International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 24th Mar 2020. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-03

Title: **OVERVIEW ON BIOMETRIC BASED DELICATE COMPUTING METHODS FOR CLIENT VERIFICATION**
Volume 09, Issue 03, Pages: 45-58.
Paper Authors

SHAIK RAZIA, ARPITA ROY, MOHAMMED ALI HUSSAIN

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

OVERVIEW ON BIOMETRIC BASED DELICATE COMPUTING METHODS FOR CLIENT VERIFICATION

***SHAIK RAZIA, **ARPITA ROY AND *** MOHAMMED ALI HUSSAIN**
*Associate Professor,**Assistant Professor,*** Professor,
Koneru Lakshmaiah Education Foundation University, Vaddeswaram
razia28sk@gmail.com,arpitaroy@kluniversity,alihussain.phd@gmail.com

ABSTRACT:
Nowadays security of data and passwords is a major challenge for the mankind. Therefore, the need to solve this issue is growing rapidly and we are always in the need to come up with some better security techniques. Till date the security of passwords using biometric is considered the best option. This paper revolves around a survey of different keystroke biometric techniques for password authentication. In this paper a detailed study of various artificial intelligence techniques is done that includes the domain of neural networks, genetic algorithms, fuzzy rule-based systems, statistical analysis, support vector machine and hybrid systems. The researches in each domain are discussed in detail. From the results it can be concluded that techniques involving neural networks and genetic algorithm give low error rate and higher accuracy, though, fuzzy rule-based systems and support vector machine have lesser complexity factors. However, this result is not absolute.

Keywords: Artificial Neural Networks, Fuzzy Rule-Based Systems, Genetic Algorithms, Support Vector Machine, Password Authentication, Keystroke Biometric

1. INTRODUCTION
With the advent of time, new technologies and innovations came into existence. Computers have become the most important part of the society. With the discovery of the new technologies, somewhere the security is compromised. New ways to stop any hindrance to the security is the biggest challenge of today‘s world. As in our modern society, we rely too much on computers and store our sensitive information on it; it had become more and more necessary to protect our systems from intruders. In the year 2011, there was an online attack on various companies, which resulted in their network shutdown and secure data of millions of users were compromised. Normally we use simple password based authentication technique to protect our data from the unauthorized access. Such text-based techniques used for the authentication process are vulnerable to common attacks like shoulder-surfing, hidden cameras and hackers etc. To overcome such problems an advanced technology dealing with biometric schemes are in use. Although these techniques are effective but still use of these biometrics techniques like thumb impression, facial recognitions, retinal scan, finger prints detection, digital signatures etc requires certain supplementary and expensive tools,

which results in rapid increase in cost. To overcome these problems, there is a need of the simple and low cost technique for the security of the systems and data. In this study we are discussing the techniques for the user authentication by using individual's behavioral characteristics where the characteristics like typing pattern, time and speed of a particular person, which can be obtained using basic input device- keyboard, are monitored.

There are basically two categories of attacks on system: Active attack and Passive attack.

1. Active attacks: Such attack includes non-authentic users which change the existing data stream or creates new invalid data streams. These are further divide into 4 different types: masquerade, replay, modification of message, and denial of service. a. Masquerade: This type of attack occurs when one user fakes its identity to be the different user. b. Replay: This occurs when intruder capture the actual data sequence and retransmit it later pretending as the authentic user. c. Modification of message: This simply involves the process of changing or modifying some part of the original message, which is to be transmitted. d. Denial of service: In this case, the messages get delayed which give an unauthorized result.

2. Passive Attacks: Eavesdropping or snooping on transmission of messages basically considered as passive attacks. The goal here is to access the information that is being transmitted in the system. There are two categories of the passive attack are: a. Release of message content. b. Traffic Analysis: Here the attacker can discover the location and identity of original host.

