ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 11(46), DOI: 10.17485/ijst/2018/v11i46/139332, December 2018*

Password Security Enhancement using Dynamic Keystrokes. A Review

Arifa Awan*, Shahzad Nizamani and Noor Zaman

Mehran University of Engineering and Technology Jamshoro, Sindh, Pakistan;
arifa.awan05@gmail.com; shahzad.nizamani@gmail.com, nooruzaman@gmail.com

Abstract

Backround: These days growing more comfortable authentication techniques in computer, protection is a biggest task. In latest years, keystroke biometric verification system has been an lively region of study because of its short fee and simplicity of combination with computer safety systems. Keystroke analysis (KA) validation systems are a much less general shape of get entry to controller, despite the fact that they may be gaining recognition. Keystroke Analysis are the specific timing facts which describes precisely whilst every key modified into pressed. Keystroke dynamics is a biometric factor that means 'something you do'. **Methods**: This review work highlights in details about the keystroke dynamics, keystroke biometrics, biometric features, keystroke biometric performance and the models related to the keystroke biometrics. In this review work, almost 25 research papers were thoroughly highlighted and reviewed. **Findings**: Based on those research papers, the authors were concluded that keystroke biometric technique is the most suitable method for password security system also some conclusion has been drawn and discussed in the end of this review paper. Additionally, the authors highlighted the research gaps based on reviewed papers in this work.

Keywords: Password Security, Keystrokes Dynamics, Keystroke Biometrics, Features, Performance and Models.

1. Introduction

Keystroke analysis firstly introduced in 1980 as a technique for finding out the individuality of series of characters that entered through conventional PC keyboard. Researchers focused at the keystroke pattern in phrases of keyboard duration and keyboard latency[1,2]. The keystroke biometric is one of the less-studied behavioral biometrics. Majority of the structures developed formerly had been experimental in nature[3]. Keystroke typing system is basically a sample popularity gadget that functions through getting typing data from a character, extracting a characteristic set from the developed records, and associating this option set in opposition to the pattern set inside the database.

Biometric widely classified in two components: enrollment section and authentication / verification phase. At some stage in the enrollment section as validated as shown in Figure 1[4], in which person's biometric statistics is received, processed and stored as reference file in a record. This could be prohibited as a manual for future use through the device in subsequent authentication operations. In the direction of the authentication/verification phase consumer biometric statistics is obtained, and processed. The authentication choice are based totally and absolutely on the results of an identical approach of the sparkling provided biometric to the pre-stored reference templates.

**Author for correspondence*

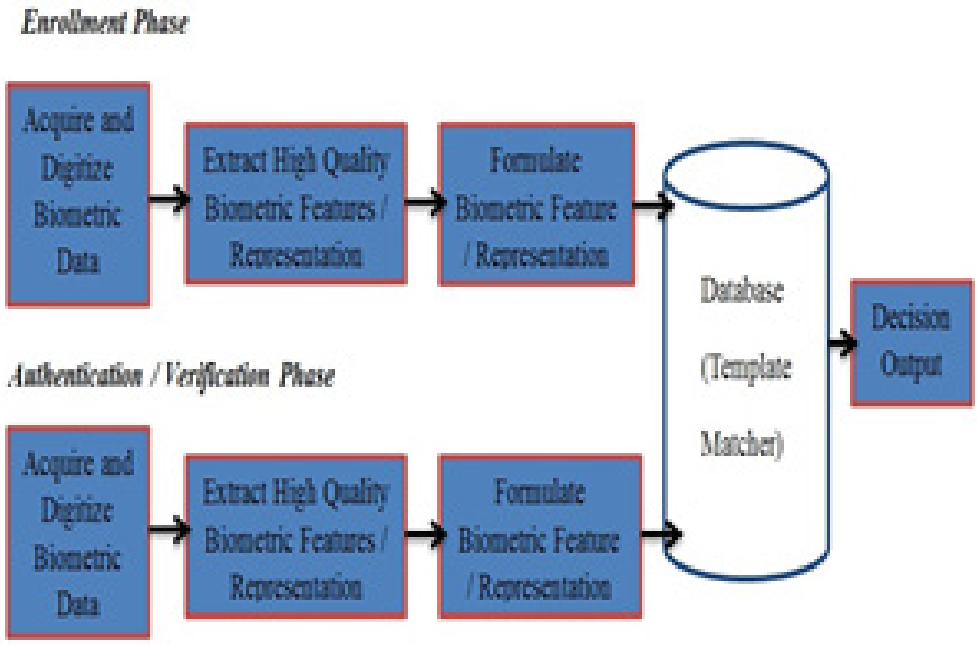

Figure 1. Biometric System[4].

