Biometric Keystroke Authentication: A Survey

*[1]Firdous Kausar, [1]Alanoud Mohammad AlAbdulhadi, [1]Areen Nasser AlYahya,
[1]Sarah Abdullatif AlSarami
Department of Computer Science, College of Computer and Information Science,
Imam Mohammad bin Saud Islamic University, Riyadh, Saudi Arabia
[1], Corresponding Author firdous.kausar@ccis.imamu.edu.sa

Abstract

As the dependence on computers and computer networks has been increasing, the need for authentication has increased. Many technologies exist for authentication such as using passwords, smart cards, and biometric. Biometric authentication methods rely on common biological characteristics such as fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, Keystroke Dynamics (KD), DNA and signatures. KD is one of behavioral biometrics, and it depends on two main factors: the pattern of rhythm and speed of typing. It can be easily applied to into the existing computer without requiring any special sensor or hardware, it just needs a keyboard. In this survey, we are going to observe a collection of KD algorithms to try to find a best outcome based on special measurements for these algorithms.

Keywords*: Biometric Keystroke, Authentication, biological characteristics, Keystroke Dynamics, behavioral biometrics*

1. Introduction:

Keystroke Dynamics (KD) is part of a class of biometrics known as behavioral biometrics, and this biometric belongs to user authentication approach, which it is under computer security field.

A definition of computer security based on The NIST [1] Computer Security Handbook [NIST 95]: "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)". This definition provide three key goals that are the core for computer security: confidentiality, integrity and availability, which can be summarized by "CIA". A failure of a system to guard any of these features accounts to a security destruction or weakness [1] [2].

1. User Authentication

User authentication is the process of checking claimed identity before the release of safe resources, and forestalling unauthorized access. The authentication can be achieved by matching unique short-form provided by an individual. This short-form divided into three categories: knowledge, token and biometrics as summarized in Table 1 and discussed as follow [3] [4]:

Knowledge: Something the individual knows. It often comes in the form of a personal ID or a password. It has been used to access systems in the past three decades. Effortless and high acceptance is main advantages for Knowledge. However, it includes a gap in information security because ease of loss or stolen as a result of bad behavior for most people [1] [4].

Token: Something the individual possesses, such as credit card and devices nanoparticles. It is a famous way because it is cheap, simple and deployment. Nevertheless, its limited use because ease of loss and stolen and not a safe the whole time [1] [4].

∗ Corresponding Author
Received: Nov. 11, 2015, Revised: Jan. 04, 2016, Accepted: Jan.17, 2016

Biometric: Something the individual is (static) or does (dynamic). Biometric technologies are defined as automated methods for checking or perceiving identity of individual in view of physiological or behavioral characteristics. It is the most protected and standard authentication tool. It cannot be lost, stolen, or overheard, and in the nonappearance of physical destruction, they provide a possibly guaranteed way to determining someone's identity [1] [5] [6].

1.1. Physiological biometrics: are a person's physical characteristics such as fingerprints, face, and iris. It is unique and high accuracy, also cannot change. However, it may suffer from low acceptance in public and the cost of equipment may be higher [7].

1.2. Behavior Biometric: Feature depend on what a person does, or how the person uses the body because each person has a unique pattern in how they interact with a computer equipment. Behavioral characters include audio, signature and rhythms of typing. Further, they do not need for user interaction significantly. Therefore, in general it is accepted more than physiological biometrics. However, they are typically substandard compared to physiological biometrics in terms of variability (voice changes along with aging factor) and may consequently influence in verification precision [7] [8].

Table 1. Overview of different User Authentication approaches [4]

Approach	*Advantage*	*Disadvantage*	*Example*
Knowledge	Effortless High acceptance	Forgotten Shoulder spoofing	Password PIN
Token	Cheap Simple deployment	Lost and theft	Smart card Mini devices
Biometrics	Deter sharing Unique Unforgettable	Cost Invasive	Fingerprint Voice Keystroke

Authentication process based on two steps: Identification step and Verification step. Identification step is giving an identifier to the security system (Identifier should be allocated carefully, because authenticated identities are the foundation for other security services, such as access control service.). Verification is creating authentication information that confirms the matching between the entity and the identifier [1].

