Digraph Approximation with an Adaptation Technique for Mobile User Authentication through Keystroke Dynamics

Christy James Jose, Jijo Francis, Rajasree M.S

Abstract— Mobile devices have evolved at a proliferating rate and are now used in almost all aspects of life. With these the ability to store potentially private or sensitive information on these devices has also increased. Hence an intrusion detection and prevention system is a necessity for preserving the confidentiality and integrity of users. Keystroke dynamics which refers to detailed typing pattern of a person is used to model user behavior and use the so formed footprint for user identification and intrusion detection. A neural network based system using monograph and digraph timings with digraph approximation and adaptation technique is proposed for keystroke dynamics in mobile devices for free text data. With adaptation mechanism, the missing monographs and digraphs and also the time bound variations of user keystroke time variations are captured and adapted. The combined use of digraph approximation and adaptation yields a False Acceptance Rate (FAR) and False Rejection Rate (FRR) of 0% for 22 users. The impact of adaptation on other performance measures like accuracy, specificity, sensitivity and Mean Square Error(MSE) is also studied.

Index Terms— Keystroke Dynamics, Intrusion Detection, Adaptation Mechanism, Keystroke Authentication.

I. INTRODUCTION

The popularity of the computing devices have soared at a much higher rate and mobile device are used more than desktop and laptop computers combined nowadays [1]. Along with the rise in the use of mobile devices the threats associated with them have also increased exponentially.

Intrusion can be defined as a sequence of related actions performed by a malicious adversary that result in the compromise of confidentiality, integrity or availability of a target system.[2] The basic objective behind intrusion detection is to verify users identity and allow access only to a valid user while denying access to an masquerader.

A password based authentication is the most widely used authentication mechanism being used [3]. The main issue with password based authentication is that an impostor can gain access to a system by using a stolen password, hence password authentication by itself doesn't guarantee a really secure mechanism for authenticating user. A strong method of authentication should utilize the following factors to achieve a secure authentication system. Following are the factors which needs to be addressed i) something we know ii) something we have iii) something we are [4].

Revised Version Manuscript Received on September 26, 2015.

Christy James Jose, Department of Electronics and Communication, Govt. Engg. College Barton Hill, Thiruvananthapuram, India.

Jijo Francis, Department of Electronics and Communication, Govt. Engg. College Barton Hill, Thiruvananthapuram, India.

Rajasree M.S, Director and Professor of Indian Institute of Information Technology and Management – Kerala, Thiruvananthapuram, India.

Biometric authentication along with password authentication can cover all these three factors and provide a secure authentication mechanism. There are two types of biometric authentication mechanisms. They are Physical and Behavioral biometric authentication mechanisms. Physical bio-metric relies on something which the users are. Such authentication will be done by making use of the physical characteristics such as facial features, palm prints, retina pattern, finger print, and iris pattern as well as hand geometry. It is based on some direct measurement of a part of the human body. Behavioral biometrics includes techniques such as signature, voice recognition and keystroke dynamics which are based on users behavior. Physical biometric authentication as well as signature and voice recognition cannot be used for continuous authentication hence keystroke dynamics is preferred.

There are two types of authentications. They are static and continuous authentication. Static authentication will authenticate a user only at the beginning of the session while in continuous authentication the user will be monitored and authenticated continuously throughout the session. Hence keystroke dynamics are used. The typing rhythm of any individual is unique just like their handwriting. Hence a user can be identified based on the habitual typing pattern. Keystroke dynamics can be combined with password authentication to get best results.

II. RELATED WORK

From the early 1980s keystroke dynamics as a biometric authentication have captured much interest among researchers. The oldest work related to keystroke dynamics is that of Gaines et.al [5]. As a part of Rands research project on Computer Security, sponsored by National Science Foundation, California, a study was conducted to determine whether statistical characteristics of typing of an individual is unique.

Ingo Deutschmann et al.[6] studied on the best methods for Continuous Authentication. Keystroke dynamics, Mouse movements and System footprint have been studied and their performance analyzed. It was deciphered that Keystroke dynamics was a better authentication technique when compared to Mouse movements and System footprint.

The work of Fabian et. al [7] is one of the earliest in the field of Keystroke dynamics in the early 1990s. A free text based approach wherein the user is authenticated for free text was introduced. The number of words per minute (wpm) was recorded and later clustering criterion based on a heuristic scheme of minimization of a performance index was used to validate an user. An acceptance rate of 80%, 85.6% and 90%

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

respectively were achieved for Euclidian distance measure, Non weighted probability and weighted probability measure respectively for free text data.