This paper contains the review of various studies on ―User Authentication based on Keystroke Dynamics‖ on different Soft Computing domain, i.e., Neural Networks, Genetic Algorithm, Fuzzy Rule-Based Systems, Statistical Analysis, Support Vector Machine (SVM) and Hybrid Systems. In this paper the most important studies that have been done in selected soft computing domains during the last 20 years are highlighted with special attention to last 5 years. The main focus of this paper is to bring all the important studies done on user authentication using keystroke over the last 20 years under one roof and compare the studies based on different domain of soft computing.

This paper has been organized as follows: In the second section Keystroke Dynamics definition and the studies on user authentication based on keystroke dynamics using soft computing are detailed. In section three, the studies are classified based on their domain, i.e., Neural Networks, Genetic Algorithm, Fuzzy Rule-Based Systems, Statistical Analysis, Support Vector Machine (SVM) and Hybrid Systems, and they are detailed accordingly. In the fourth section, conclusions are discussed. Section four contains the Conclusion of this paper. At the end, the references from which this paper is reviewed are presented.

2. KEYSTROKE DYNAMICS

Livia C.F. Arujo, Luiz H.R Jr. and Miguel, Lee L Ling, (2005) proposed a system that used the static key stroke dynamics in the

user authentication. This system took the time of key up and down as input and the ASCII codes of each key pressed was captured while typing the string. The main features used to analyze and perform the various experiments were: a. Key code b. Latency c. Key duration It Recognized 3 types of users a. Genuine user b. Imposter user c. Observer Imposter user After the successful authentication with some sample data the proposed system created the new updated template that included new samples and discarded the oldest one. The False Rejection Rate (FRR) of this system was: 1.45 percent and False Acceptance Rate (FAR) was 1.89 percent. [33]

In 2007, Rajkumar Janakiraman and Terence Sim proposed a system to detect whether Keystroke Dynamics is feasible to be used as a biometric in a setting where users continue with their normal daily activities of emailing, web surfing, and so on. They also proposed a new Goodness Measure for computing the standard of a word used for Keystroke Biometrics. The Held Time (Ht), Interkey Time (It), Sequence and Feature Vector (Ft) were captured from the user‘s key press behavior and the probability density function (pdf) was estimated from the samples of Sequence collected and this pdf was represented as a Histogram. Two types of Classifiers were used for the identification of the user. Classifier A was intended to recognize a person from a single sample of a sequence arising in the keystroke data. On the other hand, Classifier B was intended to identify a person from multiple samples of the same sequence arising in the keystroke data. The result of this study was divided into two categories:

Result I - For Sequences that are English Words:

SEQUENCE	MEAN OF ACCURACY	STANDARD.DEVIATION OF ACCURACY
FOR	0.0598	0.1224
TO	0.0838	0.1841
THE	0.0562	0.1504
YOU	0.0512	0.0733
IS	0.0538	0.0432
IN	0.0573	0.0669
AND	0.0878	0.2682
OF	0.0991	0.2809

Results II - For Non-English Sequences:

	Y	ACCURACY
FOR	0.7955	0.2319
TO	0.9455	0.1184
THE	0.8409	0.2443
YOU	0.7364	0.2985
IS	0.9591	0.0796
IN	1.000	0.0000
AND	0.8318	0.2191
OF	0.8000	0.1927

From the tables it was evident that the Classifier B outperformed Classifier A. [9]

In 2009, Patrick Bours and Hafez Barghouthi gave a new technique of authentication which they called Dynamic Authentication or Continuous Authentication. In this technique they monitored whether the current user was the same as the user who performed the initial static authentication. For the continuous authentication they designed a penalty-and – reward function to measure the confidence that the user had not changed during a session. The authenticity of a user was checked in two steps: firstly for static authentication, then for dynamic authentication. In static authentication, if a person provided an input that too far from his own template then it was called False Non Match and if a person provided an input that was so close to another person‘s template that these two matched then it called False Match and the probability of occurrence of these errors was expressed in False Non-Match Rate (FNMR) and False Match Rate (FMR). Continuous Authentication was done on the basis of how a user used the system as normal during a longer period of time instead of typing a fixed text a number of times. During that period of time information was collected and template was created on how a user used the keyboard and the average duration and latency time was calculated together information about the stability. The confidence level was implemented by using a penalty and reward function C which was initialized to 0 at the start of the session. If the timing information was correct the value of C was increased and if it was incorrect the value of C was decreased. Special care was taken to see that the value should not become negative. Experimental Results showed that the average number of keystrokes needed to lockout an intruder varied between 79 and 348. This showed that an intruder was locked out fairly quickly. Future research could be done on continuous authentication system by combining keystroke dynamics with mouse usage. [10]

