المجلة الإلكترونية الشاملة متعددة التخصصات
العدد السادس والعشرون شهر(7) 2020

"Investigating The Impact of The Variability in Keystroke Dynamics on Building a Reliable Biometric Template"

Khamiss M. S. Ahmed
Department of Computer Science
Faculty of Information Technology
Sebha University, Libya
km.ahmed@sebhau.edu.ly

Salwa Ali
Department of Networking
Faculty of Information Technology
Sebha University, Libya
sal.ali1@sebhau.edu.ly

Mahmmoud Alawan
Department of Computer Science
Faculty of Information Technology
Sebha University, Libya
m.lawan@sebhau.edu.ly

Abstract— One of the most important issues in gaining access rights to computer resources is user authentication. Passwords are the most commonly used method for computer authentication systems. This paper examines how factors such as individual typing ability, typing behavior, and password familiarity affect the use of keystroke dynamics with password authentication. The proposed study designed a multi-session experiment with twenty participants in which is collected and analyzed information samples related to these factors. This can be done by specifying the users' typing skills that subsequently will help in specifying the suitable features (heterogeneous or aggregated) to model users. This results show that the aggregated features seem to be the best representation for skilled and slow typists with an approximately 10 typing samples, regardless of the password familiarity, while normal typists were more suited to the heterogeneous features to form their typing behavior with 15 samples. This study also presents a novel method for imposter data collection, thereby allowing a more accurate assessment of security. The results demonstrate that it is not only the complexity of the password that determines the strength of the individualistic features of a user; it is also the way in which the user interacts with the keyboard.

Keywords- behavioural biometric; keystroke dynamics; password authentication; features extraction; statistical algorithm.

I. INTRODUCTION

The most significant issues in gaining access rights for computer resources is user authentication are knowledge-based, object-based and biometric-based (Bonneau et al.,2015). Passwords and biometric techniques have been utilized as a form of multifactor authentication, taking advantage of the individualistic features offered by biometric models to improve the limited security of a lone password. In this way, biometric-based authentication can serve to strengthen the verification process of users' identities (Harakannanavar & Renukamurthy & Raja, 2019). Biometric systems can be physiological, consisting of those features of the individual body that can be used to uniquely recognize someone, such as fingerprints, facial recognition and retinal scanning; or they can be behavioral, taking advantage of a person's behavior to distinguish them from others, noting effects such as gait and keystroke dynamics (Avasthi & Sanwal, 2016).

Keystroke dynamics, which measure the habitual pattern of a user's typing rhythm, offer a natural pairing with password authentication (Imane et al., 2018). Keystroke dynamic intelligence can be built in software and keystrokes can be easily collected at enrolment and used as a second factor along with the passwords for authentication (Yohan & Hanry & Dion , 2018).

In terms of keystroke behavior, each individual has various typing attributes, such as keystroke duration, error frequency, typing speed and keystroke interval time, and the level of uniqueness offered by keystroke dynamics is determined from extracting such features (Singh et al., 2019). Therefore, using passwords in addition to keystroke dynamics as a two factor authentication suggests a potential benefit in terms of security, deploy ability and usability. However, keystroke features can also demonstrate significant variations in typical typing models; if not modeled accurately, it can be difficult to translate the theoretical benefits of keystroke dynamics to a practical authentication solution (Chen et al., 2019). The inconsistency of keystroke features may occur because of the complexity level of the typed text, the individual typing proficiency and/or familiarity with the text.

The proposed study examines the behavioral impact of keystroke dynamics in terms of three factors:

1. Typing ability, such as an individual's typing speed and accuracy.
2. Typing behavior, such as an individual's use of "caps lock" versus shift keys when capitalizing password characters.
3. Password familiarity, such as whether or not an individual is enrolling with a self-chosen versus a server-issued password.

The aim of this study to designed a multi-session experiment in which the participants used the proposed enrolment and authentication software under several experiment conditions that were designed specifically to determine the impact of the above factors. The analysis of these conditions demonstrates that by determining a user's typing ability and behavior at enrolment, and explicitly recognizing whether a policy of user- or system-chosen passwords is being used, a more reliable biometric template can be constructed for each user. This means that when users are categorized based upon their typing ability and behavior, keystroke dynamics can be more effective.

