DESIGN AN ALGORITHM FOR CONTINUOUS AUTHENTICATION ON SMARTPHONE THROUGH KEYSTROKE DYNAMICS AND TOUCH DYNAMICS

Pragya Vaishnav

PhD Scholar, AIIT,
Amity University, Jaipur, Rajasthan, India
pragya.vaishnav23@gmail.com

Manju Kaushik

Associate Professor, Dept. of
AIIT, Amity University, Jaipur, Rajasthan, India
mkaushik@jpr.amity.edu

Linesh Raja

Assistant Professor,
Dept. of Computer Application,
Manipal University, Jaipur, Rajasthan, India
lineshraja@gmail.com

Abstract:

In today's world smartphone has turned more into a necessity rather than an accessory. It has become our personal assistant due to all the applications of smartphone. Mobile security is the main concern of every smartphone users as everyone do all kind of transactions through smartphone, keeps the confidential data in their mobile. Password authentication is no more trustworthy authentication process, password can be steal through finger oil or shoulder surfing. Continuous authentication is an authentication technology to confirm the identity of the user throughout the session. Keystroke and touch dynamics is behavioral biometric authentication which verify the identity of the user using their typing and touch behavior on the smart devices. In this study author proposed KDSmart system for all the smart devices to enhance the authentication process. FAR 1.66%, FRR 6.73% and EER 4.1% achieved to confirm the authenticity of KDSmart system.

Keywords: Keystroke Dynamics, Touch Dynamics, KDSmart system, FAR, FRR, EER

1. Introduction

The importance of smart phones in human's daily life is undeniably everlasting. This is because there is on growing enormous transformation in the smart phones are no longer the ordinary communication device it used to be. It has become the colossal point of interest for individuals and businesses alike, 91% people says that their smartphone is very important and for 60% it is even more important than coffee [13] because smart phones offers courtesy of the various incredible features and opportunities through mobile applications and its services. Everyone used to do all their financial transection (banking, purchasing and all kind of payments), keeps personal data, use social media and even keeps their password file as well in their mobile. Now the time is where everyone is fully occupied and dependent on all these apps, and cannot imagine their life without these apps. Chart 1 shows the percentage of using mobile apps in their smartphone.

In this paper chart 1 represented real image of today's world. In smartphone keypad lock and password is very common solution to protect the mobile's data and these are less secured authentication methods, it cannot protect user's personal data and files as password and keypad lock is easy to crack by hackers and anyone can steal it through finger oil and shoulder surfing [20].