2. Keystroke Dynamic (KD)

KD Authentication is a way to identification and verification based on the rhythms and patterns of the typing on the keyboard. It is a type of behavioral biometrics because the bio factor (what the user is doing). The first appearance was through the so-called "fist the sender," in World War II by military intelligence to find out who sent Morse code [4] [7] [9].

KD systems work in two different modes: identification mode (training) and verification mode (testing). Identification is the process of attempting to know the person's identity through analyzing a biometric pattern calculated from the person's biometric features. A person's identity is checked in the verification mode. "The pattern that is verified is only compared with the person's individual template" [3]. Keystroke verification techniques divide into two approaches: static and dynamic (continuous). Static verification approaches analyze keystroke verification attributes only at particular times giving extra security than the traditional username/password, for instance through the user login sequence. Static approaches afford more robust user verification than simple passwords nevertheless the detection of a user change after the login authentication is impossible. Dynamic verification, on conflicting, displays the user's typing behavior throughout the progression of the interaction. "In the Dynamic process, the user is monitored on a regular basis throughout the time he/she is typing on the keyboard, allowing a real time analysis" [3]. It implies that even after a fruitful login, the typing patterns of a person are continually dissected and when they don't coordinate the user's profile, access to the system is blocked. Verification phase is decision process in which the system chooses whether the feature extracted from the given typing pattern of password matches with the template of the requested person. In order to give an unequivocal answer of access acceptance or rejection [3] [10].

Feature extraction is the process of transforming the biometric data to feature vector, which can be utilized for classification. The KD have several feature those are as follow: Di-graphs, Tri-graphs, N-graph, Overall typing speed, Rate of errors (how often the user has to use backspace), The tradition of using additional keys in the keyboard, The order that user press keys when writing capital letters, (is shift or the letter key released first?) and The power used when pressing keys while typing (requires a specific keyboard). Overall typing speed and rhythm depend on the person, for example, writing the series of letters "the" for a person who's fluent in English will be faster than other person who's fluent in French [10].

Di-graphs, which are the time latencies between two following keystrokes. This type is normally used. It is divided in two types: Dwell Time (DT) and Flight Time (FT). DT is the length of time when you press on the key. DT can be calculated by $DT_n = R_n - P_n$ as shown in

Figure **1**, and n indicates the position of the proposed DT. The total number of timing vector of DT (V_{DT}), that can be find as follow [4]:

$$V_{DT} = \{DT_1, DT_2, \dots, DT_s\} \qquad (1)$$

where s means the summation of characters in a string [4].

FT is the length of time to release current key and pressure on the following key. FT may occur in four different forms and the formula to compute each form are listed in this way [4]:

$$FT_{Type,1} = P_{n+1} - R_{n,} \qquad (2)$$

$$FT_{Type,2} = R_{n+1} - R_{n,} \qquad (3)$$

$$FT_{Type,3} = P_{n+1} - P_{n,} \qquad (4)$$

$$FT_{Type,4} = R_{n+1} - P_{n,} \qquad (5)$$

as shown in

Figure **1**, and n indicates the position of the proposed FT. The total number of timing vector of FT (V_{FT}), that can be produced is shown as follows [4]:

$$V_{FT} = \{FT_1, FT_2, \dots, FT_s\} \qquad (6)$$

where s means the summation of characters in a string. Further, when you type a string of characters, the time between the first character and finding the right character is flight time, whereas the time during which was the key is pressed is dwell time.

Tri-graphs, which are the time latencies between every three following keys, and likewise [4] [9].

N-graph is defined as the timing extent between three or more sequential keystroke events. "It is better known as the elapse time (ET) between a key and the nth key event of a typing string" [4]. Notwithstanding many combinations of ET, but it can be extracted; next equation is the most commonly used when n-graph is concerned [4]:

$$ET_K = P_{K+n} - P_K, \qquad (7)$$

P denoted to the time stamp of pressing a character, and n indicated to nth number of graphs employed, where k means status of the intended elapse time. The total number of timing vector of ET in n-graph shown as follow [4]:

$$V_{ET} = \{ET_1, ET_2, \dots, ET_{S-n+1}\}_{,,} \qquad (8)$$

s indicates to the summation of characters in a typing sequence [4].