II. KEYSTROKE DYNAMICS

Recent developments in biometrics have made it possible to gain advantages from the unique characteristic of humans. Nevertheless, certain biometric methods like fingerprints suffer from some limitations in terms of their requirement for special hardware (Masaoud et al., 2013). The idea that solves this issue is to generate the biometric information of users from a typical input device. In practical terms, the keyboard is the most input device regularly used by users. Keystroke dynamics is considered as valuable and flexible means of user authentication. It aims to compare the activity of current users with the stored sample of their biometric reference (Obaidatet al., 2019).

Keystroke dynamics application must monitor users' typing rhythms and learn the individualistic pattern that can be used to characterize them (Abualgasimal &Osman, 2011). Each individual has various typing attributes, such as keystroke duration, frequent error, typing speed and keystroke interval times. One benefit of using this method is its ability to systematically and invisibly monitor a person's keystroke; thereby determining whether or not he/she is authorized to use the system (Joyce & Gupta, 1990).

A. Features

The keyboard is recognized by the operating system as an input device, wherein two events are recorded – the key presses and the key releases, so that representative features of individuals can be extracted (Banerjee & Woodard, 2012). As showed in Figure (1), several different attributes can be derived from the individual's typing behavior, which are defined as their keystroke dynamics, as described by these two events over the duration in which a password is entered.

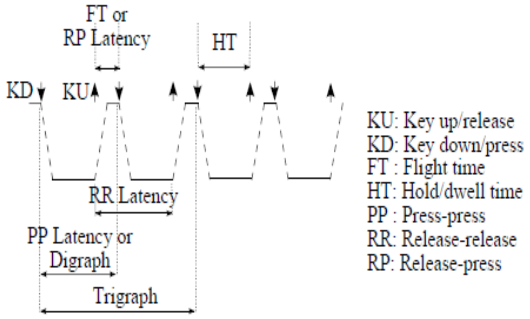

Figure 1.Keystroke dynamics' features (Banerjee & Woodard, 2012).

The first viability study of the use of a timing pattern of keystroke dynamics as an authentication method was conducted by Gaines et al. (Gaineset al.,1980) who defined the following features. The time duration between pressing and releasing a key is called hold time or dwell time. Certain layouts of keyboard can also measure the pressure on a key while typing (Joyce & Gupta, 1990). Applied digraph latencies between three letters (Magalhaes & Henrique,2005), and the application of a sole flight time feature (Haider& Abbas & Zaidi,2000). A recent study conducted by (Balagani et al., 2011) classified keystroke features as homogeneous if they involve only holding down a key or only an interval key latency, heterogeneous when they contain both key hold and key interval latencies, and aggregated if they combine (aggregate) key hold and key interval latencies, e.g., key press latencies add key hold and interval latencies.
Time latency was one of the most universally used features in many early studies. Three types of latencies can be considered: press-to-press (PP), release-to-release (RR), and release-to-press (RP). PP and RP are also called digraph and flight time respectively (Banerjee & Woodard, 2012). Some research has asserted that using a combination of flight time and dwell time features offers better performance than using the features on their own (Raghui et al., 2011), (Rybniket & Panasiuk & Saeed, 2009), (Georgios et al., 2016). Similarly, combining the dwell time feature along with the time latencies has been shown to offer a better performance than other combinations.

B. Classification methods

User classification based upon entered keystroke data is performed using the similarities and dissimilarities of the collected data against pre-computed templates. Whether or not the user is authenticated will depend upon the extracted details being within the predetermined tolerance limit (threshold) (Karnan & Akila & Krishnaraj, 2011). If the score is lower than the threshold, the claimant is accepted, otherwise rejected. The threshold value is determined according the required level of security by the application. Several statistical metrics have been suggested to quantify the performance of the biometric system (Giot & El-Abed & Rosenberger, 2012).
There are various classification techniques that can be used for the attempt-template comparisons, including statistical methods, neural networks, pattern recognition approaches and hybrid techniques. Considering the statistical approaches, the simplest methods are based on the mean and standard deviation of the features in the template (Khamiss et al., 2012). The comparison can be made using hypothesis tests, t-tests and distance measures such as absolute distance, weighted absolute distance, Euclidian distance (Haider & Abbas & Zaidi, 2000).