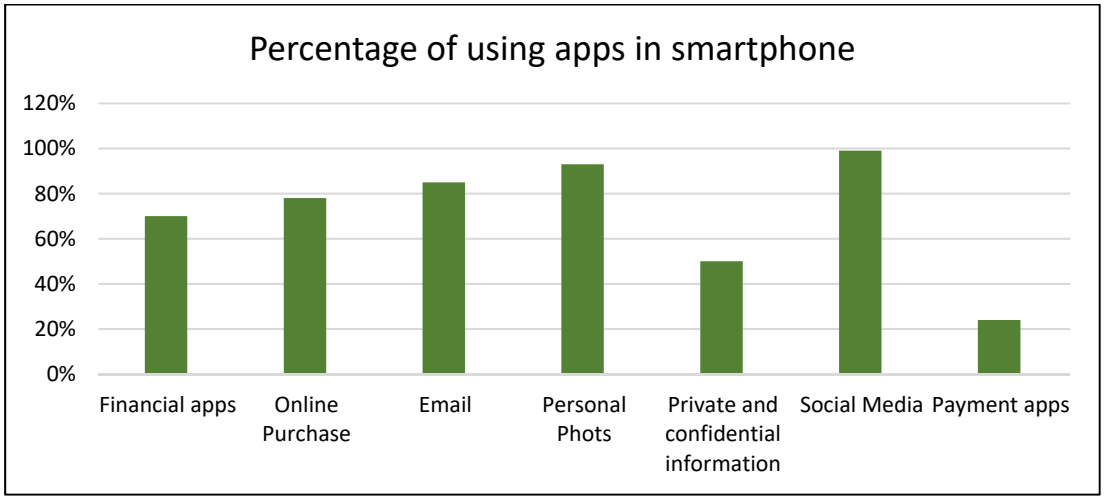

Chart 1 Percentage of using mobile apps in smartphone

Hence password authentication is no more secure method [25]. Therefore every individual are on risk as their personal and sensitive data are stored and can be accessed by unauthorised persons through stealing or accidental loss of a smartphone can reveal any professional and personal information kept on smartphone Chart 2 shows the probability of percentage of the unauthorized data access by theft if smartphone lost.

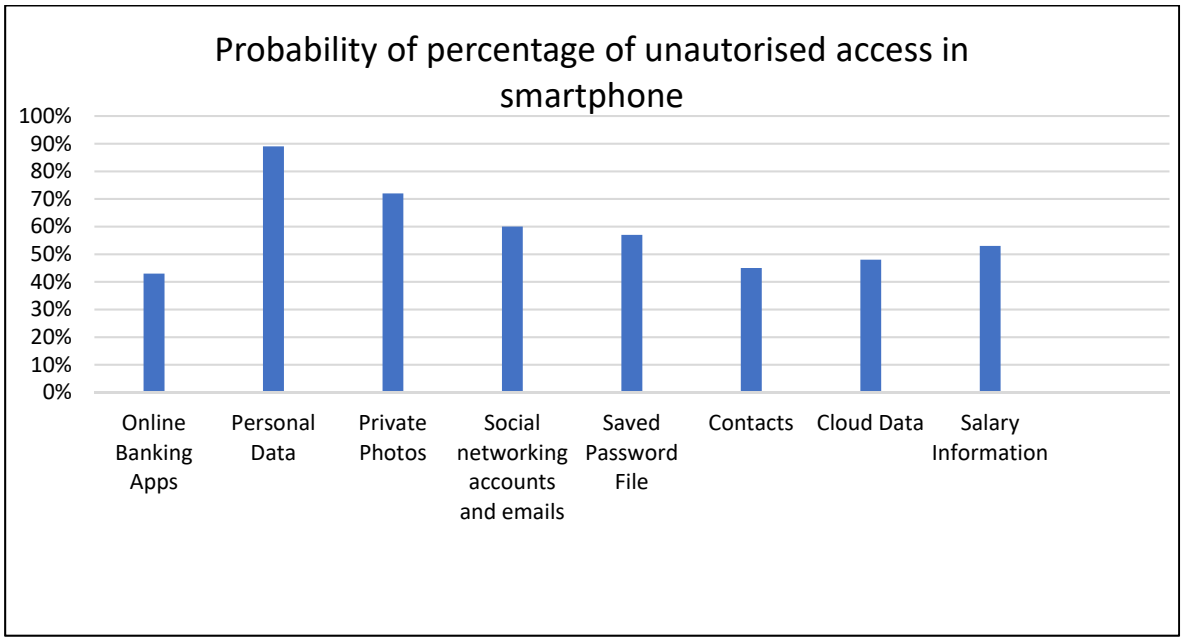

Chart 2 the probability of percentage of the unauthorized data access on smartphone

Continuous authentication is a great solution and it is require to monitoring the user throughout the session. It is advance mechanism to enhance the security of smartphone because it keeps eye on users even after login the application.

Keystroke Dynamics and Touch Dynamics is a behavioural based biometric authentication technology which confirms the identity of the user through their typing and touch behaviour on the smartphone. Author proposed KDSmart system to improve authentication method in smart devices. In KDSmart system keystroke dynamics method used for login the application and for continuous authentication touch dynamics method implemented. In this paper author collected 208 participants data for FAR, FRR and EER analysis and for checking the validity of

the system pared t-test applied, 600 data captured from 200 participants in three times for result analysis in section 3. Author designed an algorithm to improvise the authentication process using keystroke dynamics and touch dynamics section 3.4.

