Decision Making Process in Keystroke Dynamics

Mohd Noorulfakhri Yaacob¹, Syed Zulkarnain Syed Idrus¹,², Wan Nor Ashiqin Wan Ali¹,², Wan Azani Mustafa³, Mohd Aminudin Jamlos³ and Mohd Helmy Abd Wahab⁴

¹School of Human Development and Technocommunication, Universiti Malaysia Perlis, Perlis, 01000 Perlis, Malaysia.
²Center of Excellence Geopolymer and Green Technology, Universiti Malaysia Perlis, 01000 Perlis, Malaysia.
³Faculty of Engineering Technology, Universiti Malaysia Perlis, 01000 Perlis, Malaysia.
⁴Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia, Malaysia.

Abstract. Computer system intrusion often happens nowadays. Various methods have been introduced to reduce and prevent these intrusions, however no method was 100% proven to be effective. Therefore, to improve the computer’s security, this writing will explain the application of KD in the application system. The effectiveness of KD could not guarantee one hundred percent to prevent the computer intrusion, but it can be used as a second level of security after the login page in the application system. The pattern and time taken while typing by an individual is the core for the second level of security check after the login page. This writing will elaborate and conclude past studies related to KD on the aspects of decision-making process. Various methods of processing KD data that have been used are listed and the results of the study are compared. The results of this writing are expected to help new researchers in the process of evaluating KD data.

1. Introduction

Most of the computer systems used a login page that contain username and password which must be completed by respective user as the procedure for using the system. However, if the username and password is available to another user, that person could access the system using this data. He/she will have the access to the system which is not supposed to be available for them. This will initiate computer’s security breach. Security breach is extremely dangerous as confidential information that related to medical, safety, security and financial will be exposed to irresponsible parties.

Additional security features have been introduced to tighten control over systems that use these usernames and passwords such as limiting the Internal Access to some IP Addresses, Mac Addresses, Smart Card Access and additional device for security enhancements. However, the intrusion is still occurred because it is likely to arise from the internal intrusion of the organization itself. Therefore, to minimise this intrusion, the application of Keystroke Dynamic (KD) in a system can be used.

KD is a process for identifying how an individual use the keyboard for typing. This KD dynamic is categorized as behavioral biometric. The system that uses this KD method as a process of identifying users should record the way the respective user typing the username and password in the
enrolment process. The typing time difference between the letters are recorded for comparison against the time recorded during the enrolment process with the current typing time by the respective user. Various methods and approaches have been introduced to help the system analyse using KD.

This writing presents and summarizes the results of past studies related to decision making process in Keystroke Dynamics. The result of this writing can provide a comprehensive overview of KD in terms of data extraction methods, methods of keystroke data analysis and the performance of past studies using specific methods. This will further help researchers continue their studies on KD in the future.

This writing is related to the methodologies used by previous studies to analyse keystroke data (Decision making process).

2. Decision Making Process

Decision making process is a crucial process in identification against a group of records or massive information [2]. In KD, multiple technique can be deployed to identify the process of decision making. Decision is made by comparing similarities or near similarities of an object against a group of objects based on predetermined score [3]. Measurement criteria normally used in KD to measure performance is False Acceptance Rate (FAR) and False Rejection Rate (FRR).

i. FAR - FAR refers to the percentage ratio between accepted system intruder as valid user and the actual amount of real intruder using a system [4]. FAR is also known as False Match Rate (FMR) [5].

ii. FRR - FRR refers to the percentage ratio between the actual user system or a legitimate user is denied or restricted for use and the number of actual users of the system [6]. FRR is also known as the False Non-Match Rate (FNMR) [5].

Based on both metrics above, FAR and FRR can be interconnected by mutually exclusive because it is impossible for FAR and FRR to happen simultaneously. Figure 1 shown relationship between FAR, FRR and Equal Error Rate (EER).