C. Keystroke entry and sample sizes

Keystroke recognition concentrates on the text input where abundant keystroke information is provided to allow the use of robust statistical feature measurement (Araujoi et al., 2005). In this respect, the analysis of keystroke dynamics can be categorized into static text, and dynamic or free text. The static analysis includes examining keystroke dynamics for a predefined text in the system. Dynamic text, on the other hand, involves periodic observation of keystroke behavior (Banerjee & Woodard, 2012).
In terms of using a familiar password, in the first study to use login information as short text to evaluate keystroke dynamics, participants were asked to provide their username and password samples eight times (Joyce & Gupta, 1990). An extended investigation of this study utilized four short texts provided by users – username, password, first and last name – over a period of eleven months, though the exact number of samples was not

clearly defined (Shinde & Shetty & Mehra , 2016). While in some cases subjects typed their passwords twelve times (Magalhaes & Henrique , 2005), only five samples were used to create the biometric template in work examined by others [28], where it was claimed that the number of samples required from users should not be less than ten samples in order to acquire a unique keystroke pattern. Confirming this, (Zhong & Deng & Jain, 2012) conducted a study in which participants were required to type their username and password ten times.
In terms of an unfamiliar password, several studies exploited imposed passwords in their experiments. Giroux et al. conducted a study in which subjects were given the password cosc1757 and asked to type it twenty times (Giroux & Wackowiak, 2012). Likewise, (Douhou & Jan , 2009) required participants to type an imposed username patrick and password water83 20 times. And another study required users to type their names and the imposed fixed phrases University of Missouri Columbia (Bleha & Obaidat, 1991).

III. METHODOLOGY

This study describes the experiment that covered multiple scenarios to gather the keystroke information of users' typing ability and behavior, taking into account their familiarity with the password. The proposed study started with a typing speed test that allowed classifying the participants based upon their individual typing speed and accuracy, followed by two enrolment scenarios: one with an imposed (unfamiliar) password, and the other with a familiar password. It hypothesize that users' keystroke dynamics may not have a significant difference between two sessions of an experiment, regardless the familiarity level with the password, so that not too many samples are needed to form the biometric template. Additionally, since the users will perform the enrolment process with the system provided password and each of whom will subsequently have to provide his/her personal password.
The experiment was performed with the initial involvement of 20 participants; however, the analysis of the data was evaluated on 16 participants (5 females and 11 males), as 4 users did not complete all tasks. The number of samples applied in this experiment was up to 20 samples per user in two different sessions (10 samples per session).
In order to evaluate how the number of samples affects the individuality of users' biometric templates, two different templates produced for each user. The first template created from the first ten samples in the first session, and the second produced from the first ten samples in the first session plus the first five in the second session. Selecting the first ten samples to produce the first template is normal procedure applied in the enrolment process of any biometric system, as it contains the information regarding the learning phase, which means that the samples have a relatively higher variation in terms of how the users will type the passwords.
The *assessment of typing speed* was performed using the following text, which was adapted from an online typing speed test with the password *Bx3ag7Fn* (CalculatorCat, 2012): *"Conversation should be pleasant Bx3ag7Fn without scurrility, witty without affectation, free without indecency, learned without conceitedness, novel without falsehood"*.
The typing speed was calculated on the basis of the number of typed keystrokes per second, while the accuracy rate was calculated as the ratio of the number of correctly typed words and the total number of words in the text (Slusher, 2012). The typing speed test takes advantage of applying a two session enrolment. This means that subjects will perform the typing speed twice (once each session), increasing the accuracy of the speed measurement as it is averaged over the sessions. Performing the typing speed twice also ensures that the resulting speed value represents the user's skills, avoiding inconsistencies that might appear if users' typing speed did not reflect their actual speed in one session.