2. Related Works

Keystroke dynamics and touch dynamics research has been grown in the last decade in a scientific discipline where system and models are examined through public samples, and experimental outputs are echoed by all. Tanapat Anusas-amornkul proposed 3 classification methods, i.e. k Nearest Neighbors (KNN), Random Forest, and Naïve Bayes, used as data categorization and they used 10-fold cross validation for validate the data and evaluating the percentage of accuracy and EER is comparing the classification techniques[28].

According to Kyle R. Corpus Naïve Bayes provides the worst performance and for time based feature Random Forest classification provides the best performance. It gives 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. 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 [20].

Arwa Alsultan 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 this authentication system continuously runs. On FRR modality experiment, continuous fusion authentication, performance test more gives accurate rather than FAR[2].

B. Draffin, J. Zhu, KeySens is a structure which is used for micro-behaviour, without any related data of the entered text. It find out the specific position of touched of every key, length of the key down, the pressure of the touch or the location to identify user even of figure press. To recognize an unauthorized user, Author needs 5 key downs with a 32.3% of FAR and a 4.6% of FRR, after 15 key down with a 14% value of FAR and a 2% value of FRR [5].

Jong-hyuk Roh 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 [15].

Marlies Temper 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, Zdeˇnka Sitov´ay Jaroslav ˇSedˇenkay Qing Yangz introduced HMOG, 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 sections data which were captured through 100 users in the form of two motion positions i.e., sitting position and walking position. 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, tapping and keystroke dynamic features. Here author received 7.16% from walking and 10.05% from sitting. Their outputs shows that HMOG is 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 output with 15.1% EEE and, the energy overhead of dataset collection and feature extraction was very 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 [29].

Chandrasekar Venko Vivekanandha proposed a method for authentication on Smartphone which will take user's finger print, login details and login on the basis of the biometric rules for password typing. Author had three stages and two steps. The stages are 1. Fingerprint 2. Login details like username and password, 3. Keystroke dynamics. Two steps are 1. Enrolment Time (Training Time), 2. Verification Time. They are providing the extra level security Based on this approach [11].

Darren Cilia Frankie Inguanez. is using 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, Sung-Hoon Lee1 analyzed sensor based attribute. They got the Up Up (UU) feature to arrange each individual user they used timing features set and the statistical 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 statistical features from the sensor based features. [27].

Mudhafar M. Al-Jarrah 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% [22].

Arwa Alsultan1 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. [3].

For Android Smartphone touch screen devices Asma Salem 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 set like time duration, size, finger pressure and area of each 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 [4].

According to G. Forsen 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 saprated through the way of typing by their names[16].

Zheng et al. measured the user's tapping behaviours on Smartphone's touch screen by using four features like size, acceleration and time. Through the data of 4 digit and 8 digit PINs both, they calculated the outcome of the system by using all the experiments. Giuffrida et al [30].

Buchoux et al. They used for terms of PIN and the second was keystroke measurement on the time of sign in process. They captured key events and inter-key latencies for further evaluation. Author used 20 subjects group to calculate the implementation. According to author statistical classifiers approach is applicable for Smartphone's, but a 4-digit PIN is very less to get appropriate output [1].

Research has done in last decade on keystroke dynamics were based on timing and touch features of smartphone. Authors defined different positions of using smartphone and calculated FAR, FRR and EER based on different positions. In this research author use *pared t*-test to check the genuine user and fake user identity. Author implemented continuous authentication for smartphone to check the identity of the logged in user after login the application. Author captured 600 data from 200 users in three times to get accurate result in result analysis.

3. Proposed KDSmart System

3.1 Background

The proposed KDSmart (keystroke dynamics smart) System are applicable for all the android based devices (Smartphone and Tablets). This system provides the security to all the applications where user perform their financial transaction, store their private data and do other confidential work on mobile application as well. This system has three phases: Registration phase, Login phase and Final Testing Phase.

Registration Phase capture all the keystrokes and touch data and store that data in MYSQL database on server, author used base64 sha1 for encrypt the password and unique id.

Login phase compares the login keystroke data with registered keystroke data and if data comes under the pass-value then user can login the application.