Arik Messerman, Tarik Mustafi´c, Seyit Ahmet Camtepe and Sahin Albayrak (2011) provided a non-intrusive identity verification scheme based on behavior biometrics where keystroke dynamics based-on free-text was used continuously for verifying the identity of a user in real-time. In this study, the scalability was improved and an adaptive user model was provided through which the solution took the change of user behavior into consideration in verification decision. Also, a new distance measure was identified which enabled the researchers to verify identity of a user with shorter text. Each evaluation run was prepared by learning the minimum number of required user events per profile (initial enrollment). This initial state was then used separately for attacking and testing purposes.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

The result suggested that the short response times must be highlighted with respect to our daily-use scenario. The number of false results was reduced by this method. [1]

In 2011, Emanuele Maiorana, Patrizio Campisi, Noelia González-Carballo, Alessandro Neri discussed the viability of applying keystroke dynamics to execute user authetication on mobile phones. The advantage of utilizing template selection techniques for keystroke authentication was also explored. In the process it was presumed that the timestamps produced by the mobile phone, and associated to press and release events of a key, could be obtained and worked on. Four different approaches were taken into account for template selection: a) Minimum Distance Criteria (MDIST) – The authors sorted the set of the N keystroke acquisitions that were obtained according to their mean distance from the other ones and selected the E dynamics analogous to the least mean distances as characteristic for the user. b) Greedy Maximum Match Score (GMMS) – This motioned to reduce the overall distance between the set of the E elected templates and the set of the N- E non utilized accessions. c) Agglomerative Complete Link Clustering Approach - This approach could be susceptible to the choice of eccentricity, if there in the actual set of accessions. d) Fuzzy C-means Clustering Algorithm – It was employed for template selection in signature biometrics.

m	(external Far) eFAR	(internal Far) iFAR	FRR
1	0.73%	0.66%	9.48%
2	1.66%	1.33%	3.45%
3	2.61%	2.61%	1.84%
Execution Time (ms)	409	457	554

In January 2018, Junhong Kim, Haedong Kim and Pilsung Kang studied different Keystroke Dynamics based password authentication methods and proposed a new KDA method for freely typed text based on a user-adaptive feature extraction method and machine learningbased novelty detection algorithms. Here the authors considered the typing speeds of two consecutive keys (digraphs) to define a changeable set of user-dependent keystroke features. The experiment was executed in two languages (Korean and English) and done with 150 participants and 13,000 keystrokes per user. The suggested system gave the best equal error rate of 0.44. The authentication performance was increased by 45.35% for Korean and 39.00% for English using this procedure. [45]

3. CLASSIFICATION BASED ON DOMAIN OF WORK

3.1 NEURAL NETWORKS

M. S. Obaidat and B. Sadoun in 1997 explained the use of keystroke dynamics for verifying computer systems and networks access using the keystroke dynamics of computer user‘s login string as characteristic patterns using pattern recognition and neural

network techniques. It used Pattern Recognition Techniques, like Kmeans Algorithm, Cosine Measure Algorithm, Minimum Distance Algorithm, Bayes' Decision Rule, Potential Function and Neural Network techniques, like Back propagation Neural Network (BPNN), Counter propagation Neural Network (CPNN). It also used Fuzzy ARTMAP, Radial Basis Function Network (RBFN), Learning Vector Quantization (LVQ) Network, Reinforcement Neural Network (RNN), along with Sum of Product Network (SOP), Hybrid Sum of Product (HSOP) Network in the process. A better accuracy result was obtained when considering hold times alone than that when inter-key times were considered only. From the results it was observed that the most successful neural network algorithms had better classification accuracy as compared to the most successful traditional pattern recognition techniques. This means that using neural network to identify computer users was not just plausible but was very successful. [21]