A. Data processing and classification

As a result of the choice of password, the study anticipated different behaviors regarding the capitalization of letters in the password, which was confirmed by the subsequent experiment: some users used the caps lock key to produce the capital letters, whereas others used the shift, regardless of the familiarity with the context. Two such examples are shown in Figure (2). In addition; there was a noticeable overlapping in the keystrokes' order when using the shift key to produce the capital letters. In some cases, the shift key event occurred before the actual key, and vice versa in other cases. However, such behavior did not appear with users who used caps lock keys, and that made extracting the individualistic keystroke features challenging. Such behavior presented an interesting result to analyses, though also presented options for pre-processing as part of the data collection.

Cap lock Press Caps lock Released, B Press, B Released, Cap lock Press Caps lock Released, B Press, B Released, Cap lock Press Caps lock Released, X Press, X Released, 3 Press, 3 Released, A Press, A Released, G Press, G Released, 8 Press, 8 Released, Back space Press, Back space Released, 7 Press, 7 Released, Cap lock Press Caps lock Released,, F Press, F Released, Cap lock Press Caps lock Released, N Press, N Released.
Shift Press, Shift Press, Shift Press, Shift Press, Shift Press, Shift Press, Shift Press, Shift Press, Shift Press, Shift Press, Shift Press, Shift Press, B Press, B Released, Shift Released, X Press, X Released, 3 Press, 3 Released, A Press, A Released, G Press, G Released, 7 Press, 7 Released, Shift Press, Shift Press, Shift Press, Shift Press, Shift Press, Shift Press, F Press, Shift Released, F Released, N Press, N Released.

Figure 2: The key events of two different users, one using "caps lock" And the other "shift keys" when typing the imposed password (Bx3ag7Fn)

Consistent with previous research (Araujoi et al., 2005), both hold times and flight times were extracted from the input data. Nevertheless, the way in which the features were extracted from users in this paper was slightly different. Since there is an overlapping issue related to producing the capital letters using shift keys, using shift does not itself form a homogeneous feature like other keys; yet, the caps lock can be considered as a separable feature as it doesn't cause any overlapping issues. Therefore, it was decided to combine the features where the capital letter is produced by the shift key, regardless of the order of the shifts' events. As illustrated in Figure (3), the way in which the features were extracted differs from previous research in order to take this novel requirement into account.

In terms of data classification, this study adopted the algorithm of (Magalhaes & Henrique , 2005) which is based on the mean, median and standard deviation of the users' raw data, where the match of the tested (TLP) data is increased if the following condition is true: min(mean, median) * (0.95 – std/mean) ⩽ TLP ⩽ max(mean, median) * (1.05 + std/mean). According to their research, the user is accepted if the average match was equal to or greater than 70%.

Shift Press	B Press	Shift Released	B Released
=one feature			
Shift Press	B Press	B Release	Shift Released
=one feature			
Caps Lock Press	Caps Lock Released	B Press	B Released
= two seprable feaures (Caps Lock Press, CapsLock Released : one feature; CapsLock Released, B Press : one feature)			

Figure 3. Different features producing the capital letter

IV. RESULTS

In result was observed that the participants' typing speed ranged from 1 to 5 keystrokes per second, and the accuracy rate was between 28% and 100%. Grouped users into three categories according to their keystroke rate per second (kps): slow (1 kps) - users: U1-U7; normal (2-3 kps) - users U8-U18; and skilled (4-5kps) - user U19 and U20.

Figure (4) shows the typing speed and accuracy results for the participants based upon their entering of the pre-defined text. The main observation across the different speed groups is that the rates of accuracy vary considerably for the slow typists, while there is relative consistency in the accuracy for the normal typists. Confirming this, the result of the t-test showed that there was no significant difference in the accuracy rate associated with the normal typists as opposed to slow typists, whose accuracy rate witnessed a significant difference between the two sessions.

