Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 8, July 2021: 200-211

User Identification on Smartphone through Authentication Using Keystroke Dynamics

Ms. PragyaVaishnav[a],Dr. ManjuKaushik[b] and Dr. LineshRaja[c]
[a] Research Scholar, AIIT, Amity University, Dept. of AIIT Jaipur,Rajasthan,India,
[b] Associate Professor, Dept. of AIIT, Amity University, Jaipur, Rajasthan, India,
[c] Assistant Professor, Dept. of Computer Application, Manipal University, Jaipur,Rajasthan,India,

Abstract:-

Currently Smartphone has become primary necessity for populace. Everyone managetheir personal and confidential data on mobiles. However it is essential to increase the security of the smartphone.Authentication is a process or action to verify the identity of a user or process and it prohibitsthe unauthorised access from intruders. Password is the universal key component of authentication that is easy to crack as everyone can remember the password. Therefore it is required to use advance mechanism to enhance the security.Keystroke dynamics is a secure and authenticbehavioural biometricbased technique based on typing behaviour of any individual. This technique identifies the identity of the userthroughtheir typing behaviour on keyboard. In this paper author comparing the features and methods of keystroke dynamics to find the best accuracy result mention in Table 2 of section 2 and comparing the different positions of using smartphone to get the best EER as well in Table 3of section 5.

Keywords:- Keystroke Dynamics, Dwell Time, Flight Time, Accelerometer, Gyroscope

1. Introduction

In day to day life smart phones have become a boon for every individual, for both purposes: professional and personal use. TOUCH screen came with revolution, provided high flexibility, user input technologies, and better serviceability for mobile computing devices. Smartphonedesigned with touch screens have become dominant in our life with expanding rich features, increased computing power, and maximum storage volume. Maximum applications (banking, emailetc.) which were run on computersnow universally run on smartphone. Smartphone contains private and sensitive information such as personal photos, videos, contact numbers and address, email, ATM/credit/debit card numbers, passwords, banking details, business data, and even corporate secrets. Most of the users keep their personal and sensitive data on their mobiles.

Therefore every individual are on risk as their personal data are stored and accessed using smart phones. The stealing or accidental loss of a mobile can reveal any professional and personalinformation kept on smartphone, Table 1 shows, if Smartphone is lost or an unauthorized access has done, the information are immediately under on serious security risk. Hence the personal data on smartphone creates risk. Keypad lock and Password are very common solutions to protect the smartphones. Android phones have geometric pattern on a grid of points and iPhones have 4 digits PIN, these PIN and the pattern are security features as everyone apply on their smart

phones. To unlock the device password/PIN/ and pattern have major weaknesses. Table 1[37] shows the probability of percentage of the unauthorized data access by theft if smartphone lost.

Table **1** confirms the following:

- Created Password has less entropy.

- Due to left finger oil on the screen it is traceable and disclose therefore easy to crack.
- Security is not available against shoulder surfing attacks as password does not store personal identity of the individual [27].
- The pattern lock does not provide a unique fingertip capability of the multi-touch screens where everyone can use multiple fingertips to connect with a smartphone.

Types of Data	**Percentage of probability of accessed data**
Personnel data	89%
Private photos	72%
Online Banking App	43%
Social networking accounts and personal email	60%
Saved Password file	57%
Contact	45%
Cloud data	48%
Salary Information	53%

Table 1 percentage of the unauthorized data access by theft

A secureuser authentication program is based on typing rhythm on smartphone, called as KEYSTROKE DYNAMICS, is fully capable to remove all gap of password authentication.