Needless to mention that the importance of biometrics within the leg of information safety is large, especially in the form of authentication. Biometric authentication consists of positive levels which include records accumulating via any kind of sensors, feature extraction from the amassed information and creation of styles with the usage of positive pattern popularity algorithms. In summarization, biometric systems consist of automatic strategies to authenticate an individual based on a physiological or behavioral feature, as stated by using the Biometric Consortium[5]. However; for disadvantages, no reliability in Keystroke device like different biometrics which final pretty prolonged time body. Keystroke biometrics can lead inconsistency within the typing style due to casual typing, the usage of unattached hand for coming into the password and sticky hand after an extended conference.

With the advancing technology, the virtual world goes one step further every day in order to offer all the services that are necessary for us. Our presence in social media is also increasing in direct proportion to the services offered to us. Users can easily discuss their daily basis social or personal activities through their personal social media accounts. In the other era, with internet banking, we can perform our bank transactions without leaving our homes. We believe that we protect all these operations behind some key combinations we think are personal and private. In this regardd and with the advancement of technology day by day and such usage via different information systems (ATM, internet banking, social media accounts, e-mail addresses, etc.) are increasing in direct proportion[6].

This evaluation stresses the basics & essentials of Keystroke Dynamics and extravagant debate on the basis of reviewed literature. We reviewed in this review article: keystroke dynamics, keystroke biometrics, keystroke features and keystroke models and were discussed in details. In the last, on literature reviewed in this paper, we find few literature gaps and written in this paper.

2. Biometric Features

Biometric features are sure traits and characteristics that a man or women possesses. The time period biometric derives from the Greek words which suggest existence

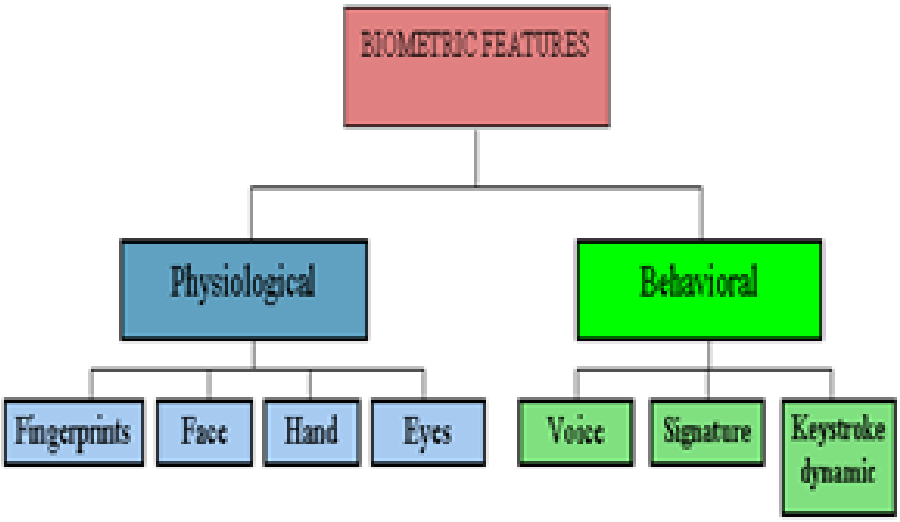

Figure 2. Biometric system features.

and measure respectively. Biometrics had been used since the early years of humanity and feature offer the ability to understand and distinguish someone through his feature capabilities. Biometric widely categorized in two elements: physiological versus behavioral features as shown in Figure 2. A physiological biometric would grow to be aware of with the useful resource of 1's voice, DNA, hand print or conduct. Behavioral biometrics is associated with the conduct of someone, such as however no longer confined to typing rhythm, gait and voice. Researchers have cited the time period behavior metrics to explain the latter elegance of biometrics. Biometric technology allow us to distinguish and discover human beings between every different & after a positive extraction and evaluation of their functions. A gadget that extracts and analyzes functions like this is known as a biometric system[4].