A method for keystroke dynamic authentication using typing style analysis is proposed in the works of John et.al [8]. Data were collected from valid and forger users. The signature pattern of the user from login username was captured. The best results were obtained when Inductive learning classier method was used. The minimum Type I error (FRR) obtained was 17% and minimum Type II error (FAR) obtained was 12%.

Fabian Monrose and Aviel D. Rubin works reflect key-stroke dynamic authentication of users based on feature sets determined through factor analysis[9]. The mean and standard deviation of the feature and its timings were captured. It was then compared with reference signature timings and classification done using different classifiers. The performance of Bayesian classifier was found to be superior over other methods with correct identification performance measure of 92.14% [9].

Livia C. F. Araujo et al. [11] proposed Key Code, Down-Down time, Down-Up time, Up-Down time as features using statistical classifier. The study has concluded that best results were obtained when all the four features were used simultaneously for keystroke authentication. The performance aspects considered were Familiarity of target string, 2 trial authentication, adaptation mechanism, timing accuracy and number of samples enrolled. An adaptation mechanism had been implemented for higher accuracy. A FRR of 1.45% and FAR of 1.89 % have been achieved for static authentication by this technique.

P. Campisi et al.[12] proposed a static keystroke dynamic authentication system using cellular keypads. Statistical classifiers with four time based key-stroke features Press Release(PR), Press Press(PP), Release Press(RP), Release Release(RR) were used. Template for each user was prepared by finding mean and variance of each feature and storing in database for verification. Normalization techniques was used for refinement in global distance and achieved EER as low as 13.15%.

Real intrusion data sets were used by Gissel Zamonsky Pedernera et al.[13] for focusing on intruder behavior. A technique based on digraph and trigraph times computed were implemented. R-distance, A-distance and Weighted A-distance were the distance measures used between sessions and Adapted K-means and Adapted Subtractive Clustering algorithms used. The use of the median instead of the mean and using features extracted from relations between several sessions instead of those taken from single sessions alone are some of the novel improvements implemented by Gissel et.al's work[13]. A hit rate of 80% was obtained for free text data using this technique.

M. S. Obaidat and D. T. Macchairolo introduced a new system to identify computer users using a multilayer neural network [14]. They experimented with three neural networks: a multi-layered feed forward network using back propagation algorithm, a sum of product network trained with back propagation algorithm and a hybrid architecture that combined the two. In terms of accuracy the back propagation network provided the highest accuracy of 97.5% while the hybrid sum of product developed by combining the two neural net-works gave an accuracy of 96.2% with lesser training times than both back propagation and sum of product neural net-works.

M. S. Obaidat and Balqies Sadoun [15] work authenticates an user based on password as well as static keystroke authentication. The concept of Hold time for keystroke dynamic authentication was proposed in this work. Previous techniques with neural network [14] used the feature of Inter-key time alone for capturing keystroke timings.

A new concept based on event sequences was implemented by Zahid Syed et al.[16] for authentication using key-stroke dynamics. They have come to an inference that there is not much correlation between typing proficiency of user and event sequence data and that event sequences have the potency to be used for keystroke dynamics for user authentication.

The work of J. Morris Chang et al.[17] focuses on using keystroke dynamics for active authentication based on the degree of disorder between the digraph times to cope up with time varying issues. They proposed a new concept called cognitive finger print for Keystroke dynamic authentication. It is based on the fact that same digraph part of two different words may differ(cognitive factor). The use of cognitive typing rhythm yielded an FAR of 0.055 and FRR of 0.007 which give more accurate results when compared to previous works.

A continuous authentication through keystroke dynamics with lower error rates was proposed by Ahmed A. Ahmed and Issa Traore. A new approach for free text analysis of keystrokes using monograph and digraph and neural networks to predict missing digraphs based on relation between monitored key strokes[10] was implemented. An FAR of about 0.0152% and FRR of about 4.82 % was achieved for free text data in their work.

III. METHODOLOGY

As the previous works point out there is a tradeoff between statistical classifier and neural network model for keystroke dynamic authentication. Statistical classifier methods have the advantage that they can be easily be adapted to a new user whenever a new user needs to be enrolled. At the same time it suffers from the lower FAR and FRR. On the other hand neural networks provide a better FAR and FRR but at the cost of time taken for retraining the network each time a new user is added.