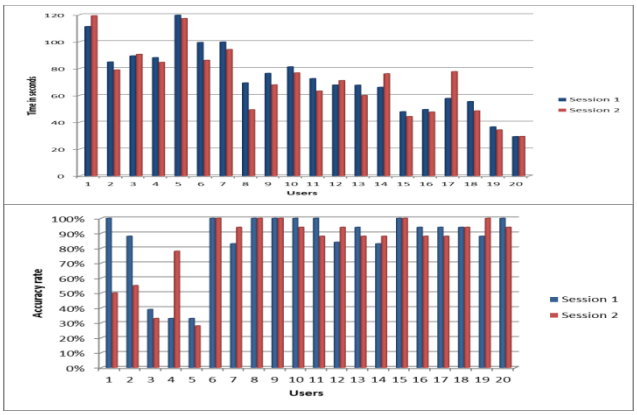

Figure 4.Total time taken to type the imposed password versus accuracy rate

Figure (5) demonstrates the variation in the individualistic features of the subjects after combining the features set of the first session, compared to the variance level of users' keystroke attributes based on two enrollment sessions (20 samples). It is noticeable that using only the first ten samples reveals a better dimensionality of combined features between the subjects, which helps in differentiating them. Considering the users' typing ability, it appears obvious that increasing the number of samples to 20 did not affect the features' discriminability among slow and skilled users; whilst, some normal typists lost their individualistic attributes (e.g. U12-U16). All in all, it seems that the variance of the users' aggregated features did not experience a significant change by increasing the number of samples to 20.This result agrees with previous research (Balagani et al., 2011) in that using 10 samples would be sufficient to model the individualistic feature of users.

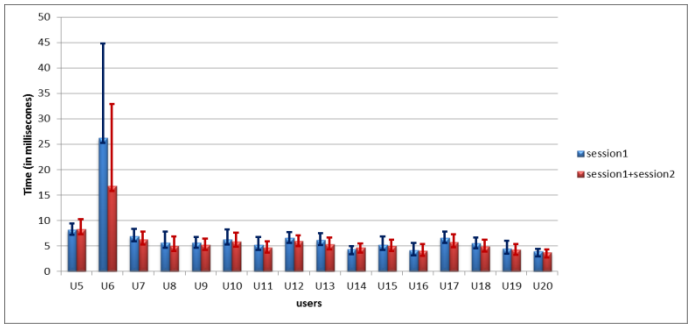

Figure 5.The representation of the combined features from 10 samples against 20 samples

In terms of the enrolment with a familiar password, different passwords have been provided by different users, all of which were strong in terms of the security requirements. Importantly, the complexity of users' passwords was determined by considering their length and placed into two groups: Group 1 ranges between 6 to 8 characters; Group 2 ranges from 9-12 characters. Table (1) shows the distribution of users and their corresponding group.

Table 1.The classification of users corresponding to the complexity of their passwords

User	U5	U6	U7	U8	U9	U10	U11	U12	U13	U14	U15	U16	U17	U18	U19	U20
Group	2	2	1	2	2	1	1	2	1	1	2	2	1	1	2	2

Figure (6) reveals the heterogeneous features associated with U8 and U12 while enrolling with the unfamiliar password using 10 samples and 15 samples. Although both users were classified as normal typists, their individualistic attributes could clearly be defined when they typed the same password (Bx3ag7Fn).

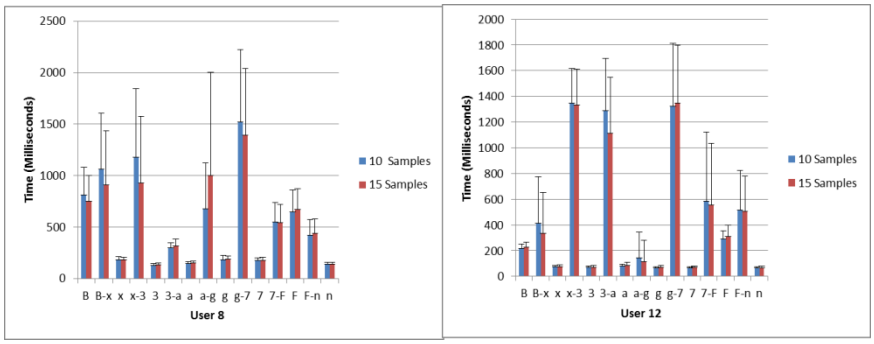

Figure 6.The heterogeneous features associated with two different users typing the imposed password

The analysis of the data shows that there is no significant difference in the heterogeneous features associated with users' keystroke dynamics between the two sessions. On the other hand, examining the difference between the heterogeneous attributes would not be relevant in terms of the familiarity of the password. This is due to the fact that the heterogeneous features associated with users' familiar passwords differ from the imposed password, and that the analysis of the statistical test cannot be made in this term.