In 2008, Hai Wang and Shouhong Wang stated that the traditional text based schemes for user authentication had some drawbacks. No verification table was needed in the neural network approaches to authenticate the password. There was no verification table that was required for this purpose; rather, it encrypted the neural network weights that were stored in the system. Long training and recall approximation times were the limitation that already existed in layered neural network techniques. Hopfield neural network approach was applied to authenticate the user. Hopfield neural network was used here for optimization problem solution and pattern recognition. The password authentication scheme proposed by Hai Wang at el. was divided into three parts A. Recognition procedure. a) Choose ID and password first. b) System computed the encrypted passwords using algorithms. c) Id and password were converted to bit binary numbers. d) N-bit number was used to train n-node Hopfield neural network by modifying weights. e) N-bit number was used to update the HNN. B. Login Authorization process. a) User Provided Id and passwords b) System captured encrypted password. c) Id and password converted to p-bit pin code. d) Weight was adjusted according to HNN. e) If N-bit code was provided as input to HNN was matched with the output then the user was authorized else rejected. C. Password change procedure.

a) First user needed to perform the whole authorization procedure. b) Then needed to follow the registration process to change the password. Hopfield neural network provided better accuracy and quicker response time to registration and password change. [39]

3.2 GENETIC ALGORITHM

Ki-seok Sung and Sungzoon Cho (2006), discussed about user authentication based upon the typing behavior of the user, called the keystroke dynamics. Here the timing vector composing of the duration the key was pressed or released was taken into account. Thus, Genetic algorithm wrapper based approach was followed which used

the fitness function. In this paper Sung and Cho also proposed for the addition of uniqueness term in the fitness function of genetic algorithm, which measured for each chromosome how different it was from other chromosomes. Uniqueness of xth chromosome was defined as an arithmetic average of S distances to all other chromosomes. Finally, the fitness of chromosome x was defined as a simple sum of accuracy and uniqueness: Fitness(x) = A(x) + U(x). [41]

Shanmugapriya. D, Dr. Padmavathi. G. in the year 2013 discussed the keystroke dynamics to be the behavioral biometrics technology that recognized the legitimacy of the user as the user worked on a keyboard. The above mentioned paper used a new feature called virtual key force algorithm with commonly used extra timing features. Here the features were normalized by using Z-Score methods. The proposed techniques for feature subset selection were wrapper based approach using Ant Colony Optimization- Extreme Learning Machine with Analytic network process (ACOELM-ANP) and Genetic Algorithm- Extreme Learning Machine with Analytic network process (GA-ELM-ANP). Here the methodology was divided into three phases a. Feature Extraction Phase b. Normalization phase c. Feature subset Selection Phase Basic steps of algorithm ACO-ELM-ANP were:
a) Extracted the duration, latency and digraph. b) Initialized the number of ants based on the iterations. c) Took a random value for each ant, and compared the value that it should not be selected previously. Then subsets were generated for each ant. d) Using ELM-ANP the selected subset for all ants was calculated. e) The values of phenomenon according to step d were modified. f) The old ants were removed and new ones were generated. g) Steps c to f repeated until the iterations were finished. h) The best feature was set as globally best. The main factors considered here to calculate the time factor were: Feature duration, Flight Time, latencies, digraph, tri-graph and virtual key force measures. [4]