2. Related work

Author explained his survey paper what is keystroke and their feature[6], Author explained about digraph and trigraph and also explained about motion sensors[28], Author proposed 3 classification, i.e. k Nearest Neighbors (KNN), Random Forest, and Naïve Bayes, which is used as data categorization and they are using 10-fold cross validation to validate the data and evaluating the percentage of accuracy and the EER is comparing the classification techniques[31]. According to author Naïve Bayes provides the worst performance and for time based feature Random Forest classification provides the best performance. we get higher accuracy percentage by easy password. Hence, kNN gives the best percentage of accuracy for keystroke dynamics and touch device sensors, which is very near by Random Forest. Digraph (2G) keystroke count on two successive keys, trigraph

(3G) keystroke count on three successive keys, hold time, and completion time of typing. Author proposed statistical count like average, variance, and standard deviation. For the acceleration, author used the average. According to author prototype's low FAR (7.0%) specify that the model works good on blocking when someone intentionally try to access account of other. Hence, identification is little bit higher average of 60% to 70%, It doesn't mean that this system can perfectly recognize Smartphone users [19]. Author proposed fusion approach in which two mode combined first one is keystroke dynamics:-it comes with typing behaviour and second touch gesture:- it comes with tap, swipe, and pinch behaviour. Both authentication modes are made by two-class machine learning classification. On Android devices the authentication process continuously runs. On FRR modality experiment, continuous fusion authentication, performance test more gives accurate rather than FAR[6]. Author proposed Braille, a method which makes enable to read for visually impaired people. In the paper Braille, screen direction and pressure measurement are features of key stroke dynamics. braille input, screen rotation and pressure identification give high preference to provide user comfortless and flexibility[20]. Author using to check the errors. They have decided pass marks to compare the total errors. It provides accurate result [8]. Author using two methods for taking input during registration by taking password and passcode (4 digit pin). During login time they will first check password and then 4 digit pin. By this approach can know about their identity [23]. KeySens is a structure which is used for micro-behavior, without any related information of the entered text it check the exact location touched on each and every key, length of the pressed key, the pressure of touch or the touched area to identify user even of figure press. To recognize an unauthorized user, KeySens needs 5 key-presses with a 32.3% of FAR and a 4.6% of FRR, after 15 key-presses with a 14% of FAR and a 2% of FRR [8]. Author combines the different combinations of features and through these combinations they apply experiments on every user's posture. Then, he examined the performance of these feature combinations such as table, hand, and walk is the performance of postures. The pre-processing gave good results with scaling and standardization and without pre-processing distance algorithm also got better result using mean absolute deviation or standard deviation [17]. Author introduces a novel continuous biometrics authentication method combined two authentication feature keystroke dynamics and touch gestures. This assesses the feasibility approach they applied it in mobile banking application which applied on Android devices. This assessment collects the data from 25 users and got a 98.2% of accuracy [21]. For continuous authentication, Author developed HMOG system, a set of feature of behavioural biometric authentication applied on mobile user. Author assessed HMOG from three points of view which are BKG, energy consumption, and continuous authentication. Their assessment applied on multi-session data thatwere collected from 100 participants in the form of two motion positions i.e., sitting and walking. During walking they received 8.53% authentication EER through combining HMOG with tap features, and during sitting 11.41%, it is less than from EERs received from user with tap or HMOG features. They got the lowest EERs by using fusing HMOG, tap and keystroke dynamic features here author achieved 7.16% in walking and 10.05% in sitting. Their results shows that HMOG is a good for throughout monitoring in authentication of individual and especially during walking HMOG increase the performance rate of taps and keystroke dynamic attribute as well. For BKG, as compare to 25.7% of tap and 34.2% of swipe attribute HMOG gives lower 17.4% of EER. Furthermore, with tap features, fusion of HMOG gives the better accuracy with 15.1% EEE and, the energy overhead of sample collection and feature extraction is less when sensors were collected at 16Hz then less than 8% energy overhead. It shows that HMOG is good for energy-constrained devices like mobiles [33]. Author developed a system by using that system which is based on the swipe movements he can differentiate an authorized user from an unauthorized user. He displayed the performance of every user, and between them, the

