. Young and R. Hammon, "Method and apparatus for verifying an individual's identity", *Patent No. 4,805,222*. U.S. Patent and Trademark Office, Washington D.C. 20231, 1989.

[3] M. S. Obaidat and D. T. Macchairolo, "A multilayer neural system for computer access security", *IEEE Transactions on Systems, Man,*

[4] J. Park, S. Kang, and S. Park, "Trends in world wide web security technology", *Korea Information Science Society Review*, vol. 15, no. 4, pp.37-44, 1997.

[5] D. Davis and W. Price, *Security for Computer Networks*, John Wiley & Sons, Inc., 1989.

[6] G. Forsen, M. Nelson, and R. Staron, "Personal attributes authentication techniques", in *Rome Air Development Center Report RADC-TR-77-*

[7] *Man-Machine Studies*, vol. 39, pp. 999-1014, 1993. *1033*, A. Griffs, Ed., New York:RADC, 1977.

[8] J. Leggett, G. Williams, M. Usnick, and M. Longnecker, "Dynamic identity verification via keystroke characteristics", *International Journal of Man-Machine Studies*, vol. 35, pp. 859-870, 1991.

[9] M. Brown and S. J. Rogers, "User identification via keystroke characteristics of typed names using neural networks", *International Journal*

[10] Neural networks for Pattern Recognition; Christopher M. Bishop Oxford university ;1995

[11]Fundamentals of Neural Networks:Architectures,Algorithms and applications; Fausett Laurence ;1994

[12]Neural Computation : A Beginner's Guide ; Orchard, G.A; 1991

[13]Neural Networks;Muller,B and Reinhardt;Springer Verlag;1991

[14] Fukushima, Kunihiko (1975). "Cognitron: A self-organizing multilayered neural network". *Biological Cybernetics* **20** (3–4): 121–136. doi:10.1007/BF00342633.PMD 1203338

[15] Rummelhart, D.E; James McClelland (1986). Parallel Distributed Processing: Explorations in the Microstructure of Cognition. Cambridge: MIT Press.

Author's Profile:

Prof. Raghu Devarapalli is a well known Author, Administrator and Excellent teacher,with his vast experience in teaching wrote manybooks, articles and research papers. He visited many countries and worked with Europeans, Americans, Philippines,Cubans and Africans. He was a consultant for Canada projects in Ethiopia (Korsa Demographic Surveillance systems). He was a Member Board of Study, Member Examination and evaluation in Department of Computer Science& Informatics in Alemaya and Dire Dawa University's and worked with United Nations Development Project. He served as a Department Head, Dean, Principal and Visiting Professor, presently working as a Director for Nova Group of Colleges includes Engineering, Pharmacy, Management, Education Colleges at Jangareddigudem, Eluru. He is a Editorial Board Member for East African Journal of Science (EAJS) an international and multi disciplinary Journal of sciences. His early books are in C, C++, Operating systems, DBMS, Principles of Programming and Illustrating Computer Science. He received his Bachelors, Masters and Doctors degree in the field of Computer science and Information technology and he designed and guided many Projects.

Mr. Ch. Raja Jacob, well known Author and excellent teacher received M.C.A and M.Tech (CSE) from Acharya Nagarjuna University is working as Associate Professor and HOD, Department of MCA, M.Tech Computer Science & Engineering, Nova College of Engineering and Technology, Jangareddigudem. He is an active member of ISTE. He has 7 years of teaching experience in various Engineering Colleges. To his credit couple of publications both national and international Conferences / Journals. His area of Interest includes Data Warehouse and Data Mining, information security, flavors of Unix Operating systems and other advances in Computer Applications.

Smt.Y.V.K.D.Bhavani received her MCA Degree from IGNOU University, Delhi and presently she is pursuing M.Tech in Computer Science & Engineering from the year 2009 and about to complete his M.Tech in the year 2011 from Nova College of Engineering and Technology, Jangareddigudem affiliated to Jawaharlal Nehru Technological University, Kakinada. Her area of interest in Multimedia Application Development, Middleware technology, Distributed Database, Software Engineering and interested in developing software projects.