3.3 FUZZY RULE-BASED SYSTEMS

Salvador Mandujano and Rogelio (2004) proposed a system which was based upon a clustering, which was described to improve the user authentication and to determine the password sharing using the technique of fuzzy cmean algorithm. In this system c-mean was used to train the individuals, based upon the user‘s behavior by entering the passwords through keyboards using keystroke dynamics. These c- mean profiles used the DES (Data Encryption Standard) encryption technology, which used the actual password as key and all passwords were read at the time of logging in using the mechanism of access control, so that the user‘s identity could be validated. By using the additional variables in the authentication equation the password sharing and password stealing had been reduced by using the c - mean technique. This made the security of password authentication process more

reliable and stronger as compared to the traditional text based password security systems. [40]

In 2015, Bindiya Bansal, Kulwinder Singh studied on how to enhance the intrusion detection system performance by the use of fuzzy rule base. They also checked the severity of attacks. This study was carried out in three steps. First step was the identification of critical factors. This was the initial and most important step of fuzzy inference process as whether an intruder has entered into the network or not was checked in this step. This was done by using five factors: Existence, Sequence, Partial Order, Duration and Interval. Fuzzification was done in the second step. This phase involved the designing of the fuzzy expert system for the identification of attacking behavior and severity of attacks. In this phase, input and output variables were defined. Third step was for Fuzzy Rule Construction. The rule in the fuzzy system is in simple if-then statements. Finally, Fuzzy Inference Rule Generation was done in the fourth step. The fuzzy set of attack and range was assigned. Attack had four fuzzy sets namely Null, Low, Medium and High. The range for null was in between 0 to 2.5, for low was in between 2.2 to 5.3, for medium was in between 5 to 7.7 and for high was in between 7 to 10. This system reduced the false alarm rate and increased performance of system. This fuzzy rule based system was scalable because it provided consistency in performance and reliability with regards to the increased traffic over the network. [25]

3.4 STATISTICAL ANALYSIS

In 2012, Romain Giot and Mohamad El-Abed and Christophe Rosenberger provided a new kind of dataset in which users had typed both an imposed and a chosen pairs of logins and passwords and presented a statistical analysis of well known assertions such as the relationship between performance and password size, impact of fusion schemes on system overall performance, and others such as the relationship between performance and entropy. A dataset was created of genuine samples and imposter samples by collecting data over email from the students of school of engineering and some of their colleagues. The Equal Error Rate (EER) was individually computed for each user and, its averaged value was presented under EERi. EERg presented the EER with the same threshold for all the users (EER was computed with a global intra-scores and inter-scores set). [29]

E A Kochegurova, E S Gorokhova, A I Mozgaleva, in 2017, had written a paper related to creating a keystroke dynamics recognition algorithm and developing a software, which is able to identify users according to their keystroke dynamics. The authors had created an algorithm based on probabilistic-statistical method for the authentication of the users. In the process two users attempted for authorization using their keystroke dynamics. 20 attempts were made out of which the first user succeeded 17 times and the second user succeeded 18 times. Thus the result said 0.875% accuracy of the proposed system. [46]

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

3.5 SUPPORT VECTOR MACHINE (SVM)

Romain Giot, Mohamad El-Abed, Baptiste Hemery, Christophe Rosenberger (2011) proposed a new method based on the Support Vector Machine (SVM) learning satisfying industrial conditions in which few samples per user were needed during the enrollment phase to create its template. In this method, users were authenticated through the keystroke dynamics of a shared secret (chosen by the system administrator). The GREYC keystroke database was used that was composed of a large number of users (100) for validation purposes. Experimental results show that, even though the computation time to build the template could be longer with this method (54 seconds against 3 seconds for most of the others), its performance outperformed the other methods in an industrial context. [8]

In 2011, Deian Stefan, Xiaokui Shu, Danfeng (Daphne) Yao studied the effects of synthetic forgery attacks in the context of biometric authentication systems. Their study was mainly focused in evaluating the security of keystrokedynamics authentication against synthetic forgery attacks. The analysis was performed in a remote authentication framework called TUBA that was designed and implemented for monitoring a user‘s typing patterns. Classifications in the experiments were done with the help of Support Vector Machine (SVM). It was found that the classification was robust against synthetic forgery attacks, using the first-order Markov chain model. [42]