The proposed approach is based on the works of Ahmed A. et.al [10]. The main advantage of our approach is that neural networks are used and the changes in genuine user's typing behavior due to improved typing proficiency is incorporated and missing monographs and digraphs are updated as and when the keys are typed. A neural network based fitting approach for the user under consideration is made use of.

Training needs to be done only for the particular user who needs authentication. Validation can be done by testing with other intruder data sessions. A neural network scheme using both monographs and digraphs will be used. A sorted time mapping technique with digraph approximation will be used as in the works of Ahmed A. et al.[10]. An improvement to

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

this method is proposed by inculcating an adaptation mechanism along with the digraph approximation which would significantly improve the user authentication through keystroke dynamics.

A. Design

The basic steps in implementing the neural network architecture is modeling monograph and digraph user profile followed by enrollment and verification as shown in Fig. 1. The following subsections elaborate the design principles used in this work.

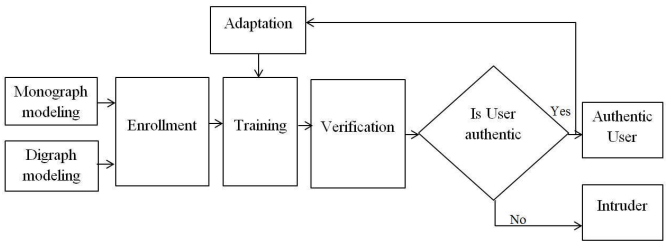

Figure 1. General Block diagram of Keystroke dynamics architecture

1) Sorted Time Mapping Table

Sorted Time Mapping (STM) is a technique used to prepare user profile. This mapping technique is used for preparing both monograph and digraph models which in turn will represent the user profile. Fig. 2 shows the basic block diagram of Sorted Time Mapping technique. The technique for preparing Sorted Time Mapping table is enumerated below:

(i)Process the raw keystroke data and divide it into monograph and digraph keystroke data.

(ii) Compute average keystroke timings for each key code for monographs. In case of digraphs compute average keystroke timing for each "To" key code irrespective of the "From" key code.

(iii) Sort the key codes based on the average keystroke timings in ascending order. This is done by sorting module

(iv) Assign key orders to each key code in the same order obtained in the sorted data. This is done in mapping module.

(v) The key code, key order and key timing information so obtained is sorted in database. This constitutes the Sorted Time Mapping Table for monograph as well as digraph keystroke data.

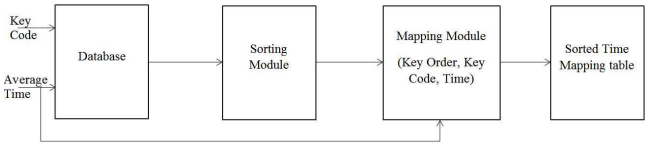

Figure 2. Basic steps of making STM

Table I and Table II illustrate an example of processing keystroke data and preparing a Sorted Time Mapping table from it. Table I shows four sample key codes with their average keystroke timings. This data is sorted in ascending order and the key orders assigned in the same fashion as the sorted data's order as illustrated in Table II. This constitutes an STM table.

TABLE I: Sample Keystroke data provided to sorting module

Key code	Average Time(ms)
65	101.2
66	21
67	56.23
68	17.5

TABLE II: STM for sample data

Key code	Key order
68	1
66	2
67	3
65	4

2) Monograph Modeling

Monograph is an event consisting of only a single key at a time. Monograph modeling consists of capturing monograph timings and preparing Sorted Time Mapping table for the monograph data.

Monograph timing of a key code can be computed as the time difference between key DOWN event and key UP event for that key code corresponding to the key which was pressed and released. Only alphabets, space, backspace and enter key is considered under the purview of this work. Only the available monographs will be used for preparing Sorted Time Mapping Table while the missing monographs will be left out from further verification.

With the new proposed adaptation mechanism the missing monographs will also be updated as soon as a valid user logs in the missing monograph data as some point of time. Such an approach is proposed to increase the accuracy of the system. An example of monograph user profile is illustrated by Table III.

TABLE III: Monograph user profile for sample data

Key order	Key code	Average hold Time(ms)
1	68	17.5
2	66	21
3	67	56.23
4	65	101.2

3) Digraph Modeling

A digraph is an event consisting of two consecutive key events. For capturing digraph data the raw data is taken, and the difference in timings of “UP” and “DOWN” key events gives the digraph time. Hence a digraph consists of a "From" key code, a "To" key code and the fly times between them.