![Figure 1: Relationship between FAR, FRR and Equal Error Rate (EER) [1].](image)

EER is a performance measurement normally used to make a comparison. Referring to figure 2.2, EER is the point of overlap between FAR and FRR. The lower the value of EER means a better system [7]. It is however impossible to reach 0% EER in biometrics method [8]. Highest EER ever reached in recognition using biometrics is via physical recognition that is as high as 0.1% (Jain, Ross et al. 2004).
User typing styles stored in a system must be comprised of multiple extra features that can be analyzed by researchers. Raw data being stored should include, time distance between two keys being pressed or released [9], pressure [10], finger size for some devices [11, 12], keyboard type [7] and finger movement pattern if recorded from mobile devices [13]. Following listed a few techniques normally used in research by researchers to measure KD recognition performance.

(i) Neural Network
(ii) Statistical Method
(iii) Fuzzy Logic
(iv) Support Vector Machine

2.1. Neural network
Technique employed by Neural Network is similar to the biological structure found in human nerve [14]. It is also known as artificial neural network [15]. Neural Network is inspired by the basic structure of biological neurons in the human brain. Interconnected neurons forms a network, allowing an interpretation be made easily and learned [16]. It is capable of learning all types of pattern and function. It is also easy to use for solving complicated problems including its usage in computer field especially KD.

Some example of neural network technique being used in researches are:

i. Multi-Layer Perceptron (MLP)
ii. Radial Basis Function (RBF)
iii. Learning vector quantisation
iv. Self – Organizing Map

These neural network techniques normally produce high precision in identifying or learning something, however it involves high computing cost [17] and take a long time to attain answers or result [18]. Systems using neural network techniques can only operate in smart phones with a minimum of 512 MB RAM [19].

Keystroke dynamics study using neural network method has begun to be implemented as early as 1993 [20]. The study was conducted using 24 volunteers and acquired an 8% FAR and 9% FRR. Neural network technique used in their study was Perceptron.

Later in 1999, this neural network method was used by Capuano, Marsella [21]. He used the technique of Radial Basic Function Network- Or known as RBFN on 10 volunteers. The accuracy obtained is between 78% up to 100% for 10 volunteers.

In 2007, this neural network method was also used in the KD study using a mobile phone [22]. The study focused on entry of pin number on mobile phone. A total of 18 volunteers are required to type a 4-digit characters and another 14 volunteers required to type a 11-digit pin number. The results obtained an average EER of 12.8%.

Also in 2007, another study was conducted by Loy, Lai [23] using neural network technique called ARTMAP-FD. The study was carried out against 100 users and obtained an EER of 16.5% for the pressure, EER of 14.94% for latency and EER of 11.78% for both.

KD study using neural network continued in 2009. The study was conducted on the pressure on the touch-screen smartphone by using the Probabilistic Neural Network (PNN) [10]. EER obtained from these studies is 1%. Studies similar to Saevanee and Bhattarakosol [10] has also been made by other researchers in the same year. Ali and Salami [24] also studied aspects of pressure on the touch screen, but they use different neural network technique called Multilayer Feedforward Network (MFN) and acquired FRR and FAR of 0% for both. There were only 7 people involved in this research.

In 2010, Nguyen, Le [25] conducted a research on KD by adding to the features of measurement with regard to typing sound signal besides lag and stress. The method used for analyzing was Fast Artificial Neural Network Library (FANN) which gained 4.2% FAR and FRR of 5.55%.
Additionally, in 2010 KD research using Soft Computing techniques have been implemented by Karnan and Akila [26]. They used the technique called Back Propagation Neural Network (BPNN) to analyze the data obtained. A total of 25 volunteers participated in this study and the results obtained have achieved an accuracy of 92.8%.

Subsequently in 2013, Draffin, Zhu [27] has conducted a study on the use of KD on smartphones. They have examined the characteristics of micro-behavior (finger drift, specific location on each key touch, force of touch) recorded during the use of the smart phone. The study was conducted on 13 volunteers. Analysis of the data obtained using Artificial Neural Network (ANN) technique is between 14% and 2.2% for the FAR and FRR.

The use of neural network method was continued by Ahmed and Traore [28] by studying KD based on free words. A total of 17 people involved in this study. The results obtained EER of 2.13% by using Deep Neural Networks (DNN).

In 2015 Deng and Zhong [29] has conducted a study using the KD on user authentication against mobile devices such as smartphones. Data analysis technique used was Deep Neural Network and he has obtained an EER of 2.8% and up to 5.5% for the 55 volunteers.