Keystroke analysis is the method of investigating the means of user kind on the console and establish a system in which user support its habitual typewriting rhythm. A user's typewriting pattern is also distinctive as a result of comparable neuro-physiological factors that build written signs are displayed. In simple words, Keypad dynamic is interactive biometric[7].

Natural alternative for laptop login & network security, the interactive biometric of keystroke analysis makes use of the way and pace in which a person types data on a keyboard or keypad. The keystroke pattern of a user are identify to increase a completely exceptional biometric pattern of the consumer's capturing sample for login confirmation. Vibration facts can be used to produce an outline for login use in both documentation and confirmation obligations. The obtained records required to study keystroke dynamics is acquired by using keystroke classification. Generally, all that is engaged with categorization of typing style and the sequence of typescripts corresponding to the direction in which keys had been pressed for rcording the time[8]. This can be used for finding dwell time and flight time. Figure 3 shows the analysis between dwell time and flight time. Latency time corresponds to the dwell time and is the fundamentally measures between key press and key release. While the flight time is the time period among releasing one key and pressing the following key as shown in Figure 3[9]. Highlighting some statistics about keystroke parameters used for calculating the hold time and flight time: the keystroke latency is that the combination of hold and flight time. Key Press Latency (KPL) is that the time

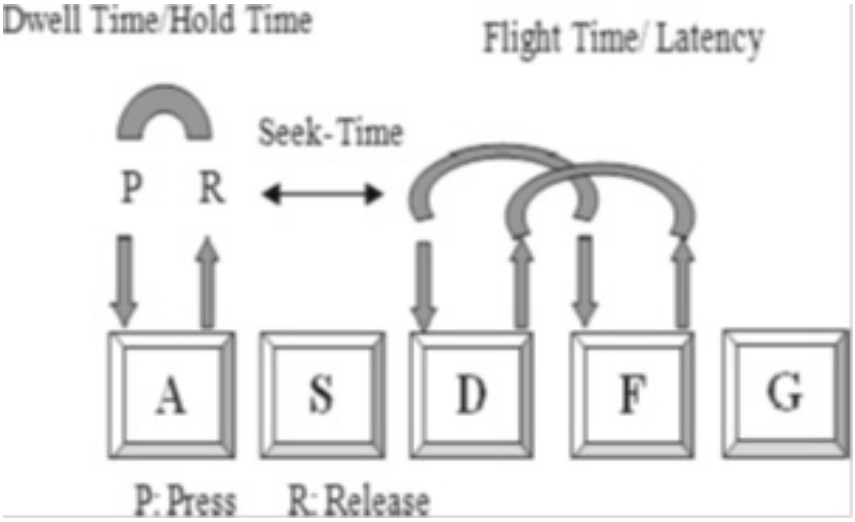

Figure 3. Dwell time and flight time (keystroke dynamics for user authentication)[9].

between 2 sequent keys press and key release Latency (KRL) is that the time among consecutive keys unleash[9].

3. Biometric System Performance

Due to exceptional enlisting on the achieving indicator, environmental modifications, deformations and noise, it's considerably out of the query that two samples of the same biometric feature, received in dissimilar phases, especially coincide; because of this the matching is accomplished via using some algorithmic rules that computes a similarity score and matches it with an reputation threshold: just in case the similarity is more than enough good, the device claims that the 2 samples coincide[10–12]. Some time the password matches incorrectly in biometric feature and the common reasons for that will be measured in terms of FRR and FAR and as shown in Figure 4 [13].