Preparing a STM for Digraph is different from that of Monograph. Though a digraph consists of both "From" and "To" key codes only the "To" key codes are taken and the times added together and averaged irrespective of the "From" key codes. With the "To" key codes and average times computed, STM is prepared. It is impossible to have all possible combinations of digraphs. Hence the missing digraphs will be left out initially and later approximated by digraph approximation explained in following subsection. An illustration of digraph user profile is shown in Table IV.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

TABLE IV: Digraph user profile for sample data

(From, To) key order	Average Fly Time(ms)
(4,1)	20.3
(4,2)	18.4
(4,3)	-
(4,4)	-
(5,4)	41.5
(5,1)	12.2
(5,3)	48.3
(5,2)	-

4) Digraph Approximation

Digraph approximation is a novel feature introduced by the works of Ahmed A. et.al [10]. It is impossible to introduce all the possible combinations of various digraphs and its timings. Hence during verification stage most of the digraph data may be missing and this might result in an erroneous performance. In fact the usage of digraphs is a free text environment is even more challenging. Digraph approximation is the answer to all these problems.

TABLE V: Digraph user profile after Digraph Approximation

(From, To) key order	Average Fly Time (ms)
(4,1)	20.3
(4,2)	18.4
(4,3)	**54.4**
(4,4)	**36.8**
(5,4)	41.5
(5,1)	12.2
(5,3)	48.3
(5,2)	**22.6**

In this approach all the available digraphs from the raw data captured is first processed and STM prepared with them. Only the available digraphs will be listed initially. The missing digraphs will then be approximated to fill the void spaces. This is done by first training a digraph neural network and feeding the key orders to the neural network to obtain estimated fly times as output from the digraph neural network as illustrated in Fig 3. Table V shows a digraph user profile after digraph approximation. The values in bold depicts the approximated fly time.

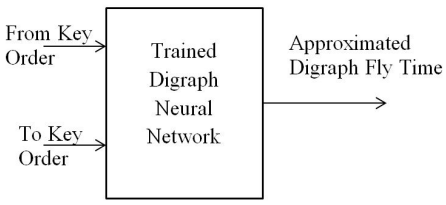

Figure 3. Illustration of basic block of Digraph Approximation

5) Enrollment

The process of enrollment is illustrated in Fig. 4. The monograph module consists of a feed forward neural network with one input node, one output node and a hidden layer consisting of 16 nodes. Digraph module consists of a feed forward neural network with two input nodes for the "From" and "To" key codes. There will be one output node and 40 hidden nodes in hidden layer.

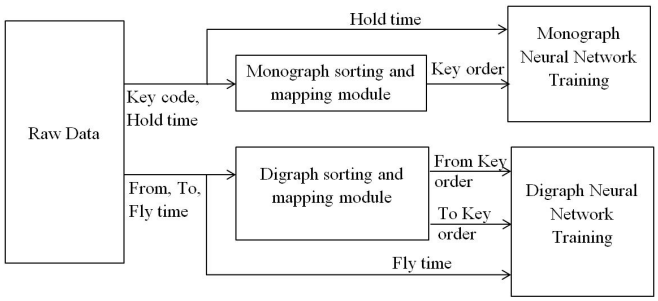

Figure 4. Illustration of User enrollment system

In both the modules Levenberg-Marquardt algorithm is used with tan-sigmoidal transfer function in hidden layer nodes and linear transfer function in input and output nodes. Neural network fitting approach is used for training both the neural networks for the given monograph and digraph user profiles. The number of epochs is fixed at 1000 for easy convergence.

6) Verification

Verification is the process whereby a user's session is authenticated through keystroke dynamics. The raw data captured from the user is processed to obtain monograph and digraph keystroke timings. The key order corresponding to each key code is fetched from the STM table of monograph and digraph for the respective networks.

The expected key stroke timings of monograph and digraph neural networks is then compared with the actual keystroke timings of the user to be authenticated and the deviations will be found out as shown in Fig. 5. The deviation of test user timing from the user profile timings will be combined and given to decision network to get the authentication result.