A. The authentication peocess: the evaluation of the classification algorithm

Since different users typed others' passwords, the results show whether or not different users can impersonate the genuine users' password without them having the knowledge that what are typed are other users' passwords. The strength of the provided passwords ranges between users. Despite this, the passwords might not be strong enough when it comes to the keystroke dynamics as a second factor of the password. The biometric system makes the authentication decision based on a predefined threshold value, which sat to 70% in this experiment. If the score is lower than this value, the claimant is accepted, otherwise it is rejected. The most striking point in Figure (7) is the coincidence of the FRR and FAR at 0.0% in three passwords associated with users 7, 17 and 20 The value for which FRR and FAR is identical is called ERR (Equal Error Rate), which represents a good way of examining and comparing biometric systems. The lower the ERR, the more accurate is the system. As a result, the passwords associated with the users 2, 17 and 20 are most likely to be challenged.

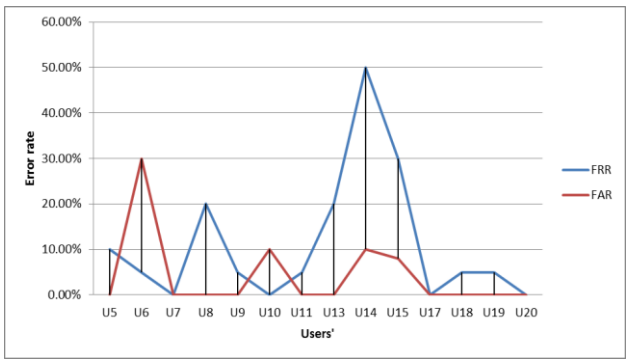

Figure 7.The performance of the classification algorithm

Considering the difficulty level of the password, it must be noted that it is not only the complexity of the password that specifies the distinctive characteristic of the users' keystroke dynamics, but also the way in which the user interacts with the keyboard.

V. DISCUSSION

The findings suggest that there is a relationship between the time that users took to type the text, their typing speed and accuracy. While an individual with normal typing speed maintains their accuracy rate with the time they took to type the text, slow typists demonstrated certain inconsistencies between these factors. Interestingly, the results proved that users with different typing skills can maintain a certain level of variation in typing

unfamiliar passwords in different contexts, showing a level of discriminability between their keystroke features. Since individuals have different typing skills and different behaviors on the keyboard, the enrolment environment should be specified, considering all these factors, to determine the number of required samples and which features are to be deployed.

VI. CONCLUSION

The result of this study showed that it is the typing accuracy rate that specifies the variations within the keystroke features. While the variance of the features associated with slow typists decreased as they were familiar with the password, users typing at normal speed demonstrated unequal variance. Skilled users, on the other hand, preserved a certain level of variance on their keystroke dynamics, regardless of familiarity with the context. In conclusion, it seems that employing the relevant attributes to model the users and taking into account the users' typing skills help in forming a clear picture of the users typing behavior. By doing so, building an effective individualistic template while maintain a usable, reliable robust enrolment within the biometric system.

VII. FUTURE WORK

This research has thrown up many questions in need of further investigation. Since few users were slow and skilled typists, further research is recommended to evaluate the experiment with the involvement of more participants with different typing skills to draw a clearer conclusion about the study. Moreover, it could be interesting to explore whether or not skilled individuals can slow their typing and impersonate slow typists. More broadly, the study is also in need of capturing the keystroke dynamics associated with the users' passwords in different occasional time situations. In doing so, the full picture of the user's typing behaviour can be drawn. More importantly, it could worthwhile investigating the extent to which a specific level can shoulder a surfing attack being replicated, to monitor the typing behaviour of individuals.