The study of KD on mobile devices has also attracted the interest of Corpus, Gonzales [30] to include several additional criteria for user authentication. Additional criteria are detecting how the user holds their personal phone. This criterion is measured by an accelerometer sensor on the smartphone. The study was conducted on 30 volunteers. The results obtained show that there is increasing recognition performance from 49.44% to 61.11% when additional criteria are used with the KD. FAR obtained was 7.0%.

Latest in 2017, Mondal and Bours [31] have been introducing and using User Pairwise Coupling techniques to analyze data for his research in the field of KD. A total of 500 keystroke obtained from a total of 64 students. The results obtained an increase in confirmation accuracy by 7% compared to the usual methods.

Latest in the year 2018, Kim, Kim [32] introduced and utilized the Recurrent Neural Network (RNN) method to analyze the data for their research in KD field. They have research this RNN method against long sentences and free sentences. Based on the study results made on 120 participants using this method, user authentication accuracy recorded 5%-6% compared to other methods.

Following are summaries of previous researches utilizing neural network technique in their research regarding KD (Table 1).

| Researcher                | Year | Participants | Neural Method  | Result           |
|---------------------------|------|--------------|----------------|------------------|
| Bleha and Obaidat [20]    | 1993 | 24           | Perceptron     | FAR: 8%; FRR: 9% |
| Capuano, Marsella [21]    | 1999 | 10           | RBFN           | Accuracy: 97%    |
| Clarke and Furnell [22]   | 2007 | 32           | Feed forward multi-layered perceptrons | EER: 12.8% |
| Loy, Lai [23]             | 2007 | 100          | ARTMAP-FD      | EER(Pressure): 16.5 |
| Saevanee and Bhattarakosol [33] | 2009 | 10           | PNN            | EER 1%           |
| Ali and Salami [24]       | 2009 | 7            | MFN            | FAR: 0% FRR 0%   |
| Sulong and Siddiqi [34]   | 2009 | 30           | RBFN           | FAR: <2%         |
| Nguyen, Le [25]           | 2010 | 20           | FANN           | FAR: 4.12%; FRR: 5.55% |
| Karnan and Akila [26]     | 2010 | 25           | BPNN           | Accuracy: 92.8%  |
| Draffin, Zhu [27]         | 2013 | 13           | ANN            | FAR: 14% | FRR: 2.2% |
| Ahmed and Traore [28]     | 2014 | 17           | Neural Network | FAR = 0% | FRR = |
5.01% | EER = 2.13%

Deng and Zhong [29] 2015 55 DNN EER: 2.8% - 5 %

Corpus, Gonzales [30] 2016 30 Neural Networks Performance improve 49.44% to 61.11% FAR: 7 %

Mondal and Bours [31] 2017 64 ANN Accuracy: 90%

Kim, Kim [32] 2018 120 RNN Accuracy: 5-6%

2.2. Statistical Methods

Statistical method approach is a method frequently used by researchers until nowadays. Since 1980, Gaines (1980) has researched KD of 7 volunteers using Statistical-test as a method of analyzing the data. The results obtained reached up to 95% accuracy.

In 1997, the statistical method touted as Probabilistic and Euclidean Distance was used by Monrose and Rubin [35] in a study on the KD. Data obtained from 31 volunteers is collected in the duration of 7 weeks. The accuracy of the results obtained from those studies was 90%.

Monrose and Rubin [35] next performed a follow-up studies on other methods to analyze the data for user authentication using KD [36]. In the year of 2000, they have used the k-Nearest Neighbor (k-NN) techniques to analyze data on 63 volunteers. The results of this follow up study obtained the accuracy between 83.22% and 92.14%.

The use of k-Nearest Neighbor method has attracted Mantyjarvi, Koivumaki [37] to use it in the study of user authentication using KD. Their study focused on the virtual keyboard. The results obtained had the accuracy of between 78% and 99%.

In 2005, the statistical method called the Standard Deviation (SD) was used in the study by de Magalhães, Revett [38]. They review the effectiveness of the use of KD in websites using passwords. The result’s obtained EER is under 5%.

Next, this standard deviation method has also been used by Modi and Elliott [39] to study the strength of user passwords typing style spontaneously (Spontaneously Generated Password). The study was conducted on 42 volunteers and resulted with 0.33% FAR and 94.87% FRR.