random forest classification shows the remarkable output. 94.97% accuracy achieved the system using this classifier. The output shows that every user can be verifies based on his unique typing rhythm [2]. Author proposed a novel approach for authentication on Smartphone which will take user's fingerprint, login is and password. Author has three phases and two stages. The phases are:- 1. Fingerprint 2. Login username and password, 3. Keystroke dynamics. Two stages are:- 1. Enrolment period (Training period), 2. Verification Period. They are providing the extra level security Based on this approach [10]. Author is applying a Least Squares SVM classification with RBF kernel. They are exploring, discussing and finding result by Digraphs and Trigraphs features by using misclassification analyses and overall typing session's verses sentence to sentence classification [12]. Especially for mobiles which are lace with advanced sensors and to find out accurate result for Smartphone devices, author analyzed sensor-based attribute. They got the Up Up (UU) feature to arrange each individual user they used timing features and the min, max, and mean feature and sensor-based features for getting accurate result. This represent higher accuracy rate rather than timing based features. Normal and Moving postures is not getting good accuracy but they got higher accuracy from the min, max, and mean features from the sensor-based features.

In the Table 3 posture, key timing and the sensor-based features was not showed unique patterns of keystroke [29]. Author proposed Medians Vector Proximity method which is good in user authentication to get efficient anomaly detection performance. This method shows comparison between training vector and testing vector, applied on classifier which involves simple threshold limits comparison. It increased performance of anomaly detection, 92% of Hit Rate, still 0.08 at EER point is too much less than the criteria of industry 99.999%[24]. Author is using SVMs and DTs classification to arrange each and every user in the form of the given timing features. It is free-text for user authentication this is the fact that they have considered. They generated accurate output. They provide full knowledge for user authentication. The FAR and FRR rates gave acceptable result but FAR gave little bit better result from the both. In Arabic typing to authenticating users this proposed method has been successful. This method was initially produced for using with English typing. In their comparative study SVMs gave less error rates than DTs. When they compared to latency times, total time of typing gives more contribution to improve the system performance [5]. According to author FRR is lower than the FAR. Absolutely, the best procedure is if they are applying the force and the size of the keystrokes both [22]. For Android Smartphone touch screen devices author proposed behavioural authentication structure based on KSD method with NN learning algorithm. For each letter they are using virtual keyboard for capturing timing and non-timing features like duration time, size, force and position of every letter. As a second factor authentication, KSD gives allowable level in performance measures; they received 2.2 of FAR, 8.67 of FRR and 5.43 of EER [7]. According to author passwords has come into limitation and creates huge risks in existing authentication systems. Since the 1970s. 1977 a habitual patterns of the individual's typing rhythm explored from last two decade, Forsen et al. explored that individual must be differentiated by the way of typing their names[14]. Zheng et al. measured the user tapping behaviours on Smartphone's touch screen by using four features like size, acceleration and time. To use of the data of both 4-digit and 8-digit PINs, they calculated the outcome of the system by using all the experiments. Giuffrida et al [25]. Author presented the architecture of UNAGI associated with sensor-based information to a series of key-pressed occurrence [13]. Maiorana et al. is using statistical classifier, the method that shows is time paused between strokes and performed user between strokes and performed user identification [9]. Buchoux et al. They used for terms of PIN and the second was keystroke analysis duration of the sign in process. To getting this, they captured key strokes and inter-key latencies. A

group of 20 subjects used to calculate the implementation. With statistical classifiers technique is applicable for Smartphone's, but a 4-digit PIN is too less to capture appropriate output [1]. Table **2** provide the detailed comparison of keystroke dynamics algorithm.

Table 2 Comparison of Features, Algorithms, FAR, FRR, EER and Accuracy.

Study	Classification	Method	Feature	User	FAR %	FRR %	EER %	Accuracy %
Kyle R. Corpus, Ralph Joseph DL.Gonzales ,2016[19]	–	average, variance , and standard deviation	Digraph, Trigraph	6	7.0	40		60
Darren Cilia Frankie Inguanez2018 [12]	SVM with a Gaussian RBF kernel	–	Digraph	24	4	3	3.93	96
			Trigraph	24	2	1	1.42	99
Tanapat Anusas-amornkul2000 [31]	Random Forest	–	Using all features H+DD+UD + P+FA+AX +AY+AZ	20	–	–	5.1	97.90
Lin J-H, Chang T-Y, Tsai C-J,.2012 [11]	–	Mean and SD	Latency	100	11.22	12.2	12.2	–
			Pressure		14.54	14.6	14.6	
Cheng PC , Tasia CJ, Chang TY, , Lin JH.2014 [32]	–	Statistical	HT/latency	100	11.72	11.6	11.72	–
			Time, pressure, Size		9.78	19	10	
Karatzouni S, Clarke N.2007 [18]	–	–	Latency	50	15.8	9.1	12.2	–