3.6 HYBRID SYSTEMS

In 2000, Sajjad Haider, Ahmed Abbas, Abbas K. Zaidi presented a suite of techniques for password authentication using neural networks, fuzzy logic, statistical methods, and several hybrid combinations of these approaches. Their study presented approaches using typing biometrics of a user, along with the conventional login information, to identify a user. In their study, various combinations of statistical, neural, and fuzzy techniques for valid user authentication were implemented and compared. In this system genuine user was differentiated from an intruder using the inter-key delays of the password typed by the user. [28]

Pilsung Kang, Sungzoon Cho, in 2009, proposed a hybrid novelty score to improve conventional nearest-neighbor-based novelty detectors. In the proposed novelty score the average distance to the neighbors was combined with the distance to the convex hull of those neighbors. Though Local Topology was neglected in conventional nearest-neighbor-based algorithms, density along with local topology was incorporated in the method proposed by Kang and Cho. [22]

4. CONCLUSION

Password based authentication technique is the most common authentication technique people use nowadays. Several studies and techniques have been done over the years to improve the security of passwords in our systems. Some of the studies done in the field of Soft Computing for password authentication are briefed in this survey. The

studies are briefed under the category of Keystroke Dynamics Neural Network, Genetic Algorithm, Fuzzy Rule Based Systems, Statistical Analysis, Support Vector Machine and Hybrid Systems. The aim, methodology used, results and limitations of the studies are discussed in this review. The Error rate, False Acceptance Rate and False Rejection Rate of the studies are also stated in this review. From the study it can be summarized that Neural Network and Genetic Algorithm are considered to be a good approach to solve the problems of password authentication because of their lower error rate and higher accuracy, although they have higher complexity factor compared to fuzzy rule-based systems or support vector machines. As a future work we can perform password authentication using keystroke dynamics using Fuzzy Rule Based Intelligent System. We can conclude that these approaches can lead to an increased security of the systems by giving a more trustworthy technique for password authentication in a very economical way as no additional hardware is needed here besides a standard keyboard and can soon replace the costly techniques of password authentication like fingerprint detection, retinal scan, etc.

REFERNCES

[1] ArikMesserman, TarikMustafi´c, SeyitAhmetCamtepe and SahinAlbayrak,"Continuous and Non intrusive Identity Verification in Real-time Environments based on Free-Text Keystroke Dynamics" IEEE ©2011

[2] RomainGiot, Mohamad El-Abed, Christophe Rosenberger, "Keystroke Dynamics Authentication ForCollaborative Systems".

[3] Attila Mészáros, ZoltánBankó, LászlóCzúni, "Strengthening Passwords by Keystroke Dynamics"IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 6-8 September 2007, Dortmund, Germany

[4] D. Shanmugapriya,and G. Padmavathi,"An Efficient Feature Selection Technique for User Authentication using Keystroke Dynamics"IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.10, October 2011

[5] P. Campisi E. Maiorana M. Lo Bosco A. Neri, "User authentication using keystroke dynamics for cellular phones" IET Signal Processing · August 2009

[6] Fabian Monrose, Michael K. Reiter, Susanne Wetzel, "Password Hardening Based on Keystroke Dynamics" © ACM, 1999

[7] Patrick Bours, "Continuous keystroke dynamics: A different perspective towards biometric evaluation" Elsevier Ltd., 2012

[8] Romain Giot Mohamad El-Abed Christophe Rosenberger, "GREYC Keystroke: a Benchmark for Keystroke Dynamics Biometric Systems" ENSICAEN,

6 Boulevard MaréchalJuin, 14000 Caen CedexFrance

[9] Rajkumar Janakiraman and Terence Sim, "Keystroke Dynamics in a General Setting" Springer-Verlag Berlin Heidelberg 2007

[10] Patrick Bours and Hafez Barghouthi, "Continuous Authentication using Biometric Keystroke Dynamics" The Norwegian Information Security Conference (NISK) 2009

[11] FrancescoBergadano, DanieleGunetti, and ClaudiaPicardi, "User Authentication through Keystroke Dynamics" ACM Transactions on Information and System Security, Vol. 5, No. 4, November 2002

[12] Yu ZhongYunbin Deng, Anil K. Jain, "Keystroke Dynamics for User Authentication" Approved for Public Release; Distribution Unlimited.Cleared for Open Publication on 3/26/2012.