Monograph deviation and digraph deviation [10] is then combined using the equation (1).

$$D = B\,\delta_{mono} + (1\text{-}B)\,\delta_{di} \quad (1)$$

where $\delta_{di} = \dfrac{\sum_{i=1}^{N_{di}} \dfrac{|f_i - F_i|}{F_i} \times 100}{N_{di}}$

and $\delta_{mono} = \dfrac{\sum_{i=1}^{Nmono} \dfrac{|d_i - D_i|}{D_i} \times 100}{N_{mono}}$

D is the weighted percentage deviation and B is the dependability factor. The dependability factor decides how much weightage should be provided to the monograph or digraph neural network output. B=0 indicates purely digraph authentication while B=1 indicates purely monograph authentication. B=0.5 indicates equal weightage for both monograph and digraph neural networks. In this research work a dependability factor of 0.5 is used for a balanced performance. δmono gives absolute monograph deviation while δdi gives the absolute digraph deviation. Nmono and Ndi are the total number of monographs and digraphs in the session data set. di and fi are the hold and fly times for the ith mono and digraph records while Di and Fi are the hold and fly times of users keystroke data. The weighted percentage deviation D is then compared with a threshold to identify

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

whether it is an authentic user data or an unauthorized data. The optimum value of threshold is obtained from the ROC curve.

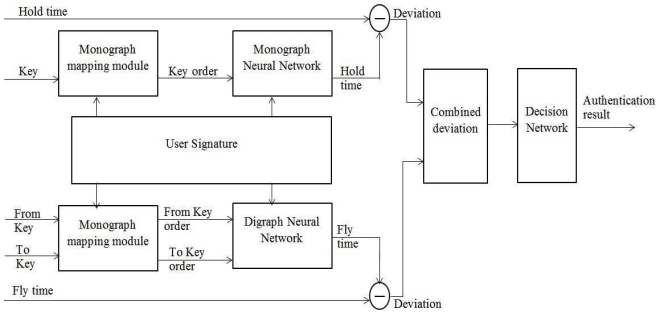

Figure 5. Illustration of User Verification process

7) Adaptation

Adaptation is a novel approach proposed in this research work. One of the major issues faced by traditional method is that once a neural network is trained with user data it cannot be modified. The typing speed or proficiency of a user may vary with time. A person who has a certain typing trait may show some variation at a different point of time. This could be due to improved typing proficiency at a later stage. Adaptation mechanism is an answer to this problem. This method is based on the assumption that a user's typing behavior won't change drastically. The basic block diagram of an adaptation mechanism is shown in Fig. 6.

The weighted percentage deviation for the given user is first computed in the verification stage. If the deviation is below optimum threshold value, data from the test user will be processed and monograph and digraph information extracted. This extracted monograph and digraph data will be added to the existing monograph and digraph user profiles. The key orders will be recomputed and the sorted time map reconstructed. With the new set of monograph and digraph data sets the monograph and digraph neural networks will be retrained. The newly updated weights of the neural network are proposed to achieve better classification result with lower error rates and better accuracy.

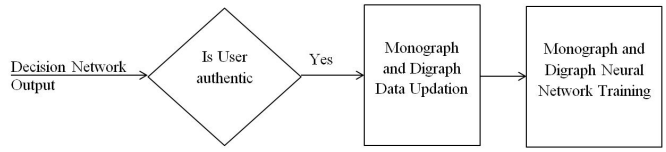

Figure 6. Block diagram of Adaptation mechanism

B. Experiment and Implementation

A mobile application with a custom keyboard has been developed to capture the keystroke data from mobile devices. Android is chosen as the development platform as it is widely used. The captured data captured is stored in XML format. The XML raw data is parsed and later processed to capture both monograph and digraph data. Fig. 7 shows the custom keyboard and the application developed for saving keystroke data.

The experiment is conducted with 22 users, one user being valid. The android .apk file is deployed in test user android mobiles and data retrieved from it. User's consists of both male and female users of various typing proficiency. A free text based data collection method is used in this approach. For this experiment numbers and special characters are excluded from the scope of this work. Once the data are collected two neural networks (both monograph and digraph neural networks) are trained with the data set of the authentic user. Training the neural network with the user data constitutes the enrollment stage. Once enrolled the efficiency of the network is tested with test data consisting of both authentic and non-authentic user data. The error rates are found out for evaluating the performance of the neural network.