3. Keystroke dynamics

Keystroke dynamics is a behavioural biometric based technique, It is automated method of identifying or confirming the identity of a user through their typing rhythm on a smartphone's keyboard. In another words it is the timing generated of typing patterns or rhythm while a person is typing on keyboard. Keystroke dynamics includes:

- Total typing speed.
- Differences of speed while finger is shifting between particular keys.
- Common errors during typing.
- Time length of keys are released.

3.1 Features

As compared of the other types of biometrics authentication system Keystroke dynamics authentication system on Smartphone provides various kind of appropriate features. These are given below:

- **Increase Security**: Keystroke patterns cannot be regenerate than written signatures, because before locking down the account, most of the security systems permit finite number of errors during input attempts. If keystroke pattern is changed, then can be easily regenerate new typing biometric template.

- **Continuous Monitoring**: In Keystroke dynamics through user typing rhythms it is possible to keep monitoring to check the identity of the user rather than login time. Without any instruction user re-authentication can be easily performed and can monitor to the user continuously till the end of the session. Therefore, safety level of protection keep continues even after login session without any compromise of serviceability. This is up most best remarkable feature of keystroke dynamics biometrics rather than other physiological biometrics.

- **Flexibility**: If in case when a password linked with a keystroke dynamics template and it get compromised, then can easily generate a new keystroke dynamics template whenever a new password is generated. This is an advantage which is not in other physiological biometrics. For instance, in fingerprints biometrics, by default humans have only 10 fingers in hands to use so the number of replacements is limited and with iris or face recognition is same, if they get changed, then there is no any substitution.

- **Transparency**: Keystroke dynamics authentication program needs less or nothing extra involvement from a smartphone individuals,because the receiving and processing of typing rhythms run in the backend while the individual is working on the smartphone. Without any knowledge of users that their typing rhythms are being captured in background, and this captured data used in authentication process, and the authentication process is going on concurrently hence it is secure through additional feature of authentication.

- **Non Expensive**: In other physiological biometrics authentication techniques like iris and fingerprint biometrics that generally needs of specific hardware for use, keystroke dynamics recognition is a fully software based implementation. It is not the matter of to reduce deployment cost of specialized hardware but provide a perfect scenario for implementation in remote authentication environment. Therefore low dependency on specialized hardware is the benefit of keystroke dynamics.

3.2 Issues

To develop of a keystroke dynamics authentication system bring down a severalchallenging issues:

- **Less Computation and Communication Costs:** In mobile devices computational features are typically less than personal computers. Hence certain criteria like algorithm complexity, communication cost, and authentication delay are valuable and must be examine in the design of keystroke dynamic authentication solutions. Therefore algorithm and communication costs imported as the result of deploying in authentication must be less.

- **Lesser Energy Consumption**: Unlike desktop computers, smart devices are run through batteries. The mobile device can operate long time as minimize the energy an application consumes. Even communication is the big consumer of the battery power in a smart device (Perrucci et al., 2009) [1], Different measures, like decreasing the sampling rate or run complex computation only take place while a device is being charged, has been introduced to decrease power consumption of a smart device.

- **Increase Accuracy**: The accuracy performance of keystroke dynamics authentication system is less, rather than other physiological biometrics authentication system such as fingerprint, face recognition and iris. Because of keystroke dynamics biometrics features evolved at various moments are likely to showing a particular amount of changes because of other factors such as tiredness, mood swing, or distraction. Hence, itmust be given as how to enhance the accuracy performance of a keystroke dynamics authentication system in the design of the method.