3.1 FRR (False Rejection Rate)

The rate of rejections comparative to users who should be compelled to be successfully. Once an authorized person is rejected he/she have to be compelled to signify his/her biometric system to the device. Notice that a pretend refusal does not imply basically blunder of the machine; for instance, at intervals the case of a fingerprint-primarily built device, an inappropriate placing of the finger on the detector or messiness can results incorrect rejections.

3.2 FAR (False Acceptance Rate)

The rate of false entrees attributed to impostor for claiming a fake identification. Typically, a ways that FRR rely upon the popularity threshold (t), that is accustomed set the required security degree, and are strictly associated with each utterly very different. A lot of considerably, FRR (t) could be associate degree increasing feature and FAR (t) could be a lowering characteristic, thus if the edge inserting is extended to form the access harder for impostors, some licensed people might to boot discover it more durable to advantage get right of entry to.

Different performance indexes are normally used to evaluate biometric systems:

- EER (Equal Error Rate): denotes the system error when FRR=FAR
- ZeroFAR: denotes FRR when FAR=0
- ZeroFRR: denotes FAR when FRR=0

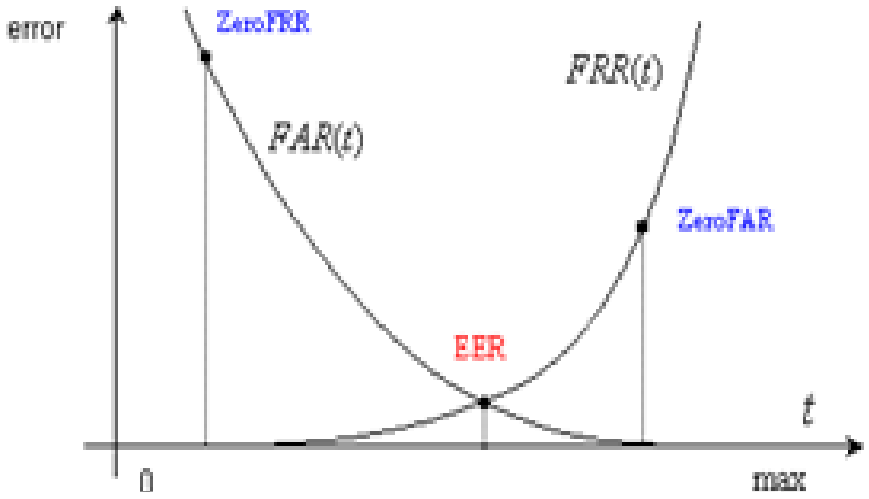

Figure 4. (FAR) and (FRR) as purposes of the threshold (t)[13].

4. Keystroke Models

For web authentication techniques, many researchers were able to locate studies that built neural networks approaches[14,15]. In the beginning many researchers were talking approximately about a technique based on a Support Vector Device (SVM). This technique exceeds all strategies inside the works up until its launched in 2011 in usage conditions, despite the fact that the computation time for enrollment stays higher. The authors in [16] discovered other usage of SVM for the application of keystroke analysis to collective structures. In spite of pretty easy strategies, the acquired consequences were nearly accurate (much less than 5% of mistakes) but it is still required to be stepped forward. However; the other model named One-class Aid Path Machines with simplest five paths in keeping with manipulators for the teaching and research seemed to provide better results. Within the tested structures of the model, best well typed passwords were taken into consideration. The problem with static password based totally authentication techniques and due to the fact that the genuine users can precise his very personal typing mistakes and being appropriately authenticated. On the other side, with the keystroke analysis implementation defined in their research, that will helps the user to type once more the PIN in a good way to have an accurate sized path. One error of this device that the key of backspace cannot be used to correct the password[17]. For keystroke analysis SVM is not the best version in it, the analysis changed into made at the performance of various strategies for keystroke analysis. However; there may be a loss of databases to check special problems and enhance systems's performances. The performance of the SVM-based system is totally depending on the technique provided in it. For this context, the technique provided in[18] research outperformed all different examined techniques. One clear decision in their work was that character thresholds improve the overall performance of system. But, it's miles expressed that the act of the approach is very passionate about our info on the spreading of the ideas and also the possitive identification itself that indicates one usage for this system. Conjointly the analysis made a sensitivity of ninety six, specificity of 93% and basic accuracy of 95%. Whereas, the outcomes of their work have a glance at imply that capturing speed and also the 1st few with the previous number of typescripts of the login ID were the foremost imortant indicators of whether login attempts became real or not.