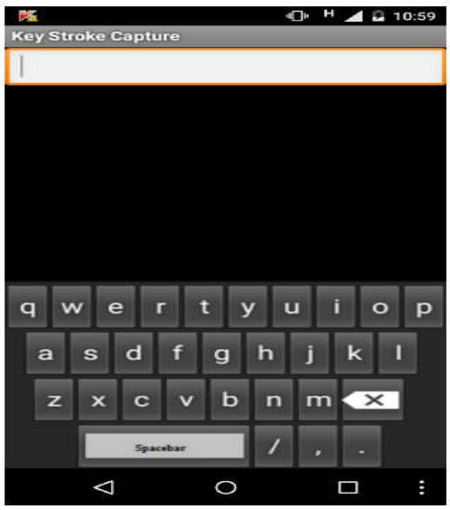

Figure 7 Mobile User Interface for capturing keystroke data

Testing the neural network is done in two stages. One stage consists of testing the test data with neural networks without adaptation. In the next stage the same test data is tested on the neural networks by incorporating the adaptation mechanism. The error rates resulting from both the testing stages are then compared to verify if there is any further improvement with the new proposed approach of adaptation. The dependability factor B is fixed at 0.5 while testing for providing a balanced weightage to both monograph and digraph neural networks. For measuring the performance of the two approaches ROC(Receiver Operating Characteristics) curve, AUROC(Area Under ROC curve), Sensitivity, Specificity, Accuracy and MSE are used.

Receiver Operating Characteristics curve is a fundamental tool for diagnostic test evaluation and is a plot of true positive rate against false positive rate for different values of threshold of a parameter. The best possible prediction method would yield a point in the upper left corner of the ROC space, representing 100% sensitivity and 100% specificity.

Sensitivity is the probability that a test result will be positive when the actual user class is validated while specificity is the probability that a test result will be negative when the actual user class is validated. Accuracy is the portion of the total number of prediction that were correct. Equation (2)-(4) gives the equations for computing specificity, sensitivity and accuracy. TP represents True Positive count, TN represents True Negative count, FP represents False Positive count and FN represents False Negative count.

$$\text{Sensitivity} = \frac{TP}{TP + FN} \qquad (2)$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

$$\text{Specificity} = \frac{TN}{FP+TN} \quad (3)$$

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+TN+FN} \quad (4)$$

The Area Under the ROC curve (AUROC) is equal to the probability that a classifier will rank a randomly chosen positive instance higher than a randomly chosen negative instance. An area under curve value of 1 indicates an excellent diagnostic test whereas a value of 0.5 has no information content. Mean Square Error(MSE) is the mean of the square of the difference between the actual user data and the predicted user timing data. Lower value of MSE indicates that predicted values of the neural network are close to the actual user input values. The MSE error for neural network is given by equation (5).

$$\text{MSE} = \frac{1}{N}\sum_{i=1}^{N}(dO(i)-mO(i))^2 \quad (5)$$

where N represents total number of predicted samples, dO represents desired output of neural network while mO represents model output.

IV. Experimental Results And Discussion

Result analysis is first done without using adaptation mechanism. Then adaptation is introduced and the results compared using various performance measures.

A. Result Analysis without Adaptation

The following results are based on keystroke dynamics analysis done using touchscreen mobile keyboard with data from 22 users. The data which is collected over a month is subjected to training as mentioned in the implementation stage. Intruder data as well as authentic user data is fed to neural network and the deviation is found out.

TABLE VI: Performance Measures of Keystroke dynamics without adaptation

Performance Measure	Value
Sensitivity	90.91%
Specificity	90.91%
Accuracy	90.91%
AUROC	0.9717
MSE	3.12×10^3

Fig. 8 shows ROC curve for the fitting network without using the proposed adaptation mechanism. Deviation from both monograph and digraph neural network is combined with equal weights given to both the neural network. The optimum ROC point from the ROC curve is for False Acceptance Rate(FAR) of 0% and a False Rejection Rate(FRR) of 9.09%. This is obtained for a threshold value of 64.12 %. An FAR of 9.09% and FRR of 0% is obtained at a threshold of 47.39%. The area under the ROC curve is 0.9917 which is close to 1, hence guarantees a good diagnostic test. Table VI summarizes the values of various performance measures computed without using adaptation mechanism.