- **Adaptation Capability**: Over the time period human behavioural characteristics typically changed, and they often change more frequently than physiological characteristics. A user's keystrokes behaviour can constantly change as the user gets friendlier with the passwords, input method, device, and other external factors. A keystroke dynamics authentication system must be efficient of accepting itself to any modifications in a user's typing rhythm.

3.3 Feature Extraction

Required data received from mobile phone are categorized into two parts, first: - keystroke data and second:- motion data. Gesture APIs is used to measure the keystroke data that grasps touch inputs from keystroke of smartphone such as "time," "size," "coordinate,". In motion sensor data, all related to movements on screen can be received from: accelerometer and Gyroscope. These features are explained in the following sections.

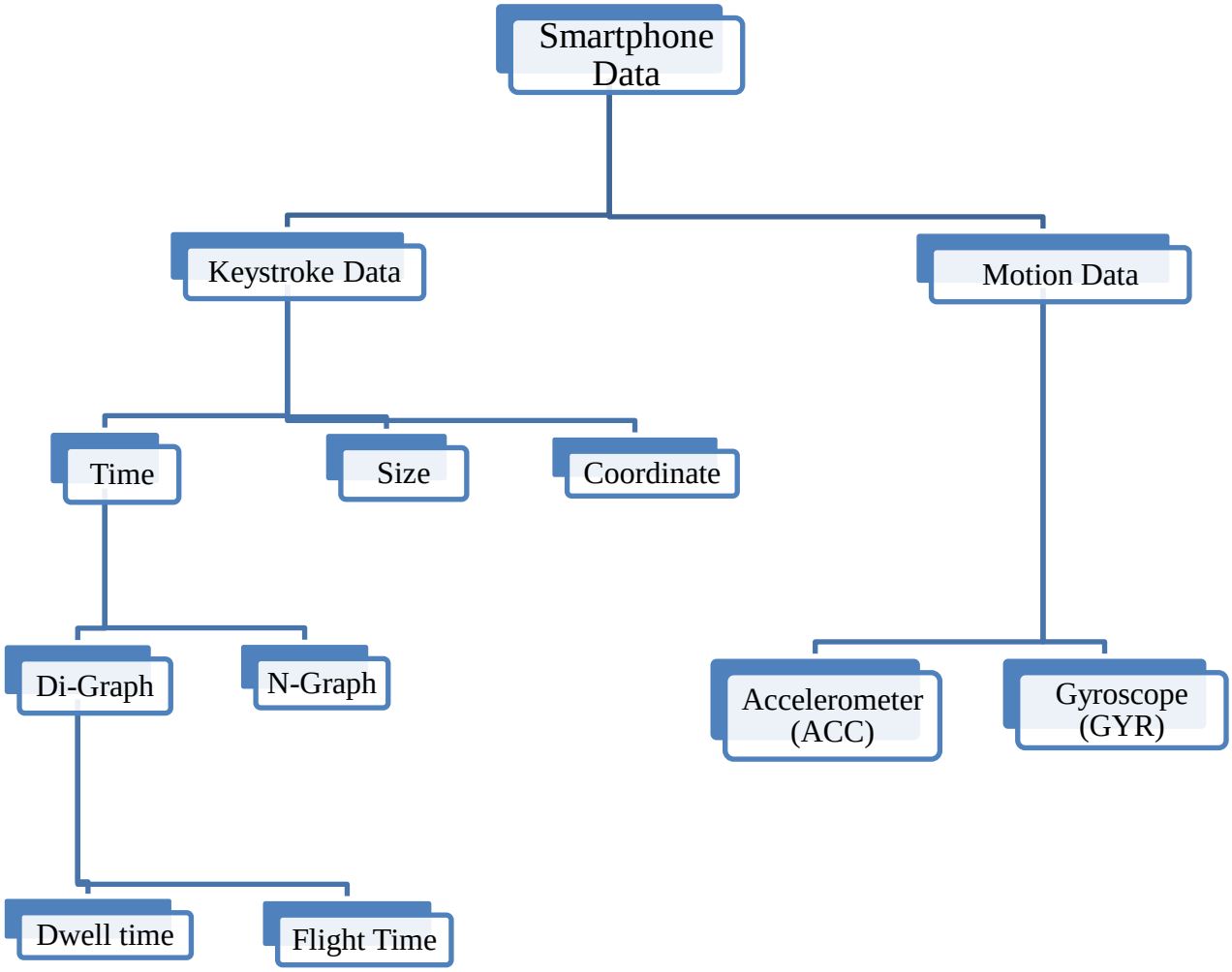
3.3.1 *Keystroke Data*

3.3.1.1 Time: "Time" returns the time when events occurred, it can be divided into two parts.

a. ***Di-Graph:*** This is main feature of keystroke dynamics. It takes timing data input from two sequential keystrokes events [30]. This is divided into two categories, Dwell Time and Flight Time both have fairly weightage in the base of frequency.

- ***Dwell Time (DT):*** Dwell time mention in touch events, it is the time of single key. It determines, how much time a key was hold on in pressing down. It called as hold time, interval, or duration as well. It is the amount of time duration between pressed and released of the single key.

- ***Flight time:*** It mention the time duration between two sequential keys in touch events. It is known as latency, latency time [38, 38], interkey time [37, 39] or interval time [40, 41]. It requires key press and release event of two keys, it may be same or different letters.



b. **N-Graph:** N-graph mention the time duration between three or more sequential keystroke events. It is proceed time between keys and the key event of a typing pattern.

3.3.1.2. Touch Data: Two data are captured based on touch:

a. ***Finger Size:*** It refers fingertip size that pressed on touch screen, it returns fingertip's size of the user each time pressing and releasing happen.

b. ***Finger Pressure:*** It determines pressure of finger on touch screen.