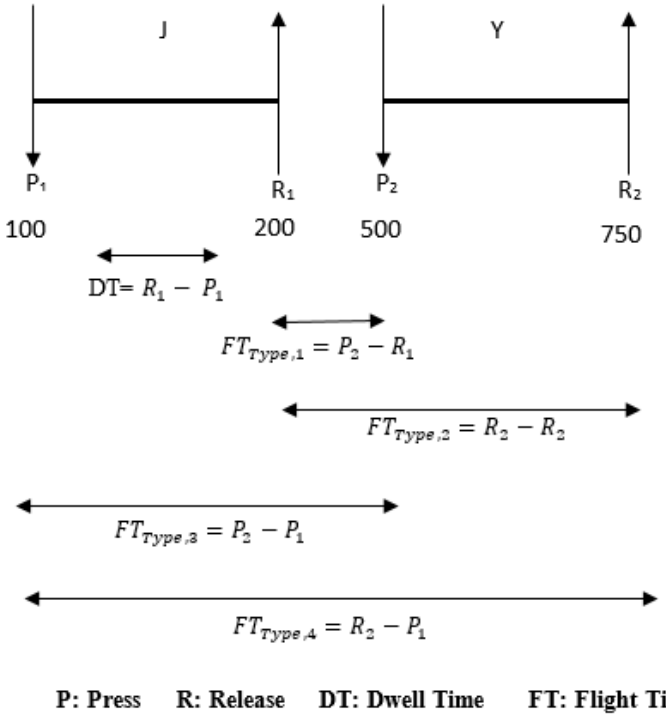

Figure 1. Relationship between Dwell Time and Flight Time [4]

Evaluating the effectiveness of KD depends on its ability to discover the real user and placebo user. This evaluate is based on three metrics [4] [10].

False Rejection Rate (FRR): "Is used to measure the rate of the system to reject the authorized person"[13]. Also it known as False Nonmatch Rate (FNR) or Type 1 error [4] [10].

$$FRR = \frac{NFR}{NAA} \times 100\% \qquad (9)$$

NFR is denoted as the numbers of false rejections; NAA is total proportion of users [4] [10].

False Acceptance Rate (FAR): It is accepted ratio (rightful users). "It is measure the ability of the system to accept the unauthorized person"[13]. Also, called False Match Rate (FMR) or Type 2 error [4] [10].

$$FAR = \frac{NFA}{NIA} \times 100\% \qquad (10)$$

NFA is denoted as the number of false acceptances respectively; NIA is total proportion of users [4] [10].

Equal Error Rate (EER): This metric used to determine the overall accuracy and compare the results with results of the other systems. Also known as Crossover Error Rate (CER) [4].
Figure 2 explains the relationship between FAR, FRR and EER.

Zero-Miss False-Alarm Rate (ZMFAR): It is another way to evaluate the effectiveness of KD which is defined as "The rate of false rejections when no impostors are accepted" [11].

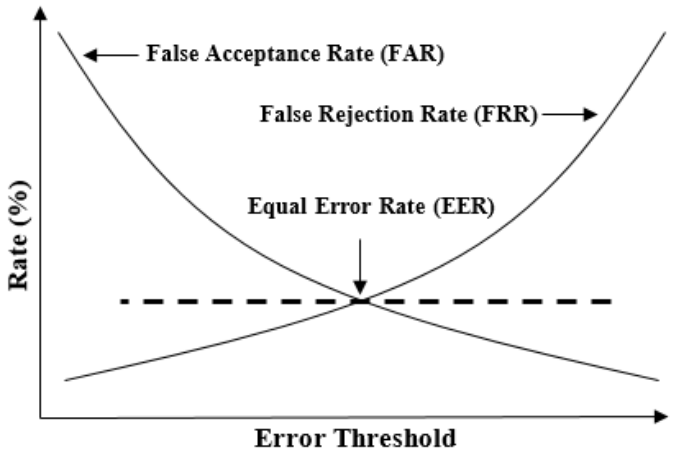

Figure 2. Relationship between FAR, FRR and EER [6]

In additionally, to determine and evaluate suitability of keystroke dynamic use seven criteria are as follows [7] :