Final Testing phase compares the touch data with the registered touch data throughout the session even after successfully login the application, if user's touch data does not match with registered touch data and not comes under pass-value then current screen will be shut down and display home screen, therefor user will not be able to do any activities on application.

Author received keystroke data and touch data on server of 200 subjects therefore data are secured on server, there is no way for user to do any changes in application as data are encrypted. Fig. 1 presenting how KDSmart system is working. The system identify the identity of the user throughout the session even after login the application by using keystrokes and touch data to check whether user is genuine or impostor.

3.2 Feature Selection in KDSmart System

All previous keystroke dynamics research are based on hard keyboard (desktop and laptop keyboard), and research has not done on continuous authentication (throughout the session) yet, all that study was only comparative studies. Sensors on smartphone helps to read all the additional features like flight time, dwell time, typing speed, typing error rate, finger pressure and finger size and it can be measured. In this research, author is using timing feature and touch feature as well as typing speed and error rate. Author is using encryption to secure the data. These feature set elements are explained as here:

- Typing Speed: - Total typing speed.
- Flight Time: - Time duration between two sequential keys on touch events.
- Dwell Time: - Time duration between key release and key press with the same key.
- Error Rate: - Counting wrong key press, delete key press and backspace key press.
- Finger Size: -Value of finger size on touch screen.
- Encryption: - Unique id and password are stored in base64 sha1 encryption form.