References

1. Bonneau , J., Herley ,C., Oorschot, P.C. van & Stajano, F. 2015. Passwords and the Evolution of Imperfect Authentication, *Communications of the ACM*, July 2015, Vol. 58 No. 7, Pages 78-87.

2. Harakannanavar,S. S., Renukamurthy,P. C., and Raja,K B. (2019). Comprehensive Study of Biometric Authentication Systems, Challenges andFuture Trends, Int. J. *Advanced Networking and Applications* Vol: 10 Issue: 04 pp: 3958-3968 (2019) ISSN: 0975-0290.

3. Avasthi,S., Sanwal ,T. (2016). Biometric Authentication Techniques: A Study on Keystroke Dynamics, *International Journal of Scientific Engineering and Applied Science (IJSEAS)* – Vol: 2, pp 215-221, Issue-1, January 2016 ISSN: 2395-3470.

4. Imane L., Guo B., Yao J., Zhiwen Y., and Abdenour H.(2018). A continuous smartphone authentication method based on gait patterns and keystroke dynamics, *Journal of Ambient Intelligence and Humanized Computing, DOI*: 10.1007/s12652-018-1123-6 , https://doi.org/10.1007/s12652-018-1123-6.

5. Yohan M., Hanry H., and Dion D. (2018). Keystroke Dynamic Classification using Machine Learning forPassword Authorization, *3rd International Conference on Computer Science and Computational Intelligence ,Procedia Computer Science* , DOI: 10.1016/j.procs.2018.08.209. Vol:135, pp564-569.

6. Singh, B. , Kaur, N., Kumar, A., and bhatia ,K.(2019). Analyzing user typing behaviour in different positions using keystroke dynamics for mobile phones, *Journal of Discrete Mathematical Sciences and Cryptography* , Vol: 22, 2019 - Issue 4: Threats & Applications for security, pp 591-603.

7. Chen ,J., Zhu ,G., Yang, J., Jing ,Q., Bai, P., Yang ,W., Qi, X.(2015) . Personalized eystroke Dynamics for Self-Powered HumanMachine Interfacing, *ACS Publications*, VOL. 9' NO. 1' pp.105–116.

8. Masaoud ,K, S Algabary., Omar ,K., Nordin ,MJ .(2013). A Review Paper on Ear Recognition Techniques: Models, Algorithms and Methods, *Australian Journal of Basic and Applied Sciences*, 7(1): ISSN 1991-8178, PP. 411-421.

9. Obaidat,M,S., Venkata,Krishna,P., Saritha,V., Agarwal,S. (2019). Advances in Key Stroke Dynamics-Based Security Schemes. In: Obaidat M., Traore I., Woungang I. (eds) *Biometric-Based Physical and Cybersecurity Systems. Springer*, Cham, pp 165-187. DOI https://doi.org/10.1007/978-3-319-98734-76.

10. Abualgasim, S.D. and Osman, I. (2011). "An application of the keystroke Dynamics biometric for securing PINs and passwords", *WCSIT*, 1(9), pp. 398-404.

11. Joyce, R. and Gupta, G.(1990). "Identity authentication based on keystroke latencies", *Communications of the ACM*, 33(2), pp. 168-176.

12. Banerjee, S.P. and Woodard, D.L, .(2012). "Biometric Authentication and Identification using Keystroke Dynamics: A Survey", *Journal of Pattern Recognition Research*, 7(1), pp. 116-139.

13. Gaines, R. S., Lisowski, W., Press, S. J., & Shapiro, N. (1980), "Authentication by Keystroke Timing: Some Preliminary Results", *tech. report* R-256-NSF, RAND.

14. Magalhaes, P.S.S. and Henrique, D.D. (2005). "An improved statistical keystroke dynamics algorithm", Proceedings of the IADIS – *Virtual Multi Conference on Computer Science*, Lisbon.