In 2007, Kang, Hwang [40] conducted a study related to KD based on fixed window, moving window and growing windows using Euclidian Distance method. EER obtained on 51 volunteers in their study was 3.8%.

The use of k-Nearest neighbor does not cease in 2002 since it was reused by Hu, Gingrich [8] in a study of user authentication using KD. The study was conducted on 19 users and achieved a 66.7% increase in speed of recognition.

Subsequently in 2013, the study of the use of KD on the touch screen has been done by Trojahn and Ortmeier [12]. A total of 152 peoples were involved in their study, the FAR obtained is 4.19% and FRR obtained is 4.59% using the statistical approach in analyzing the data.

Research on the use of KD in identifying individual students during the Online Course Assessment has been carried out by Monaco, Stewart [41] using k-Nearest Neighbor method and Euclidian Distance. The accuracy obtained in identifying students were between 88.2% and 91.5% against 40 students. Also in the year of 2013, a research on the use of user recognition using fixed-length text of various characters have been executed Rybnik, Tabedzki [42]. Data was collected online through web-based interface and via computer installed with special software. Only 7 volunteers engaged in their studies. EER obtained is 6.1%.

Corpus, Gonzales [30] conducted KD research against its use in mobile phones by introducing some additional criteria for user authentication. These additional criteria are detecting how the user holds their personal phone. This criterion is measured by an accelerometer sensor on the smartphone using the Standard Deviation of the analyzed data. FAR obtained is 7.0%, while the FRR was 40%.

Research on the use of KD in the smart phone with additional features such as the use of gyroscope sensor, the size, coordinate and acceleration sensors are also implemented. Studies using
these extra features was conducted by Roh, Lee [43] using Standard Deviation methods to analyze data. The results obtained were between 7.70% and 11.24% for the EER. Also In 2016, the study of the effectiveness of the use of sensors to help improve identification of individuals using mobile phones using KD was conducted [44]. A total of 20 volunteers participated in the study by them. Effectiveness was measured and evaluated using statistical approaches of k-Nearest Neighbor and yielded an EER of less than 0.14%.

Latest in the year 2018, the statistics method is used by Kim, Kim [32] to strengthen user recognition and authentication using KD methods. Based on research results from 150 respondents, they acquired more than 13000 keystrokes from each respondent. Average EER obtained is 0.44%. Also in the year 2018 , a study related to KD to identify Internet users under the age of 18 was conducted by Roy, Roy [45]. Method used for data analysis was FRNN-VQRS. This study was conducted against 4 datasets and resulted in achieving user authentication accuracy between 82% and 91%.

This shows that this method is still being used until now. This method is so popular because it is easy to execute and acquire low overhead. Table 2 below lists researches in KD in which researchers has used statistical approach to analyze attained data.

**Table 2 Previous researches utilizing Statistics**

| Researcher         | Year | Participants | Statistic Methods          | Result                  |
|--------------------|------|--------------|----------------------------|-------------------------|
| Gaines, Lisowski   | 1980 | 7            | Statistical -test          | Accuracy: 95%           |
| Monrose and Rubin  | 1997 | 31           | Probabilistic and Euclidean Distance | Accuracy: 90%           |
| Monrose and Rubin  | 2000 | 63           | k-NN                       | Accuracy 83.22% - 92.14% |
| Mantyjarvi, Koivumaki | 2002 | -            | k-NN                       | Accuracy 78- 99%        |
| de Magalhães, Revett | 2005 | -            | SD                         | FAR: 0.33% | FRR:94.87% |
| Modi and Elliott   | 2006 | 42           | SD                         |                         |
| Kang, Hwang        | 2007 | 51           | Euclidian Distance        | EER: 3.8%               |
| Hu, Gingrich       | 2008 | 19           | k-NN                       | Speed Auth: 66.7%       |
| Trojahn, Arndt     | 2013 | 152          | Mean and STD               | FAR: 4.19% | FRR :4.59 % |
| Monaco, Stewart    | 2013 | 40           | k-NN / Euclidian Distance | Accuracy: 88.2 – 91.5   |
| Rybnik, Tabedzki   | 2013 | 9            | k-NN                       | EER 6.1 %               |
| Corpus, Gonzales   | 2016 | 30           | SD                         | FRR: 40% | FAR: 7.0%   |
| Roh, Lee           | 2016 | 15           | SD                         | EER :7.70% - 11.24%     |
| Stanciu, Spolaor   | 2016 | -            | K-means clustering (KMC)   | ERR: 0.14%              |
| Kim, Kim           | 2018 | 150          | K-means clustering (KMC)   | EER: 0.44%              |
| Roy, Roy           | 2018 | -            | FRNN-VQRS                  | Acc: 82% - 91%.         |