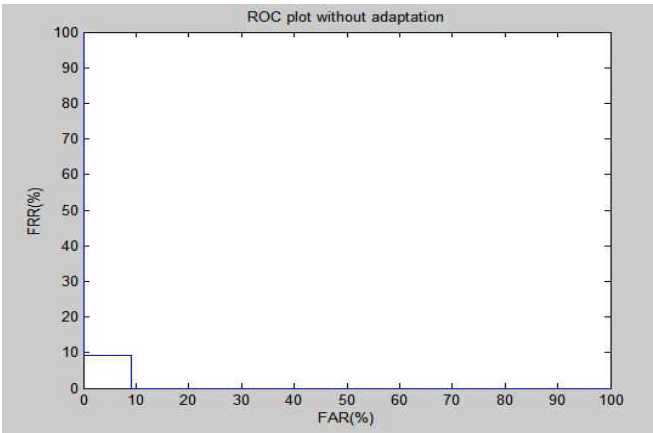

Figure 8. ROC plot without adaptation

B. Result Analysis with Adaptation

For analysis of keystroke dynamics with adaptation the same user data which was used for testing in the previous sub section is used. 22 users are validated. The users whose deviation from the genuine user profile within a stipulated threshold level is adapted using the adaptation mechanism where in the adapted data is added to the user profile database and the neural network retrained.

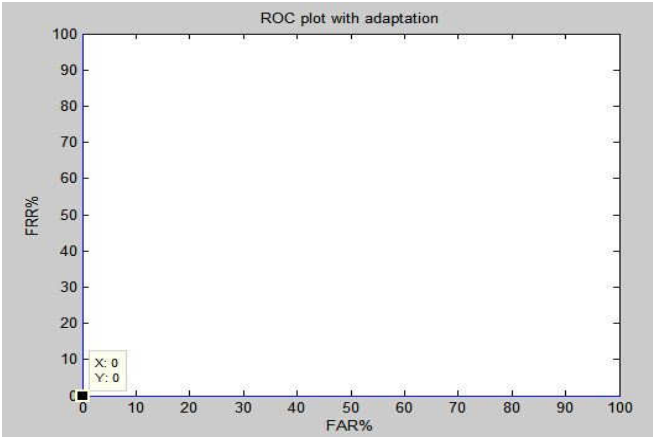

Figure 9. ROC plot with adaptation

Fig. 9 shows ROC curve for the neural network using the proposed adaptation mechanism. Deviation from both monograph and digraph neural network is combined with equal weights given to both the neural network. Following are the results obtained. The optimum ROC point from the ROC curve is for False Acceptance Rate(FAR) of 0% and a False Rejection Rate(FRR) of 0%. This is obtained for a threshold value of 21 %. The area under the ROC curve is 1 which is same as the ideal case, hence guarantees a good diagnostic analysis. Table VII summarizes the values of various performance measures computed with the adaptation mechanism.

TABLE VII: Performance Measures of Keystroke dynamics with adaptation

Performance Measure	Value
Sensitivity	100%
Specificity	100%
Accuracy	100%
AUROC	1
MSE	489

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

V. CONCLUSION

Keystroke dynamics can be used to supplement existing techniques to develop a robust intrusion detection system. In the implementation described, an attempt has been made to improve the performance of keystroke authentication system by including an adaptation mechanism. Authentication system with monograph and digraph, with digraph approximation gives the best results compared to previous works. In addition to digraph approximation a new technique of adaptation has been included and the performance measures compared.

As observed the Specificity, Sensitivity and Accuracy increased from 90.91% to 100% while using the proposed Adaptation mechanism over digraph approximation technique which is the best in class. The AUROC should be ideally 1 and use of Adaptation mechanism improved AUROC from 0.9717 to 1. Adaptation mechanism also drastically reduced the Mean Squared error from 3.12 x 103 to 489. The optimum ROC False Acceptance Rate(FAR) in both cases is 0% while False Rejection Rate(FRR) reduced from 9.09% to 0% while using Adaptation mechanism. The results clearly reflect an improvement with the new proposed approach of Adaptation mechanism which is used along with digraph approximation in mobile devices.

Keystroke dynamics has got wide scope for research and can be implemented to prevent unauthorized access by intruders. This work has been done with 22 users. Increasing the number of real user data and inclusion of techniques like event sequences holds great scope for future work.