1. **Universality:** Anyone who has a keyboard will be able to use KD [7].
2. **Uniqueness:** Because behavioral biometrics cannot be used as an absolutely unique measure for each person. Therefore, to make KD succeed, it should use unique writing style [7].
3. **Permanence:** One of the constraint of KD is that we can get different rhythms from day to day, because it is affected by (tiredness, switching computers (keyboard layout), mood, influence of alcohol and medications, etc...) [7].
4. **Collectability:** It does not need any special equipment, like other biometrics. The keyboard is enough to use as a standard to collect required data from user [7].
5. **Acceptability:** The user accepts *keystroke dynamic authentication*.
6. **Circumvention:** It is not difficult to be receive a password entered through the keyboard by keylogging software. Therefore, the implementation of KD will be a protection to data by matching input keyword with the keyword in the algorithm [7].
7. **Performance:** Behavioral biometrics affected by external factors such as working environment and fatigue, compared with physiological biometrics [7].

2. KD Authentication Methods

Access control to system by password is a popular way of authentication. KD can be added as a secondary identification method in order to increase the security [12].

Keystroke authentication has two different types of typing: Static and Dynamic. Static is referring to the examination of the user at the initial stage, for instance, authentication at the “log in” phase. While Dynamic is referring to that the examination of the user after the initial stage, for instance, after logon [4] [13].

Messerman et. al [14] mentioned the challenges that they faced during their study, which are alteration in human conducts, scalability and response time.

Types of sequence are digraph, trigraph and n-graph. Digraph latency is the timing between two sequent keystrokes. While trigraph latency is the timing between three sequent keystrokes. N-graph is similar to trigraph [9] [15]. Sim et. al [15] approved in their study that digraph is discriminable.

Over the last three decade, keystroke biometrics researches have been applying different methods which are classified to: statistical approaches, machine learning approaches, and others [2].

2.1. Statistical approach:

Statistical methods depend on calculating statistical measures which are mean, median and standard deviation, statistical t-test, and k-nearest neighbor. "Simplicity, ease of implementation, and low overhead" [4] are factors of computing the probability of the statistical methods [4].

Killourhy et. al [16] employed 14 classifiers: Euclidean, Euclidean (normed) , Manhattan, Manhattan (filtered), Manhattan (scaled), Mahalanobis, Mahalanobis (normed), Nearest-neighbor (Mahalanobis), Neural-network (standard), Neural-network (auto-assoc), Fuzzy-logic, Outlier-counting (z-score), Support vector machines (SVM) (one-class), and k-means. These algorithms were tested and compared with each other according to the lowest error rates on their own data. The research consisted of 51 users (one is authorized and the rest are intruders). In the training phase, the authorized user had to write the password 200 times in order to make the classifier monitors the authorized user's typing behaviour. In the testing phase, the classifier was operated on the timing vector for authorized user (wrote the password 200 times) and the 50 intruders (each one wrote the password 5 times) to capture the anomaly scores. They found that the best results according to: 1) zero-miss false-alarm rate (ZMFAR) was achieved by the Nearest Neighbor (Mahalanobis) classifier with 46.8%, 2) EER was achieved by Manhattan (scaled) classifier with 9.6%.

Zhong et. al [9] proposed keystroke biometrics algorithms which are based on new distance metric adjoining with Nearest Neighbor classifier. The aim of the study was to improve the accuracy of KD using static text. The new distance metric was a combination of Mahalanobis distance and Manhattan distance which was having the advantages of both of them. The authors gather the feature from 51 users. The features that they concerned about: the dwell time and latencies between two sequential keys. The outcome of their research was 8.7% EER and 42.3% ZMFAR. They compared their study with the result in [16]. They had succeeded higher results than [16].

Cho et. al [17] used in their study the Multilayer Perceptron (a special type of Neural Network Algorithm) for identity verification. They apply their work on the World Wide Web (WWW). The password length was 7 characters or more. There was 21 users as a part of the experiment. Each user had to enter the password 150 to 400 times and the last 75 timing vector was handled by the testing phase. 15 imposers had to generate 75 timing vector which was added to the authorized users' testing timing vector which make the total 150 timing vector. They notice that 62% users have perfect authentication and the FRR was 1.0%

Kang et. al [18] employed Retraining Module in their study. The authentication classifier that they operate was K-Means algorithm which was depending on Euclidian distance. They used two different approaches to update the training dataset: "moving window" and "growing window" to make the classifier adapts to the typing behavior changes. The training dataset stored two different features: duration and interval. The study was consisting 21 participants. The EER average outcome using the fixed window was 4.8%. Where the EER average using the moving window and growing window had the same outcome with 3.8%. This meant was to take more time than the fixed window by 1%.