2.3. Fuzzy logic
Fuzzy logic is a method used to analyze data by evaluating form containing multiple 1 and 0 logic [48]. In other words, Fuzzy logic is “a way to reach a goal by going through different paths” [49]. Various fuzzy logic algorithms were introduced to identify user through fuzzy logic method. In 1989, Hussien, McLaren [50] used fuzzy clustering algorithms in their research and produced EER between 5% to 10%. This method was also used by De Ru and Eloff [51] to improve user authentication process. Later in 2015, Sridhar, Vaidya [49] employed fuzzy logic technique to detect intrusion using KD. Table 3 below lists researches in KD in which researchers had used fuzzy logic approach to analyze attained data. 

Table 3: Previous researches utilizing fuzzy logic

| Researcher               | Year | Participants | Fuzzy Method    | Result         |
|--------------------------|------|--------------|-----------------|----------------|
| Hussien, McLaren [50]    | 1989 | 20           | Fuzzy K-means   | EER : 5-10%    |
| De Ru and Eloff [51]     | 1997 | 29           | Fuzzy Logic     | FAR: 0-15%     |
| Sridhar, Vaidya [49]     | 2015 | 200          | Fuzzy Logic     | FAR 0-1%       |

2.4. Support vector machine

Support Vector Machines (SVM) is a computer algorithm capable of learning or identifying an object based on a sample and later classify those objects [52]. Concept being used in SVM is known as supervised learning method where each object gets to be analyzed to allow classification process being done. Generally, classification technique utilizing SVM can be grouped into two category which is male or female. Classification distribution technique using SVM is also being used in KD researches.

In 2004, Yu and Cho (2004) used SVM technique to analyze data obtained for user identification using SVM. They produced SVM novelty detector with Gaussian kernel to analyze data and yielded EER at 0.81%. SVM was also used by Hocquet, Ramel [53] in their research related to KD. Research on 38 users produced EER around 5%.

Next, SVM technique use in data analytic was also implemented in 2009 by Giot, El-Abed [54] to identify users. This research garnered 99% EER. Gender recognition research using KD method was executed by Giot and Rosenberger [55] in the year of 2012. Data classification using SVM was used in this research and succeed to increase recognition rate by reducing EER as much as 20%.

Subsequently, SVM technique was utilized in user recognition research based on typing style in the year of 2013 and 2014 [56, 57]. Classification categories used in this research are based on gender, age, usage of one handedness or both hand while typing, and hardness. This technique was also deployed by [58, 59] in 2014 to analyze data for Keystroke Dynamics.

SVM usage also caught the interest of Çeker and Upadhyaya [60] to study SVM usage for user recognition in KD. They have introduced three SVM methods dubbed Adaptive SVM, Deformable Adaptive SVM and Projective Model Transfer SVM. Using these methods allowed them to gain 13% increase in accuracy and recognition.

Following are summary on researches done utilizing SVM technique for KD (Table 4):

Table 4: Previous researches utilizing SVM

| Researcher       | Year | Participants | Method | Result      |
|------------------|------|--------------|--------|-------------|
| Yu and Cho [61]  | 2004 | 15           | SVM    | EER: 0.81%  |
| Hocquet, Ramel [53] | 2007 | 38           | SVM    | EER: 5 %    |
3. Conclusion
Most of the past studies related to KD from the aspects of decision making process have been summarized in this writing. There is a pattern discovered from the past study that can be summarized, the bigger the participants or lots of Keystroke data make it increasingly difficult to identify. This summary is based on the number of participants involved in previous KD dynamic studies by evaluating EER, FAR and Accuracy obtained. Therefore, based on the previous study, a conclusion can be made, that studies in the field of KD could be continue by looking at the possibility of new algorithms or other aspects that enable enhanced recognition of using KD. In addition, this writing is also expected to assist researchers in the same field to look for improvement ideas on KD for the future study. For example, the number of participants involved in the survey need to be high and the new features of recognition need to be incorporated into the next research element. This writing is expected to provide significant impact on the novice researchers who are interested in keystroke dynamics.