REFERENCES

1. G. O. Young, “Synthetic structure of industrial plastics (Book style with paper title and editor),” in Plastics, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.
2. Canalys, “Smart phones overtake client PCs in 2011”, http://www.canalys.com/newsroom/smart-phones-overtakeclient-pcs-2011 , Feb. 2012.
3. Kruegel, Christopher, Fredrik Valeur, and Giovanni Vigna, “Intrusion detection and correlation: challenges and solutions”, Vol. 14, Springer Science & Business Media, 2005.
4. Clarke, Nathan L., and Steven M. Furnell. "Authentication of users on mobile telephones–A survey of attitudes and practices." Computers & Security 24, no. 7 (2005): 519-527.
5. Boatwright, Michelle, and Xin Luo. "What do we know about biometrics authentication?." In Proceedings of the 4th annual conference on Information security curriculum development, p. 31. ACM, 2007.
6. Gaines, R. Stockton, William Lisowski, S. James Press, and Norman Shapiro. “Authentication by keystroke timing: Some preliminary results”, No. RAND-R-2526-NSF. RAND CORP SANTA MONICA CA, 1980.
7. Deutschmann, Ingo, Peder Nordstrom, and Lina Nilsson. "Continuous authentication using behavioral biometrics." IT Professional 15, no. 4 (2013): 12-15.
8. Monrose, Fabian, and Aviel Rubin. "Authentication via keystroke dynamics." In Proceedings of the 4th ACM conference on Computer and communications security, pp. 48-56. ACM, 1997.
9. Robinson, John, Vicky M. Liang, J. Chambers, and Christine L. MacKenzie. "Computer user verification using login string keystroke dynamics." Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on 28, no. 2 (1998): 236-241.
10. Monrose, Fabian, and Aviel D. Rubin. "Keystroke dynamics as a biometric for authentication." Future Generation computer systems 16, no. 4 (2000): 351-359.
11. Ahmed A. Ahmed and Issa Traore, "Biometric Recognition based on free-text Keystroke Dynamics", IEEE transactions on cybernetics, vol. 44, no. 4, April 2014, 458-472.
12. Araújo, Lívia CF, Luiz HR Sucupira, Miguel Gustavo Lizarraga, Lee Luan Ling, and João Baptista T. Yabu-Uti. "User authentication through typing biometrics features." Signal Processing, IEEE Transactions on 53, no. 2 (2005): 851-855.
13. Campisi, P., E. Maiorana, M. Lo Bosco, and A. Neri. "User authentication using keystroke dynamics for cellular phones." Signal Processing, IET 3, no. 4 (2009): 333-341.
14. Pedernera, Gissel Zamonsky, Sebastian Sznur, Gustavo Sorondo Ovando, Sebastían García, and Gustavo Meschino. "Revisiting clustering methods to their application on keystroke dynamics for intruder classification." In Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2010 IEEE Workshop on, pp. 36-40. IEEE, 2010.
15. Obaidat, M. S., and D. T. Macchairolo. "A multilayer neural network system for computer access security." Systems, Man and Cybernetics, IEEE Transactions on 24, no. 5 (1994): 806-813.
16. Obaidat, Mohammad S., and Balqies Sadoun. "Verification of computer users using keystroke dynamics." Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on 27, no. 2 (1997): 261-269.
17. Syed, Zahid, Sean Banerjee, and Bojan Cukic. "Leveraging variations in event sequences in keystroke-dynamics authentication systems." In High-Assurance Systems Engineering (HASE), 2014 IEEE 15th International Symposium on, pp. 9-16. IEEE, 2014.
18. Chang, J. Morris, Chi-Chen Fang, Kuan-Hsing Ho, Nicholas Kelly, Pei-Yuan Wu, Yixiao Ding, Chris Chu, Stephen Gilbert, Ahmed E. Kamal, and Sun-Yuan Kung. "Capturing cognitive fingerprints from keystroke dynamics." IT Professional 15, no. 4 (2013): 24-28.

Christy James Jose is working as Associate Professor in the Electronics & Communication Engineering Department of Government Engineering College, Barton Hill, Trivandrum Kerala. He received his B Tech degree from the MG University and his M Tech from Kerala University. His areas of interest include Mobile Computing, Security and Distributed Computing. He is a life member of ISTE.

Jijo Francis received his Bachelor of Technology Degree from Sree Chitra Thirunal College of Engineering, Thiruvananthapuram. He is currently pursuing his Masters Degree at Govt. College of Engineering, Barton Hill, Thiruvananthapuram, India.

Dr. Rajasree MS, received the Ph.D degree in Computer Science and Engineering, from Indian Institute of Technology, Madras. She has been the Professor an d head, Department of Computer Science in College of Engineering, LBS Institute of Technology for Women, Thiruvananthapuram . She is a Member of IEEE, ACM, CSI and a life member of ISTE. Currently she is the Director and Professor of Indian Institute of Information Technology and Management – Kerala

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.