3.3.1.3. Coordinate: "Coordinate" gives coordinate values for horizontal axis and vertical axis, when a key has pressed (Dn) and releasing (Up) on screen of a smartphone. It refers coordinates of a point where individual has touched.

3.3.2 Motion Sensor

a. ***Accelerometer (ACC)*:** The accelerometer is a technique which has improved the individual's experience on touch devices like mobiles and tablet PCs. The important feature of this technology is to accept the change of orientation even when the position is changed from horizontal to vertical and vertical to horizontal. Actually this technique calculate the direction change and positions of the touch screen, An accelerometer measures linear acceleration of movement, "Accelerometer" measures device's accelerometer () of 3 axes, lateral axis, longitudinal axis, and vertical axis.

b. ***Gyroscope (GYR)***: "Gyroscope" refers the amount of rotation (rad/s) of a device by 3 axes, axis (pitch), axis (roll), and axis (yaw). If phone turns it permits the device to rotate the screen from portrait to landscape as well as use the device orientation.

3.4 Performance Evolution

False acceptance error (FAR), and false rejection error (FRR) are types of errors in user authentication. They are discussed in below section.

3.4.1. False Acceptance Rate (FAR)

It shows percentage of error of accepting a fake user consider as an authorized user. FAR notify about the authentication of the smartphone, if it is a safe authentication or not. FAR percentage is higher, if fake user's even intruders simply can login the authentication system.

FAR = (Number of wrong acceptances / Total number of intruder attempt made) * 100.

3.4.2. False Rejection Rate (FRR)

It shows the percentage of error of rejecting an authorized user as a fake user. FRR define about the originality of the system whether it is useful or not. If FRR percentage is higher, an individual can be failing in the authentication and has to re-login the authentication process every time till correct login

FRR = (Number of wrong rejections / Total number of genuine attempts made) ∗100

3.4.3. Equal Error Rate (EER)

EER shows a number of performance metric, it evaluate and compare the overall accuracy level from other biometrics authentication methods. EER acquire through finding the interception point of two graphs, first is FRR and the second is FAR.