Primary ID is important indications whether user typing attempt became correct or not.

Exciting outcomes of this paper specify that the letter of the password places are very important for deciding whether or not an individual can login. The choice of the password holder acquired the least quality of it measured in reorganizing and all the characters of their ID will compared with their hypothetical level illegal user. Similarly, for the real user of the login ID, the primary few linked in comuting and concluded digraphs had been secure to make a correct type. The uses of alternative technologies that embrace keystroke that analysis through neural network. Also are offered at the state of obtaining for examining the SVM technique. In[19], the authors targeted at the generally used MLP / BP version additionally to the multi technique victimization neural network. In their study quite 100 students and staff were invloved. They required to find and to sort the identical phrase "Thurs1day" variety of intervals they required. 10-customers were nominated to be true users and tries accumulated once bio-data initiation amounted to 5440. Could all these were actual tries at identical time as others fake make an attempt? Some troubles raised once the utilization of a neural network on this state of affairs: given the inherent characteristic of neural network associate level of it's reaching to result an output oppression this inputs and also the models analyzed it. Therefore, it will continuously in form of associate level of fake to at least one of the particular customer's conjointly a careful the constraints selection of system may be terrible vital for neural network than for alternative fashions.

Another thanks to examine statistics received from keystrokes is the combination of characteristics[20]. A keystroke analysis reputation device is furnished via the use of a mixture approach. Essentially, the normal time and the flight time were recorded because of the system calculations. The suggested and new nonconformity values had been also calculated and saved. To take a look at characteristic records can be converted into the rankings through Gaussian possibility density function. However, a new technique called course similarity measure (DSM) also can be projected to calculate the dissimilar of sign in amongst every fixed character throughout an expression.

Finally, a weighted sum total rule is imposed through fusing the Gaussian ranking and the DSM to enhance the final word event. Values that show a mix of reside time and flight time yields higher results than the usage of them and altogether completely different measures in their[21] work. Moreover; by way of combining them with the DSM method, the peak result's progressed. The authors of [21], in locality of fusing characteristics, attempted to deliver greater worth to sort of them, deeming them bigger critical for keystroke dynamics. The resulted values displayed that keystroke dynamics is also a reliable security device for authentication, if used beside specific gadgets. It appears larger acceptable for authentication (verification) than for identity. Reside attempts how extended a key's managing pressed provides extra discriminatory and consequently extra influential than flight times (time amongst consecutive press times)[22].

Keystroke data with and without touch screen functions, consisting of pressure and finger vicinity. Facts become gathered from both gadgets time and touchscreen primarily and Android mobile based capabilities were fetched. In them, the classification accuracies were acquired by means of numerous device mastering type algorithms like area mathematician, C4.5 (J48), k-NN (IBk), SVM, random tree-plant, and MLP. The best performances are advantaged by exploitation of arbitrary forest, theorem nets, SVM and many more. Verification effects had been reaping the usage of geometer, large apple and mahalanobis distance metrics. As per[11], the observation confirmed that all-time low error (12.9%) obtained through the key distance with the employment of each order and touch screen based options. Their analysis over that touchscreen based completely utilities intensification kind and verification accuracy. Also[13] applied an analogous experiment with 152 members and a 17-digit identifiction. In passing single consultation, each participant typed the positive identification ten times at intervals the obscenity of associate degree. They determined that the strain and length of the finger will furthering to temporal order choices and will cut back the error cost of a

cellular KB device. They have a glance at set 4.19 they're much and 4.59 nothing FRR through the usage of hold time combined with di-graph, and tri-graph functions.