Curtin et. al [19] concerned with long-text inputs (600 characters). In the feature extraction phase, they applied two methods: outlier removal and feature standardization. In order to take decisions, they made use of Nearest Neighbor classifier using Euclidean distance. The study was tested on 8 individuals who gone through the experiment 3 times, each experiment has its own factors. In the first experiment the Recognition accuracy accomplished 100%, while the second 98.5%, and the third 97%. Then they added 22 individuals to the experiment, and the accuracy of 30 individuals was 94.7%. Where the accuracy was 98.0% for the 8 original individuals from 30 individuals.

2.2. Machine Learning Approach:

Machine Learning methods share the same concept of authenticating and classifying keystrokes and taking decisions according to stored data [4].

Shanmugapriya et. al [13] had to gather a dataset with 103 users' typing for three well known keywords (drizzle, jeffrey allen and pr7q1z). Dwell time, Flight Time, Di-graph and Tri-graph were computed by the time pressing and releasing which are stored in the dataset for each user. The new concept that the authors used is the Virtual Key Force. Virtual Key Force was calculated by "the typing speed and behavior of the user on the key board" [13] with no additional tools. In addition, they applied Genetic Algorithm and Backpropagation Neural Network in their study. They tested the dataset with

the Virtual Key Force without. They obtained more accurate results for the three keywords with more than 1%. They also noticed that training and testing time were decreased.

Haider et. al [20] followed the Evolutionary Computing techniques. They concerned in "feature's duration, latency, digraph and their combination of each user keystrokes" [20]. In the training phase, they applied three different algorithms independently to extract unique features for each user: 1) Particle swarm optimization (PSO), 2) Genetic Algorithm and 3) Ant Colony Optimization. While Back Propagation Neural Network was employed in classification phase. The experiment was involved 27 users. 100 samples from each user were tested in 7 days. The results shows that Ant Colony Optimization is the best with 0.059% average classification error and 92.8% accuracy.

Sheng et. al [21] implemented Parallel decision tree algorithm and Monte Carlo. Their study was based on static authentication. .The user is authenticated if there are three or more decision trees. Wavelet transforms was used in order extract the feature and store it in the dataset. Eight decision tree were constructed in the training phase using the dataset attached to other simulated data. For each user has its parallel decision tree which is constructed from the eight decision trees. The reason why they use Monte Carlo method to deal enormous dataset because of adding new users. 43 volunteers were provided in the training data and the tested data. The tested string was 37 length which was entered 9 times by each user. The testing dataset didn't need special equipment to construct. 9.62% FRR and 0.88% FAR were the results of their study.

Sang et. al [10] applied Support vector machines (SVM) as pattern matching method to improve the "keystroke pressure-based typing biometrics for individual user's verification" [10]. The study contained two datasets: training dataset and testing dataset which included two unique information for each user: "maximum pressure exerted on the keyboard and time latency between keystrokes" [10]. The experiment contained 5 groups of people. Each person had to enter the password 200 times (100 times for training and 100 times for testing). The password length was 6 character. The average of the training time is very short with less than 0.5 second. The calculating of the FAR in the closet sit conditions was 0.95% whereas FAR in the open set was 14.7%. FRR was 5.6%.

2.3. Hybrid Combinations Approach:

In the paper [22] the authors' study is about checking if the user is the one that he/she claimed to be, and to measure the performance of proposed approaches. They proposed 7 methods: Fuzzy Logic, Neural Network, Statistical Techniques, and the combination of these approaches. They used the intra-key delays (6 vectors which is each vector had two letters and the delay time between them) that improved the performance. The Training dataset was storing the user name, 7 length password (each user chose his\her own and wrote it 15 time). They compute the "probability of being rejected when the user is valid" [22] and" probability of being accepted when the user is a stranger or intruder" [22] for each method. They noticed that the hybrid combinations and the intra-key delays improved the performance. The disadvantage in their research that when the user records the password wrongly, the system can't handle the error (the user should rewrite the password).