4. References

1. Clarke, N.L., S.M. Furnell, and P.L. Reynolds. Biometric authentication for mobile devices. in Proceeding of the 3rd Australian information warfare and security conference. 2002.
2. Nutt, P.C. and D.C. Wilson, Handbook of Decision Making. 2010: Wiley.
3. Shi, Y., et al., Advances in Multiple Criteria Decision Making and Human Systems Management: Knowledge and Wisdom : in Honor of Professor Milan Zeleny. 2007: IOS Press.
4. Karnan, M., M. Akila, and N. Krishnaraj, Biometric personal authentication using keystroke dynamics: A review. Applied Soft Computing, 2011. 11(2): p. 1565-1573.
5. Bours, P., Continuous keystroke dynamics: A different perspective towards biometric evaluation. Information Security Technical Report, 2012. 17(1): p. 36-43.
6. Araújo, L.C., et al., User authentication through typing biometrics features. IEEE transactions on signal processing, 2005. 53(2): p. 851-855.
7. Shanmugapriya, D. and G. Padmavathi, A survey of biometric keystroke dynamics: Approaches, security and challenges. arXiv preprint arXiv:0910.0817, 2009.
8. Hu, J., D. Gingrich, and A. Sentosa. *A k-nearest neighbor approach for user authentication through biometric keystroke dynamics*. in Communications, 2008. ICC’08. IEEE International Conference on. 2008. IEEE.

9. Killourhy, K.S. and R.A. Maxion. *Comparing anomaly-detection algorithms for keystroke dynamics*. in Dependable Systems & Networks, 2009. DSN’09. IEEE/IFIP International Conference on. 2009. IEEE.

10. Saevanee, H. and P. Bhattarakosol. *Authenticating user using keystroke dynamics and finger pressure*. in Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE. 2009. IEEE.

11. Chen, J., et al., *Personalized keystroke dynamics for self-powered human-machine interfacing*. ACS nano, 2015. 9(1): p. 105-116.

12. Trojahn, M. and F. Ortmeier. *Toward mobile authentication with keystroke dynamics on mobile phones and tablets*. in Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on. 2013. IEEE.

13. Banerjee, S.P. and D.L. Woodard, *Biometric authentication and identification using keystroke dynamics: A survey*. Journal of Pattern Recognition Research, 2012. 7(1): p. 116-139.

14. Graupe, D., *Principles of Artificial Neural Networks*. 2007: World Scientific.

15. Enquist, M. and S. Ghirlanda, *Neural Networks and Animal Behavior*. 2005: Princeton University Press.

16. Wlaminowski, B.M., *Neural network architectures and learning algorithms*. IEEE Industrial Electronics Magazine, 2009. 3(4).

17. Srinivasan, K. and D. Fisher, *Machine learning approaches to estimating software development effort*. IEEE Transactions on Software Engineering, 1995. 21(2): p. 126-137.

18. Mendizabal-Vázquez, I.d., et al. *Supervised classification methods applied to keystroke dynamics through mobile devices*. in 2014 International Carnahan Conference on Security Technology (IC CST). 2014.

19. Kambourakis, G., et al., *Introducing touchstroke: keystroke-based authentication system for smartphones*. Security and Communication Networks, 2016. 9(6): p. 542-554.

20. Bleha, S.A. and M.S. Obaidat, *Computer users verification using the perceptron algorithm*. IEEE Transactions on Systems, Man, and Cybernetics, 1993. 23(3): p. 900-902.

21. Capuano, N., et al., *User authentication with neural networks*. University of Salerno Italy. http://www.capuano.biz/Papers/EANN_99.pdf, 1999.

22. Clarke, N.L. and S.M. Furnell, *Authenticating mobile phone users using keystroke analysis*. International Journal of Information Security, 2007. 6(1): p. 1-14.