5. Future Recommendations

Keystrokes dynamics has an advantages file of the typing verification techniques due to the fact that users are even currently acquainted with authenticating themselves through usernames and PIN's. Most proposed keystroke evaluation approaches are completely transparent. There are various programs that may assist from its success and distinct studies will in addition validate its exercising as an identification verifier. That is specifically applicable to the approval of keyboards as a key enter device in facts processing structures. The idea of keystroke dynamics isn't continually restricted to the traditional keyboard methods, however; any interface during which keys must to be pressed will advantage from comparable structures. Keystroke biometrics shown prime importance and most likely as the functions could also be composed without the wish for special hardware.

Through the literature surveyed in this work, the authors can concluded some research gaps: Additional scenarios which require adaptive classification algorithms in biometrics can also be evaluated. Likewise other methods to improve the performance of statistical based algorithms over time may also be investigated. Correspondingly involving experiments using the system in an actual internet security situation, like verifying the identity of online test takers. Additionally more sophisticated classification techniques might be explored, such as Support Vector Machines (SVM). Finally, although it is likely difficult to mimic another person's keystroke pattern, imposter performance can also be investigated. The literature reviewed in this work clearly highlighting for future work to explore the effects of ID/password length and typing speed as additional methods to increase the security level of this system. Also through literature, the different methods used and authenticated by the user were discussed. Amongst them Statistical and Neural network have been widely used methods. To dig-out more works include: Mobile, PDA and ATM machines.

6. Conclusion

Keystroke dynamics is a behavioral measurement and it goals to select out users primarily based completely at the typing of the people or attributes together with duration of a keystroke or key preserve time, latency of keystrokes (inter-keystroke times), typing error, pressure of keystrokes and lots of others. The analogy is made to the times of telegraphy whilst operators perceive every special via spotting "the first of the sender"[23,24].

This research highlighted the reviewed work for a remarkable verification method to computer net applications principally based on behavioral biometrics like keystroke dynamics. The keystroke dynamics method derives the possibility of appearing complicated biometrics without more system, however; greatest a keyboard tool that takes place to be part of every PC device. Inside the assessment work, keystroke dynamics tested that it could be applied to handle the overall customer verification situation and supply a moderately comfy surroundings to be greater secured in opposition to computer threats and attacks. The impact of the various biometric parts and example profiles of participants are often tested through victimization keystroke dynamics constant with the experimental consequences cited in this assessment artwork. All version algorithms acquired higher predictive average overall performance than their static (with out model) in opposite numbers. Specifically, the results in[2] showed superior predictive overall performance. Also the effects for[1] showed superior predictive overall performance and better presentation within the difference findings of the researched version, linked to former paintings using the identical CMU dataset. The Error Fee (EER) became 0.03, a reduction of 35% as compared to the highest acting version within the CMU study and a deduction of 9/11 as compared to the med-std model. At the error rate of zero.03 (3%), the Hit Rate was 93%, that shows that despite the very truth that the model contains

a better anomaly detection overall performance, it doesn't supply the desired detection strength expected in access management standards (CENELEC. European widespread: 2002). However; the keystroke biometric model will perform a secondary authentication issue throughout a multi-issue authentication tool. Keystroke biometric systems measures clearly unknown as compared to different discipline and a competely restricted wideselection of analysis were conducted as compared to completely different biometric systems. In spite of unremarkably decrease accuracies than completely different biometric modalities, keystroke biometric has number of blessings consisting of being low value, oblivious, noninvasive to the buyer and offers ability to perpetually show a system. The brand new approach based totally on consumer conduct dynamic keystroke biometric is easy in designing which affords excessive level of safety and it does not need any more hardware. The version has excellent scope and it is straightforward to place operative on the word based mostly entirely system or structures. This machine in addition is criminating the consumers on the concept of their writing behavior as an actual user and non-genuine person. This methodology have the range of software system package sever a despite their nature. With this system 2 ways in which in security is used which affords further security to word mostly based totally systems & amp: offers new direction of development to word based protection system.