Bleha et. al [23]used in their study two classifiers, the minimum distance classifier and the Bayes classifier. The study divided into two parts. In the first part, they gathered the dataset from 9 users in 9 weeks. In the second part, 10 users want through the identification system testing in 5 weeks, while 26 users want through the verification system testing in 8 weeks. The outcome of the 10 users in the identification system testing was 1.2% indecision error. In verification system testing the outcome was 8.1% FRR, 2.8% FAR. The results for all the users that had participated (32 users) 3.1% FRR 0.5% FAR.

3. Comparative Analysis

Table 2 displays the measurement computed for each method. The measurement are: False Rejection Rate (FRR), False Acceptance Rate (FAR), Equal Error Rate (EER), Zero-Miss False-Alarm Rate (ZMFAR), Training Time, Testing Time, Accuracy Rate and Error Rate. Further, the Timing is measured in second (sec). Additionally, this table provides a general view that helps to compareing between these methods, and determining which the best outcomes.

Table 2. Comparative between KD methods

	Methods	***FRR (%)***	***FAR (%)***	***ERR (%)***	***ZMFAR (%)***	***Training Time (sec)***	***Testing Time (sec)***	***Accuracy (%)***	***Error Rate (%)***
[16]	Manhattan (scale)			9.6	60.1				
[16]	Nearest Neighbor (Mahalanobis)			10	46.8				
[9]	Nearest Neighbor classifier, combination of Mahalanobis distance and Manhattan distance			8.7	8.4				
[17]	Multilayer Perceptron (Neural Network Algorithm)	1							
[18]	Retraining Module, K-Means, Euclidian distance			3.8					
[13]	Genetic Algorithm and Backpropagation Neural Network + Virtual Key Force					6	0.019	90.7	
[20]	Particle swarm optimization, Back Propagation Neural Network					.00021	0.00041	88.9	0.063
[20]	Genetic Algorithm, Back Propagation Neural Network					.030	0.00048	86.6	0.078
[20]	Ant Colony Optimization, Back Propagation Neural Network					.015	0.0004	92.8	0.059
[21]	Parallel decision tree, Monte Carlo	9.62	0.88						
[10]	Support vector machines (SVM)	5.6	Close Set: 0.95 open set: 14.7			0.4188			
[23]	the minimum distance classifier, the Bayes classifier	3.1	0.5			1.2	8.1		

4. Conclusion

The survey is focused on KD authentication witch is a part of behavioural biometrics authentication. It is economical and can be easily used into the current computer security systems with minimum change and user interaction. However, it degraded in performance when utilized over time. Therefore, the survey helping to find a better outcome between comparative methods. The result of survey as follows: The best result of the FAA was by Multilayer Perceptron (Neural Network Algorithm), and it was achieved by Chou et. Al [23]. Bleha et. Al [23] could found the lower percentage of FAR by two classifiers, the minimum distance classifier nearby the Bayes classifier. The best percentage for the ERR was earned by Nearest Neighbor (Mahalanobis) by Killourhy et. al [14]. Also, the greater outcome of ZMFAR accomplished by Killourhy et. al [14] through Manhattan method. The lower Training Time, Testing Time, Accuracy Rate and Error Rate were by Haider et. al [18] with 0.00021 sec for Training, 0.00041 sec for testing, 92.8% for Accuracy and 0.059 for Error Rate which the experiment produced by the Particle swarm optimization classifier, Back Propagation Neural Network classifier.

5. References

[1] W. Stallings and L. Brown, COMPUTER SECURITY PRINCIPLES AND PRACTICE, 2ed ed., New Jersey: Pearson Education, Inc., publishing as Prentice Hall., 2012, pp. 62- 65.

[2] H. Systems, "Hitachi-id.com," 2015. [Online]. Available: http://hitachi-id.com/concepts/security.html. [Accessed 9 November 2015].

[3] D. Shanmugapriya and G. Padmavathi, "A Survey of Biometric keystroke : Approaches, Security and Challenges," *International Journal of Computer Science and Information,* vol. 5, no. 1, pp. 115-119, 2009.

[4] P. S. Teh, A. B. J. Teoh and S. Yue, "A Survey of Keystroke Dynamics Biometrics," *The Scientific World Journal,* vol. 2013, no. 2013, pp. 1-24, 2013.