[13] Sylvain Hocquet, Jeans-YvelRamel, and Hubert Cardot, "User Classification for Keystroke Dynamics Authentication" SpringerVerlag Berlin Heidelberg 2007

[14] Emanuele Maiorana, Patrizio Campisi, Noelia González-Carballo, Alessandro Neri, "Keystroke Dynamics Authentication for Mobile Phones" 2011 ACM 978-1-4503-0113-8/11/03

[15] Fabian Monrose, Aviel D. Rubin, "Keystroke Dynamics as a Biometric for Authentication" Elsevier Science B.V, 2000

[16] Hyoung-joo Lee, Sungzoon Cho, "Retraining a keystroke dynamics-based authenticator with impostor patterns" Elsevier Ltd., 2006

[17] Sally Dafaallah Abualgasim, Izzeldin Osman, "An Application of the Keystroke Dynamics Biometric for Securing PINs and Passwords" World of Computer Science and Information Technology Journal (WCSIT) Vol. 1, No. 9, 2011

[18] Sungzoon Cho, Chigeun Han, DaeHee Han, Hyung-Il Kim, "Web based Keystroke Dynamics Identity Verification using Neural Network" Journal of Organizational Computing and Electronic Commerce, Vol. 10, No. 4, pp. 295307, 2000.

[19] Kenneth Revett , Florin Gorunescu, Sergio Tenreiro et al, "A machine learning approach to keystroke dynamics based user authentication", in Int. J. Electronic Security and Digital Forensics, Vol. 1, No. 1, 2007

[20] Preet Inder Singh, Gour Sundar Mitra Thakur, "Enhanced Password Based Security System Based on User Behavior using Neural Networks"I.J. Information Engineering and Electronic Business", 2012, 2, 29 35 Published Online April 2012 in MECS

[21] M. S. Obaidat and BalqiesSadoun, "Verification of Computer Users Using

Keystroke Dynamics" IEEE TransactionsOnSystems, Man, And Cybernetics—Part B: Cybernetics, VOL. 27, No. 2, April 1997

[22] Pilsung Kang, Sungzoon Cho, ―A hybrid novelty score and its use in keystroke dynamicsbased user authentication", 2009 Elsevier Ltd.

[23] Enzhe Yu and Sungzoon Cho, "GA-SVM Wrapper Approach for Feature Subset Selection
in Keystroke Dynamics Identity Verification" IEEE, 2003

[24] Willem G. de Ru and Jan H.P. Eloff, "Enhanced Password Authentication through Fuzzy Logic" IEEE EXPERT 1997

[25] BindiyaBansal, Kulwinder Singh, "Rule Based Intrusion Detection System to Identify Attacking Behaviour and Severity of Attacks" International Journal of Advanced Research in Computer Science and Software Engineering,Volume 5, Issue 1, January 2015

[26] N.L.Clarke, S.M.Furnell, "Authenticating mobile phone users using keystroke analysis" Springer-Verilag 2006

[27] Pilsung Kang, Sungzoon Cho, "A hybrid novelty score and its use in keystroke dynamicsbased user authentication" Elsevier Ltd., 2008

[28] SajjadHaider, Ahmed Abbas, Abbas K. Zaidi, "A Multi-Technique Approach for User Identification through Keystroke Dynamics"2000 IEEE

[29] RomainGiot and Mohamad El-Abed and Christophe Rosenberger, "Web-Based Benchmark for KeystrokeDynamicsBiometricSystems: A Statistical Analysis" http://www.epaymentbiometrics.ensicaen.fr/