15. Haider, S., Abbas, A. and Zaidi, A.(2000). "A Multi-Technique Approach for User Identification through Keystroke Dynamics*", IEEE International Conference of Systems, Man and Cybernetics*, 2, pp 1336-1341.

16. Balagani, K.S., Phoha, S., Phoha, V.V. and Ray, A. (2011). "On the discriminability of keystroke feature vectors used in fixed text keystroke authentication", *Pattern Recognition Letters*, 32(7), pp. 1070-1080.

17. Raghu, D., Jacob, Ch.Raja., Bhavani, Y.V.K.D. (2011). "Neural network based authentication and verification for web based keystroke dynamic", IJCSIT, 2(6), pp. 2765-772.

18. Rybnik, M.; Panasiuk, P.; Saeed, K. (2009). "User Authentication with Keystroke Dynamics Using Fixed Text," Biometrics and Kansei Engineering, 2009. *ICBAKE. International Conference*, pp. 70-75.

19. Georgios K , Dimitrios D, Dimitrios P and Emmanouil P, .(2016). Introducing touchstroke: keystroke-based authentication system for smartphones, *security and communication networks*, vol.9: pp.542–554.

20. Karnan, M., Akila, M. and Krishnaraj. N. (2011). "Biometric personal authentication using keystroke dynamics: A review*", Applied Soft Computing*, 11(2), pp. 1565-1573.

21. Giot, R., El-Abed, M. and Rosenberger, C.(2012). "Fast computation of the performance evaluation of biometric systems: Application to multibiometrics", *Future Generation computer center*.

22. Khamiss ,M.S.Algabary, Khairuddin Omar, Md. Jan Nordin and Siti Norul Huda S. Abdullah. (2015). Ear Identification Based on Improved Algorithm of ICPSCM. *Journal of Applied Sciences*, 15: 815-820. DOI: 10.3923/jas.2015.815.820. URL: https://scialert.net/abstract/?doi=jas.2015.815.820

23. Haider, S., Abbas, A. and Zaidi, A. (2000). "A Multi-Technique Approach for User Identification through Keystroke Dynamics", *IEEE International Conference of Systems, Man and Cybernetics*, 2, pp 1336-1341.

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

25. Banerjee, S.P. and Woodard, D.L. (2012). "Biometric Authentication and Identification using Keystroke Dynamics: A Survey", *Journal of Pattern Recognition Research*, 7(1), pp. 116-139.

26. Shinde .P, Shetty .S, Mehra.M, . (2016). Survey of Keystroke Dynamics as a Biometric for Static Authentication, *International Journal of Computer Science and Information Security* (IJCSIS),Vol. 14, No. 04, pp. 203-207.

27. Magalhaes, P.S.S. and Henrique, D.D, .(2005). "An improved statistical keystroke dynamics algorithm", Proceedings of the IADIS – *Virtual MultiConference on Computer Science*, Lisbon.

28. *Anderson, A. and Hagen, S.* (2007). "Using Alert level to enhance keystroke dynamic authentication", Masters' thesis, Oslo University: Norway.

29. Zhong, Yu., Deng, Y., Jain, A.K.(2012). "Keystroke dynamics for user authentication", Computer Vision and Pattern Recognition Workshops (CVPRW), *2012 IEEE Computer Society Conference* .pp.117-123.

30. Giroux, S. and Wackowiak,Smolikkova, R. (2009). "Keypress interval timing ratios as behavioural biometrics for authentication in computer security*", IEEE 1st International conference*, p.p 195-203.

31. Douhou, Salima & Jan R. Magnus. (2009). "The reliability of user authentication through keystroke dynamics", *Statistica Neerlandica*, vol. 63, no. 4, pp. 432.

32. Bleha, D. and Obaidat, M. (1991). "Dimensionality reduction and feature extraction applications in identifying computer users," *IEEE Trans. Syst., Man, Cybern*., 21, pp. 452-456.

33. CalculatorCat (2012): www.CalculatorCat.com.

34. Slusher, Jered. (2012), "how to calculate the number of keystrokes per minutes", available online: http://www.ehow.com/how_6185939_calculate-keystrokes-per-minute.htm.