ERR = (FRR + FAR) / 2

Table 3 EER comparison according of position of using smartphone

Matrics	User	Static	Walking	Moving in Car	Hand	Table	Sitting
HT, FP, TS, p, FA, FD, FS, AV, EC [18s]	20	2.50%	9.82%	3.99%	_	_	_
HT,FP,TS,p,FA,FD,FS,AV[18]	20	2.51%	10.20%	4.06%	_	_	–
FP,TS,P,FA,FD,FS,AV,EC[18]	20	2.62%	11.39%	4.39%	–	_	_
TS,P,FS[18]	20	2.66%	4.80%	5.83%	–	_	_
HT, UU, T, FP, TS, P, FA, FD, FS, AV, EC [18]	20	2.70%	8.58%	3.79%	–	_	_
HMOG, Tap, and Keystroke Dynamics[33]	100		7.16%	_	_	_	10.05%

4. Performance measure

Author has compared the performance in two aspects.

1. Table **2** compared the methods, features, FAR, FRR, EER and accuracy of keystroke dynamics on Smartphone. In Table 1 the Darren Cilia Frankie Inguanez [12] have useddigraph and trigraph feature with SVM structure with RBF Kernel function which gave best accuracy rate and EER is 99% and 1.42% in trigraph feature. If the same feature and classification used in digraph the accuracy rate decreased and EER is increased.

2. Second: In Table **1** comparing Equal Error Rate where users using Smartphone in different position such as standing, moving, on table, in car, seating. Author observed that if the user using the smartphone during walking the chances of getting error is high. For getting accurate result it is required to take the input when the user is in static position.

5. Conclusion

This paper is survey of keystroke dynamics on smartphone have done in last decade. Author compares the methods and features in terms of accuracy and EER used in smartphone. Author founds SVM structure with RBM Kernel function give best accuracy result and also compared the different positions of using smartphone. The chances of error during static position are very low rather than other positions.

In future work will use fusion like dwell time, flight time, figure pressure, figure size with different position of using smartphone to increase the accuracy rate.

Reference

[1] A. Buchoux and N. L. Clarke,(2008) “Deployment of keystroke analysis on a smartphone,”.
[2] Adnan Bin Amanat Ali, Vasaki Ponnusamy and Anbuselvan Sangodiah,(2019)“User Behaviour-Based Mobile Authentication System,” © Springer.
[3] Alifa Nurani Putri, Yudistira Dwi Wardhana Asnar and Saiful Akbar,(2016) “A Continuous Fusion Authentication for Android based on Keystroke Dynamics and Touch Gesture,”IEEE vol 978, ED -1, PP 5090-5671..
[4] Anthony, L., Brown, Q., Nias, J., Tate, B., & Mohan S.,(2012), “Interaction and recognition challenges in interpreting children's touch and gesture input on mobile devices,” ACM,pp. 225-234..
[5] Arwa Alsultan1 and Kevin Warwick,(2016) “Free-text keystroke dynamics authentication for Arabic language,” ISSN 2047-4938 doi: 10.1049/iet-bmt.2015.0101.
[6] Arwa Alsultan1 and Kevin Warwick2.,(2013) “A Survey of Free-text Methods,” vol. 10, Issue 4, No 1.
[7] Asma Salem, Dema Zaidan Andraws, and Swidan Ramzi Saifan,(2016) “Analysis of Strong Password Using Keystroke Dynamics Authentication in Touch Screen Devices,” IEEE vol 978, ED -1 pp 5090-2657-9/16.
[8] B. Draffin, J. Zhu, and J. Zhang,(2014) “Keysens: Passive user authentication through micro-behavior modeling of soft keyboard interaction,” vol. 130, pp. 184–201.
[9] C. Giuffrida, K. Majdanik, M. Conti, and H. Bos, (2014), "I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics".
[10] Chandrasekar Venko Vivekanandha and Krishna Sankar,(2014)“Biometric Authentication Based on Keystroke Dynamics for Realistic User”.
[11] Chang T-Y, Tsai C-J and Lin J-H, (2012) “A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices,” vol 85 ED-5, pp. 1157–65.
[12] Darren Cilia Frankie Inguanez, (2018), “Multi-Model authentication using keystroke dynamics for Smartphones,” IEEE vol 978, ED -1, pp. 5386-6095.
[13] E. Maiorana, P. Campisi, N. Gonzalez Carballo, and A. Neri, (2011), "Keystroke dynamics authentication for mobile phones," ACM.
[14] G. Forsen , M. Nelson and R. Staron.(1977) "Personal attributrs authentication techniques," Tech. Rep. RADC-TR-77-333.
[15] GP Perrucci, FHP Fitzek, Q Zhang and MD Katz, (2009) “Cooperative Mobile Web Browsin,”.
[16] Hiroya Takahashi,Kanayo Ogura,Bhed Bahadur Bista and Toyoo Takata, (2016) ”A user Authentication scheme using keystroke for smartphones while moving”.
[17] Jong-hyuk Roh, Sung-Hun Lee and Soohyung Kim,(2016),“ Keystroke dynamics for authentication in smartphone” vol 978 ED-1, pp. 5090-1325.
[18] Karatzouni S and Clarke N, “Keystroke analysis for thumb-based keyboards on mobile devices,” p. 253–63, 2007.
[19] Kyle R. Corpus, Ralph Joseph DL. Gonzales, Larry A. Vea and Alvin Scott Morada,(2016), “Mobile User Identification through Authentication using Keystroke Dynamics and Accelerometer Biometrics,” ACM vol 978 ED-1 pp. 4503-4178.
[20] Mageshwari. S, Kuppusamy.K.S. “Multimodal Authentication Approach for Visually Impaired in Smartphone Platforms”.