23. Loy, C.C., W.K. Lai, and C.P. Lim. *Keystroke patterns classification using the ARTMAP-FD neural network*. in Intelligent Information Hiding and Multimedia Signal Processing, 2007. IIHMP 2007. Third International Conference on. 2007. IEEE.

24. Ali, H. and M.J. Salami. *Keystroke pressure based typing biometrics authentication system by combining ANN and ANFIS-based classifiers*. in Signal Processing & Its Applications, 2009. CSPA 2009. 5th International Colloquium on. 2009. IEEE.

25. Nguyen, T.T., T.H. Le, and B.H. Le. *Keystroke dynamics extraction by independent component analysis and bio-matrix for user authentication*. in Pacific Rim International Conference on Artificial Intelligence. 2010. Springer.

26. Karnan, M. and M. Akila. *Personal authentication based on keystroke dynamics using soft computing techniques*. in Communication Software and Networks, 2010. ICCSN’10. Second International Conference on. 2010. IEEE.

27. Draffin, B., J. Zhu, and J. Zhang. *Keysens: Passive user authentication through micro-behavior modeling of soft keyboard interaction*. in International Conference on Mobile Computing, Applications, and Services. 2013. Springer.

28. Ahmed, A.A. and I. Traore, *Biometric Recognition Based on Free-Text Keystroke Dynamics*. IEEE Transactions on Cybernetics, 2014. 44(4): p. 458-472.
29. Deng, Y. and Y. Zhong, *Keystroke dynamics advances for mobile devices using deep neural network*. 2015, Science Gate Publishing, p. 59-70.

30. Corpus, K.R., et al. *Mobile user identification through authentication using keystroke dynamics and accelerometer biometrics*. in *Proceedings of the International Workshop on Mobile Software Engineering and Systems*. 2016. ACM.

31. Mondal, S. and P. Bours, *Person identification by keystroke dynamics using pairwise user coupling*. IEEE Transactions on Information Forensics and Security, 2017. 12(6): p. 1319-1329.

32. Kim, J., H. Kim, and P. Kang, *Keystroke dynamics-based user authentication using freely typed text based on user-adaptive feature extraction and novelty detection*. Applied Soft Computing, 2018. 62: p. 1077-1087.

33. Saevanee, H. and P. Bhattarakosol. *Authenticating User Using Keystroke Dynamics and Finger Pressure*. in *2009 6th IEEE Consumer Communications and Networking Conference*. 2009.

34. Sulong, A. and M. Siddiqi. *Intelligent keystroke pressure-based typing biometrics authentication system using radial basis function network*. in *Signal Processing & Its Applications, 2009. CSPA 2009. 5th International Colloquium on*. 2009. IEEE.

35. Monrose, F. and A. Rubin. *Authentication via keystroke dynamics*. in *Proceedings of the 4th ACM conference on Computer and communications security*. 1997. ACM.

36. Monrose, F. and A.D. Rubin, *Keystroke dynamics as a biometric for authentication*. Future Generation computer systems, 2000. 16(4): p. 351-359.

37. Mantyjarvi, J., J. Koivumaki, and P. Vuori. *Keystroke recognition for virtual keyboard*. in *Proceedings. IEEE International Conference on Multimedia and Expo*. 2002.

38. de Magalhães, S.T., K. Revett, and H.M. Santos. *Password secured sites-stepping forward with keystroke dynamics*. in *Next Generation Web Services Practices, 2005. NWeSP 2005. International Conference on*. 2005. IEEE.

39. Modi, S. and S.J. Elliott. *Keystroke dynamics verification using a spontaneously generated password*. in *Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International*. 2006 IEEE.

40. Kang, P., S.-s. Hwang, and S. Cho. *Continual retraining of keystroke dynamics based authenticator*. in *International Conference on Biometrics*. 2007. Springer.

41. Monaco, J.V., et al. *Behavioral biometric verification of student identity in online course assessment and authentication of authors in literary works*. in *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on*. 2013. IEEE.

42. Rybnik, M., et al. *An exploration of keystroke dynamics authentication using non-fixed text of various length*. in *Biometrics and Kansei Engineering (ICBAKE), 2013 International Conference on*. 2013. IEEE.

43. Roh, J.-h., S.-H. Lee, and S. Kim. *Keystroke dynamics for authentication in smartphone*. in *Information and Communication Technology Convergence (ICTC), 2016 International Conference on*. 2016. IEEE.