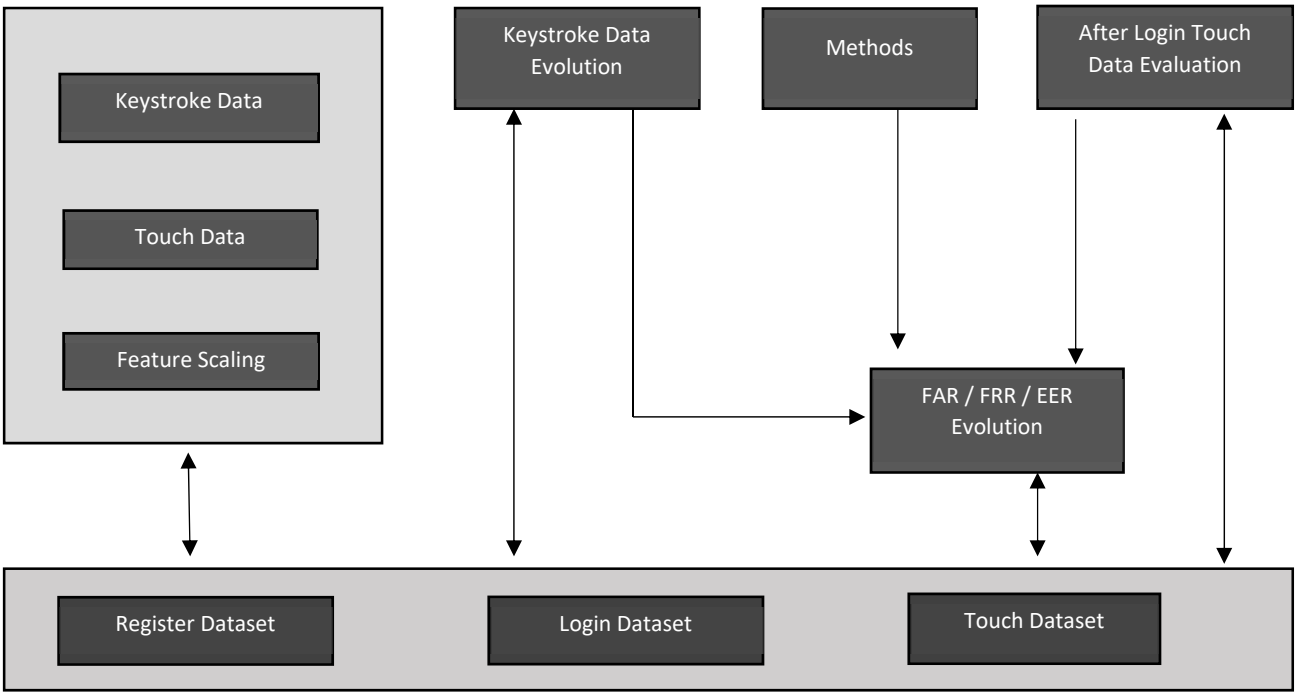

Fig. 1 Working of KDSmart system

3.3 Phases of KDSmart System

A. Registration Phase

KDSmart system provides a registration module to register the data. For registration phase 200 keystroke data and touch data are collected. The collected data records are stored in MySQL database on server and generated id and unique id for every user. base64 sha 1 is used to encrypt the unique id and password. In this phase user's name, email-id and password are entered and typing speed, flight time are calculated.
To measure typing speed author collected system's current time at the both end. When user start the typing and end the typing.

Start_time = SystemCurrentTime
End_time = SystemCurrentTime
Typing_speed = (End_time – Start_time)/1000

To calculate Flight time author collected current time of every pressed key and counted the time difference of both the key pressed and this time difference has stored. Hence author collected time difference of every pressed key. K represent the key and N represent the place number of key in word and counted the time difference of both the key pressed in words.

$$resN = (kN+1 - kN) / 1000$$
$$Flight\ Time = resN + resN+1 + \ldots..resN$$

After registering keystroke data, touch data are collected. In this study touch data are used for continuous authentication in KDSmart system. Dwell time and finger size are collected from 200 participants. To calculate Dwell time, time of action up and action down are captured and subtract both the time. To calculate finger size on screen getTouch() are used.

B. Login Phase: -

In the login phase, through user's login email-id and password the stored and save data of the user is retrieved from the database. It compares login keystroke data with registered keystroke data on server. If keystroke login data comes under the pass-value then user is able to login the system. In this research 208 user attempted the login phase module. This comparison determines the user is genuine or an impostor.

For login, user's email-id and password are required. If login email-id and password are matched and user's typing speed, flight time and error rate are calculated and compared with the registered keystroke data on server. Error rate is calculated through their typing error if user enter backspace, delete key presses or enter wrong key then it counts by one value. This KDSmart system are used further for statistical error metrics analysis (ERR, FAR, FRR).

C. Final Testing Phase : -

This is final phase for continuous authentication of KDSmart system. This module start to monitoring the user after successfully login the application till end of the session as user is not imposter. It keeps eye on every touch activity of user and compare the touch data with registered touch data continuously. If touch data not matched with registered data and it does not comes under the pass-value then immediately session will get close and user will not be able to do any activities on application as user will be considered as imposter and home screen get appeared.

3.4 Design of Algorithm

Registration Phase Algorithm

1. Capture Name, Email and Password

2. If TypingSpeed.length equals 1
   set Registration_starttime as SystemCurrentTimeMillis()
   End
   If TypingSpeed equals sample_text
   set Registration_endtime as System.currentTimeMillis()
   End
   Calculate Registration_Typing_Speed

3. Capture fixed text
   while i not equal to key_data.length
   set time as System.currentTimeMillis()
   set array[i] as time
   init i
   set varNo as array[No]
   calculate result_No = (varNo+1 - varNo) / 1000
   calculate Registration_FlightTime = result_No + result_No+1 + …..result_No

Login Phase Algorithm

1. Capture Email and Password

2. If TypingSpeed.length equal 1
   set Login_starttime as SystemCurrentTimeMillis()
   End
   If TypingSpeed equals sample_text
   set Login_endtime as System.currentTimeMillis()
   End
   Calculate Login_Typing_Speed

3. Capture fixed text
   set key_data as fixed text
   while i not equal key_data
   set time as System.currentTimeMillis()
   set array[i] as time
   init i
   set varNo as array[No]
   calculate Res_No = (varNo+1 - varNo) /
   1000
   calculate Login_FlightTime = Res_No + Res_No+1 + …..Res_No

4. Capture fixed characters
   set i1 as 1
   set a as 0
   set p as fixed characters
   calculate Result
   if a les than equal 10
   if Result equals myArray[a]

   else
   calculate count
   End
   calculate a
   else
   message “Enter correct entry”
   End