[21] Marlies Temper, Simon Tjoa, "The Applicability of Fuzzy Rough Classifier for Continuous Person Authentication".

[22] Matthias Trojahn, Florian Arndt and Frank Ortmeier, (2013), "Authentication with Keystroke Dynamics on Touchscreen Keypads - Effect of different N-Graph Combinations, ACM vol 978, ED-1 pp. 4503-4178.

[23] Mudhafar M Al-Jarrah, (2013), "Multi-factor authentication scheme using keystroke dynamics and two-part Passwords," DOI: 10.7813/2075-4124.2013/5-3/A.14.

[24] Mudhafar M. Al-Jarrah,(2012), "An Anomaly Detector for Keystroke Dynamics Based on Medians Vector Proximity," VOL. 3, NO. 6, June 2012 ISSN 2079-8407.

[25] N. Zheng, K. Bai, H. Huang, and H. Wang, (2014), "You are how you touch: User verification on smartphones via tapping behaviours".

[26] Noor Mahmood Al-Obaidi, Mudhafar M. Al-Jarrah, (2017), "Statistical Keystroke Dynamics System on Mobile Devices for Experimental Data Collection and User Authentication,"IEEE vol 978, ED-1, pp. 5090-5487.

[27] P. S. Teh, A. B. J. Teoh, C. Tee, and T. S. Ong, (2011) "A multiple layer fusion approach on keystroke dynamics," vol. 14, no. 1, pp. 23–36.

[28] Pin Shen Teh, Andrew Beng Jin Teoh and Shigang Yue1, (2013) "A Survey of Keystroke Dynamics Biometrics".

[29] Sung-Hoon Lee1, Jong-Hyuk Roh, Soohyung Kim, and Seung-Hun Jin,(2017),"A Study on Feature of Keystroke Dynamics for Improving Accuracy in Mobile Environment," pp. 366–375.

[30] T. Shimshon, R. Moskovitch, L. Rokach, and Y. Elovici. (2017), "Clustering di-graphs for continuously verifying users according to their typing patterns," pp. 445–449.

[31] Tanapat Anusas-amornkul, (2019), "Strengthening Password Authentication using Keystroke Dynamics and Smartphone Sensors," ACM ISBN 978-1-4503-7188.

[32] Tasia CJ, Chang TY, Cheng PC and Lin JH, (2014), "Two novel biometric features in keystroke dynamics authentication systems for touch screen devices".

[33] Zdeˇnka Sitov´ay, Jaroslav ˇSedˇenkay Qing Yangz, Ge Pengz, Gang Zhouz Paolo, Gastiy Kiran and S. Balaganiy, "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users".