[5] F. Monrose and A. D. Rubin, "Keystroke dynamics as a biometric for authentication," *Future Generation Computer Systems,* vol. 16, no. 4, p. 351–359, 2000.

[6] S. Bajaj and S. Kaur, "Typing Speed Analysis of Human for Password Protection (Based On Keystrokes Dynamics)," *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* vol. 3, no. 2, pp. 88-91, 2013.

[7] biometric-solutions.com, "Keystroke Dynamics," 2015. [Online]. Available: http://www.biometric-solutions.com//solutions/index.php?story=keystroke_dynamics. [Accessed 28 Sep 2015].

[8] Behaviosec.com, "Technology | Behaviosec," behaviosec, 2015. [Online]. Available: http://www.behaviosec.com/technology/. [Accessed 9 November 2015].

[9] Y. Zhong, Y. Deng and A. K. Jain, "Keystroke dynamics for user authentication," in *(CVPRW),* Providence, RI , 2012.

[10] W. Martono , H. Ali and M. J. E. Sala, "Keystroke Pressure-Based Typing Biometrics Authentication System Using Support Vector Machines," in *Computational Science and Its Applications – ICCSA 2007,* O. Gervasi and M. L. Gavrilova , Eds., Berlin, Springer Berlin Heidelberg, 2007, pp. 85-93.

[11] S. A. Ryan, "MOBILE KEYSTROKE DYNAMICS: ASSESSMENT AND," December 2014.

[12] D. Umphress and G. Williams, "Identity Verification through Keyboard Characteristics," *Int'l J. Man-Machine Studies,* vol. 23, no. 3, p. 263–273, 1985.

[13] D. Shanmugapriya and G. Padmavathi, "VIRTUAL KEY FORCE - A NEW FEATURE FOR KEYSTROKE," *International Journal of Engineering Science and Technology,* vol. 3, no. 10, pp.

7738-7743, 2011.

[14] A. Messerman, T. Mustafi, S. A. Camtepe and S. Albayrak, "Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics," in *Int'l Joint Conf. on Biometrics (IJCB)*, Washington, DC, 2011.

[15] T. Sim and R. Janakiraman, "Are digraphs good for freetext keystroke dynamics?," in *Computer Vision and Pattern Recognition*, Minneapolis, 2007.

[16] K. S. Killourhy and R. A. Maxion, "Comparing Anomaly Detectors for Keystroke Dynamics," in *Proc. 39th Annual Int'l Conf. on Dependable Systems and Networks (DSN- 2009)*, 2009.

[17] S. Cho, C. Han, D. H. Han and H.-I. Kim, "Web-based keystroke dynamics identity verification using neural network," *Journal of Organizational Computing and Electronic Commerce*, vol. 10, no. 4, p. 295–307, 2000.

[18] P. Kang, S. -s. Hwang and S. Cho, "Continual retraining of keystroke dynamics based authenticator," in *Advances in Biometrics*, vol. 4642, Springer Berlin Heidelberg, 2007, pp. 1203-1211.

[19] M. Curitn, M. Villani, G. Ngo, J. Simone, H. S. Fort and S. -H. Cha, "Keystroke Biometric Recognition on Long-Text Input: A Feasibility Study," in *IWSCCS 2006*, Hong Kong, 2006.

[20] M. Karnan and M. Akila, "Personal authentication based on keystroke dynamics using soft computing techniques," in *Proceedings of the 2nd International Conference on Communication Software andNetworks (ICCSN'10)*, Singapore, 2010.

[21] Y. Sheng, V. V. Phoha and S. M. Rovnyak, "A parallel decision tree-based method for user authentication based on keystroke patterns," *IEEE Transactions on Systems, Man, and Cybernetics B*, vol. 35, no. 4, p. 826–833, 2005.

[22] S. Haider, A. Abbas and A. K. Zaidi, "A multi-technique approach for user identification through keystroke dynamics," in *IEEE Int'lConf. on Systems, Man and Cybernetics*, Nashville, 2000.

[23] B. S, S. Charles and H. B, "Computer-access security systems using keystroke dynamics," *Pattern Analysis and Machine Intelligence*, pp. 1217-1222, Dec 1990.