7. References

1. Magalhães ST, Santos HD. An improved statistical keystroke dynamics algorithm. Proceedings of the IADIS MCCSIS; 2005.
2. Peacock A, Ke X, Wilkerson M. Typing patterns: A key to user identification. IEEE Security and Privacy. 2004 Sep–Oct; 02(5):40–7. https://doi.org/10.1109/MSP.2004.89.
3. Michael OB, MarfoMissah Y. Utilizing keystroke dynamics as an additional security measure to password security in computer web-based applications - A case study of UEW. International Journal of Computer Applications. 2016 Sep; 149(5):0975–87.
4. Pisani, Henrique P, Lorena AC, CPLF de Carvalho A. Adaptive approaches for keystroke dynamics. 2015 International Joint Conference on Neural Networks; 2015.
5. Senathipathi K, Batri K. An analysis of particle swarm optimization and genetic algorithm with respect to keystroke dynamics. 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE); 2014.
6. Emarketer. Internet hit 3-billion users [Internet]. 2014. [cited 2018 Nov 18]. Available from: 2014. https://www.emarketer.com/Article/Internet-Hit-3-Billion-Users-2015/1011602.
7. Tappert CC, Cha S-H, Villani M, Zack RS. A keystroke biometric system for long-text input. Optimizing Information Security and Advancing Privacy Assurance: New Technologies. IGI Global; 2012. p. 32–57.
8. Ali ML, Charles JVM, Tappert C, Meikang Qiu. Keystroke biometric systems for user authentication. Journal of Signal Processing Systems. 2017 Mar; 86(2–3):175–90. https://doi.org/10.1007/s11265-016-1114-9.
9. Karnan M, Akila M, Krishnaraj N. Biometric personal authentication using keystroke dynamics: A review. Applied Soft Computing. 2011; 1(1):1565–73. https://doi.org/10.1016/j.asoc.2010.08.003.
10. Calot E, Rodríguez JM. Improving versatility in keystroke dynamic systems. XVIII Congreso Argentino de Ciencias de la Computación. 2013; 1(5).
11. Abualgasim SD, Osman I. An application of the keystroke dynamics biometric for securing PINs and passwords. World of Computer Science and Information Technology Journal (WCSIT). 2011; 1(9):398–404.
12. Ponkshe RV, Chole V. Keystroke and mouse dynamics: A review on behavioral biometrics. International Journal of Computer Science and Mobile Computing. 2015 Feb; 4(2):341–5.
13. AL-Rahmani AO. An enhanced classifier for authentication in keystroke dynamics using experimental data. Master Degree Thesis. Middle East University. 2014 Jun.
14. Sawant MM, Nagargoje Y, Bora D, Shelke S, Borate V. Keystroke dynamics: Review paper. International Journal of Advanced Research in Computer and Communication Engineering. 2013; 2(10).
15. Voth D. Face recognition technology. IEEE Intelligent Systems. 2003; 18(3):4–7. https://doi.org/10.1109/MIS.2003.1200719.
16. Giot R, El-Abed M, Hemery B, Rosenberger. Unconstrained keystroke dynamics authentication with shared secret. Computers and Security. 2011; 30:427–45. https://doi.org/10.1016/j.cose.2011.03.004.
17. Giot R, El-Abed M, Rosenberger C. Keystroke dynamics authentication for collaborative systems; 2009.
18. Revett K, de Magalh˜aes ST, Santos H. Data mining a keystroke dynamics based biometrics database using rough sets; 2005. PMid:16150821

19. Pavaday N, Soyjaudah KMS. Investigating performance of neural networks in authentication using keystroke dynamics; 2007.
20. The PS, Teoh ABJ, Ong TS, Neo HF. Statistical fusion approach on keystroke dynamics; 2008.
21. Killourhy K, Maxion R. Why did my detector do that?! predicting keystroke-dynamics error rates. RAID. LNCS 6307; 2010. p. 256–76.
22. Douhou S, Magnus JR. The reliability of user authentication through keystroke dynamics. Statistica Neerlandica. 2009; 63(4):432–49. https://doi.org/10.1111/j.1467-9574.2009.00434.x.
23. Attila M, Zoltán B, László C. Strengthening passwords by keystroke dynamics. IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. Dortmund, Germany; 2007.
24. Gunetti D, Picardi, C. Keystroke analysis as a tool for intrusion detection. Continuous authentication using biometrics: Data, model, and metrics. Issa Traore: IGI Global; 2012.