[30] Pin ShenTeh, Andrew Beng Jin Teoh, Thian Song Ong, Han Foon Neo, "Statistical Fusion Approach on Keystroke Dynamics" Conference Paper · IEEE Xplore, January 2008

[31] Fabian Monrose, Aviel Rubin, "Authentication by Keystroke Dynamics" in IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 12 Issue 12, December 1997 , Page 1217-1222

[32] Pusara Maja, Brodley Carla E.,"User ReAuthentication via Mouse Movements" VizSEC/DMSEC'04, Washington, DC, USA. ACM 1581139748/ 04/0010, , October 29, 2004

[33] Araujo, L.C.F.; Sucupira, L.H.R., Jr.; Lizarraga, M.G.; Ling, L.L.; Yabu-Uti, J. B T, "User authentication through typing biometrics features", Signal Processing, IEEE Transactions on , vol.53, no.2, pp.851,855, Feb. 2005

[34] Seong-seob Hwang, Sungzoon Cho, Sunghoon Park, ―Keystroke dynamics-based authentication for mobile devices", 2008 Elsevier Ltd

[35] Ziran Zheng, Xiyu Liu, Lizi Yin and Zhaocheng Liu, ―A Stroke-based Textual Password Authentication Scheme ―in First International Workshop on Education Technology and Computer Science. 2009

[36] Seong-seob Hwang, Hyoung-joo Lee, Sungzoon Cho, "Improving authentication accuracy using artificial rhythms and cues for keystroke dynamics-based authentication", 2009 Elsevier Ltd

[37] Singh, S.; Arya, K. V., "Key Classification: A New Approach in Free Text Keystroke Authentication System", Circuits, Communications and System (PACCS), 2011 Third Pacific-Asia Conference on , vol., no., pp.1,5, 17-18 July 2011

[38] Epp C , Lippold Michael, and Mandryk R. L., "Identifying Emotional States using Keystroke Dynamics", Department of Computer Science, University of Saskatchewan, CHI 2011, Vancouver, BC, Canada. Copyright 2011 ACM 978-1-4503-0267-8/11/05, May 7–12, 2011.

[39] Shouhong Wang; Hai Wang, "Password Authentication Using Hopfield Neural Networks‖, Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, vol.38, no.2, pp.265,268, March 2008

[40] Mandujano, S.; Soto, Rogelio, "Deterring password sharing: user authentication via fuzzy c-means clustering applied to keystroke biometric data", Computer Science, 2004. ENC 2004. Proceedings of the Fifth Mexican International Conference in, vol., no., pp.181,187, 20-24 Sept. 2004

[41] Sung Ki-seok and Cho Sungzoon, "GA SVM Wrapper Ensemble for Keystroke Dynamics Authentication", in IAPR International Conference on Biometrics, 5-7 January 2006, Hong Kong.

[42] Deian Stefan, Xiaokui Shu, Danfeng (Daphne) Yao, ―Robustness of keystrokedynamics based biometrics against synthetic forgeries", 2011 Elsevier Ltd.

[43] SHAIK RAZIA, M.R.Narasingarao, "Development and Analysis of Support Vector Machine Techniques for Early Prediction of Breast Cancer and Thyroid" JARDCS (Journal of Advanced Research in Dynamical and Control Systems), ISSN: 1943-023X, Vol.9.Sp.Issue:6 page no: 869-878, 2017.

[44] Shaik Razia, P.Swathi Pryathyusha, N.Vamsi Krishna "A Comparative study of machine learning algorithms on thyroid disease prediction" International Journal of Engineering and Technology(UAE), ISSN

No: 2227-524X, Vol No: 7, Issue No: 2.8, Page No: 315-319, March 2018.

[45] Kim, Junhong & Kim, Haedong & Kang, Pilsung, "Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection", Applied Soft Computing, 62. 10.1016/j.asoc.2017.09.045

[46] E A Kochegurova, E S Gorokhova, A I Mozgaleva, ―Development of the Keystroke Dynamics Recognition System", J. Phys.: Conf. Ser. 803 01207