44. Stanciu, V.-D., et al. *On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks*. in *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*. 2016. ACM.

45. Roy, S., U. Roy, and D. Sinha. *Protection of Kids from Internet Threats: A Machine Learning Approach for Classification of Age-group Based on Typing Pattern*. in *Proceedings of the International MultiConference of Engineers and Computer Scientists*. 2018.

46. Gaines, R.S., et al., *Authentication by keystroke timing: Some preliminary results*. 1980, DTIC Document.

47. Trojahn, M., F. Arndt, and F. Ortmeier. *Authentication with keystroke dynamics on touchscreen keypads-effect of different n-graph combinations*. in *Third International Conference on Mobile Services, Resources and Users (MOBILITY)*. 2013.
48. Ferreira, N.F.L., MRSensing - Environmental Monitoring and Context Recognition with Cooperative Mobile Robots in Catastrophic Incidents. 2013: University of Coimbra.
49. Sridhar, M., S. Vaidya, and P. Yawalkar. Intrusion detection using keystroke dynamics & fuzzy logic membership functions. in Technologies for Sustainable Development (ICTSD), 2015 International Conference on. 2015. IEEE.
50. Hussien, B., R. McLaren, and S. Bleha, An application of fuzzy algorithms in a computer access security system. Pattern Recognition Letters, 1989. 9(1): p. 39-43.
51. De Ru, W.G. and J.H. Eloff, Enhanced password authentication through fuzzy logic. IEEE Expert, 1997. 12(6): p. 38-45.
52. S, M. and S.S. Kumar, Proceedings of the Fourth International Conference on Signal and Image Processing 2012 (ICSIP 2012). 2013: Springer India.
53. Hocquet, S., J.-Y. Ramel, and H. Cardot, User Classification for Keystroke Dynamics Authentication, in Advances in Biometrics: International Conference, ICB 2007, Seoul, Korea, August 27-29, 2007. Proceedings, S.-W. Lee and S.Z. Li, Editors. 2007, Springer Berlin Heidelberg: Berlin, Heidelberg. p. 531-539.
54. Giot, R., M. El-Abed, and C. Rosenberger. Greyc keystroke: a benchmark for keystroke dynamics biometric systems. in Biometrics: Theory, Applications, and Systems, 2009. BTAS’09. IEEE 3rd International Conference on. 2009. IEEE.
55. Giot, R. and C. Rosenberger, A new soft biometric approach for keystroke dynamics based on gender recognition. International Journal of Information Technology and Management, 2012. 11(1-2): p. 35-49.
56. Idrus, S.Z.S., et al. Soft biometrics database: A benchmark for keystroke dynamics biometric systems. in Biometrics Special Interest Group (BIOSIG), 2013 international conference of the. 2013. IEEE.
57. Idrus, S.Z.S., et al., Soft biometrics for keystroke dynamics: Profiling individuals while typing passwords. Computers & Security, 2014. 45: p. 147-155.
58. Gascon, H., et al. Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior. in Sicherheit. 2014. Citeseer.
59. Jain, L., et al., Passcode keystroke biometric performance on smartphone touchscreens is superior to that on hardware keyboards. International Journal of Research in Computer Applications & Information Technology, 2014. 2(4): p. 29-33.
60. Çeker, H. and S. Upadhyaya. Adaptive techniques for intra-user variability in keystroke dynamics. in Biometrics Theory, Applications and Systems (BTAS), 2016 IEEE 8th International Conference on. 2016. IEEE.
61. Yu, E. and S. Cho, Keystroke dynamics identity verification—its problems and practical solutions. Computers & Security, 2004. 23(5): p. 428-440.
62. Giot, R., M. El-Abed, and C. Rosenberger. Keystroke dynamics with low constraints svm based passphrase enrollment. in Biometrics: Theory, Applications, and Systems, 2009. BTAS’09. IEEE 3rd International Conference on. 2009. IEEE.
63. Çeker, H. and S. Upadhyaya. User authentication with keystroke dynamics in long-text data. in Biometrics Theory, Applications and Systems (BTAS), 2016 IEEE 8th International Conference on. 2016. IEEE.