Final Phase Algorithm

1. Captured finger touch
   Apply getTouchMajor()
2. Captured touch time
   Res1 = ACTION_UP
   Res2 = AXIS_PRESSURE
   Result_dwell = Res1– Res2

User Identification Algorithm

```
Typing_speed_result = Login_Typing_Speed - Registration_Typing_speed
Flight_time_result = Login_FlightTime - Registration_FlightTime
If Typing_speed_result less than 3.5 && Flight_time_result less than 1.5 && count less than 3
        Message “login successful”
else
        Message “Login Fail”
End
```

4. Result and Analysis

4.1 Data Collection:

In this research, author received keystroke and touch data from 200 subjects in database on server. The collected data consisted of 208 features subsets (Typing speed, Flight Time, Dwell Time, Finger size, Error Rate). The keystroke and touch data were captured in three phase for each participants, the first phase was for registration, it consisted 200 typing attempts, the second phase was login for true user testing it consisted 200 typing attempts and in third phase where we collected 600 attempts from 200 subjects (three attempts from each subject) for both keystroke and touch data to implement *pared t*-test. For FAR, FRR and ERR author collected 180 attempts from 60 subjects (three attempts from each subjects). For using this KDSmart system, author provided a demo to familiarize the app, therefore chances of making error during typing would be less.

4.2 Pared t – test:

A paired t-test is used to calculate difference between two variables for the same subject. Generally the two variables are separated by time. We can use this test when our data values are paired measurements. Hence, we might have before-and-after measurements for a group of people.
There are two types of hypotheses for a sample *pared t*-test, the null hypothesis and the alternative hypothesis. In this study author applied alternative hypothesis and it is defined below:-

- The upper-tailed alternative hypothesis (H1) assumes that the true mean (μ) of the sample is greater than the comparison value (m0).
- The lower-tailed alternative hypothesis (H1) assumes that the true mean (μ) of the sample is less than the comparison value (m0).

The mathematical representations of the null and alternative hypotheses are defined below:

- H1: $\mu > m0$ (upper-tailed)
- H1: $\mu < m0$ (lower-tailed)

In this study author are comparing the variables (Registered data and Login data) means measuring the difference between both the variable to check is there any difference of typing pattern and touch pattern in registration time and login time and to confirm that KDSmart system is working accurately or not and to check the identity of the users.

These *pared t*-test applied on Typing speed, Flight Time and Dwell time. For *pared t*-test author collected data from 200 user in three times at login time for getting accurate results and calculate
average of three attempts and these average compared with the registered data using *pared t*-test in SPSS software. Result of these *pared t*-test on Typing speed, Flight Time and Dwell time are given below.

4.2.1 Pared T - test on Authorized Users

Test on Typing Speed

Name of Variable 1	Name of Variable 2	Null Hypothesis	P Value Received
Key_Speed	Average	There is no significance difference between Key_Speed and Average	0.226

Interpretation:- Since p value is greater than 0.05, it can be inferred that there is no significance difference between Key_Speed (Typing speed) and Average value of three attempts of typing speed in login time.

Test on Flight Time

Name of Variable 1	Name of Variable 2	Null Hypothesis	P Value Received
Key_Flight	Average	There is no significance difference between Key_Flight and Average	0.312

Interpretation: - Since p value is greater than 0.05, it can be inferred that there is no significance difference between Key_Flight (flight time) and Average value of three attempts of flight time in login time.

Test on Dwell Time

Name of Variable 1	Name of Variable 2	Null Hypothesis	P Value Received
R_Touch_size	Average	There is no significance difference between R_Touch_size and Average	0.586

Interpretation :- Since p value is greater than 0.05, it can be inferred that there is no significance difference between R_Touch_size and Average value of three attempts of dwell time in login time.

4.2.2 Pared T - test on unauthorized users

This test applied for confirmation authenticity of KDSmart system. Author provided correct email-id and password to the fake user to check if they are able to login the application or not. So author collected 180 samples of 60 users (three times attempt of each user). Test applied on typing speed and flight time. The test got the significant difference between registered data and login data.

Test on typing speed for fake users

Name of Variable 1	Name of Variable 2	Null Hypothesis	P Value Received
Registrati-on_Speed	Average	There is significance difference between Registratio-n_Speed and Average	0.025

Interpretation: - Since p value is less than 0.05, it can be inferred that there is a significance difference between Registration_Speed and Average value of three attempts of typing speed on login time.

Test on Flight Time for fake users

Name of Variable 1	Name of Variable 2	Null Hypothesis	P Value Received
Register_Flight_Time	Averagege	There is significance difference between Register_Flight_Time and Average	0.001

Interpretation: - Since p value is less than 0.05, it can be inferred that there is a significance difference between Register_Flight_Time and Average value of three attempts of flight time in login time.

4.2.3 Result of Pared T - test: -

Pared t-test applied on KDSmart system to check the authenticity of the system which is developed to enhance the security of smartphone. This test proved

that this system is perfectly able to find the identity of genuine user and intruders. This test applied on genuine users and fake users both.

- Test applied on genuine user's data (Keystroke data and Touch data) and these test did not get any significant difference between registered data and login data. Hence it proves the data has collected during login time is the data of the genuine users.
- Test applied on fake users also, to give them genuine users email id and password to check the validity of the system. The test got differences between registered data and login data. Therefore it makes system accurate that fake user cannot login the application if their keystroke data is not match with registered data.

It also determine that keystroke pattern and touch patterns are unique, no one can copy or steal typing and touch pattern of the users. This test proved that the algorithm which is designed to develop this system is perfectly working with full efficiency.

4.3. FAR and FRR Analysis

The KDSmart system is achieved FAR and FRR value through the pass-value for each user to get the system's performance. FAR and FRR applied on both the phases login phase and final phase. Table 1 shows the analysis of FRR where 208 user has tried to login the application and use the application and it shows that how many authenticate users were rejected as a fake user and Table 2 shows the analysis of FAR to check validity of the KDSmart system that how many fake users were accepted as a genuine users. This FAR method applied on both the phases login phase and final testing phase.

No Of User	FRR
208	6.73%

Table 1: FRR analysis

No Of User	FAR
60	1.66%

Table 2: FAR analysis

EER Analysis

The dataset is analyzed using the FAR and FRR which calculates the EER value, where the pass-value is variable, i.e. it is determined separately for each subject (Typing Speed, Flight Time, Dwell time, touch size and Error Rate). The analysis is done on timing feature data only. The EER results in Table 3 shows the EER value.

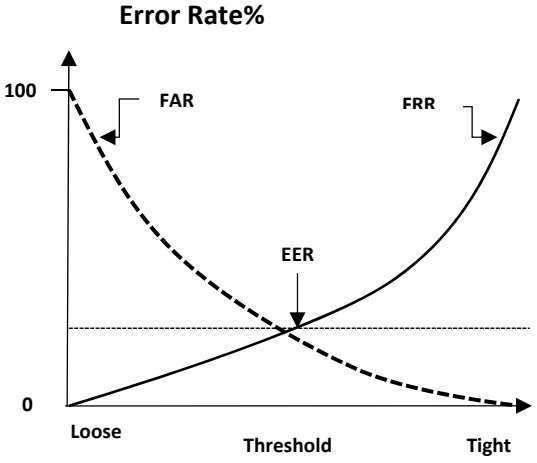

Fig. 1 Equal error rate

FAR	FRR	EER
60 Users	208 Users	4.1%

Table 3: EER Analysis

4.3.1 Result of FRR, FAR and EER

FRR result is 6.73% and FAR is 1.66%. The percentage of FRR and FRR determines system's performance. If FRR percentage is high then it can be consider but if FAR percentage is high then it cannot be consider because it is dangerous for the system. EER is 4.1% which shows the accuracy of the system. Therefore it confirms that KDSmart system accuracy is high and it is appropriate for authentication system in smartphone.

5 Conclusion

Author proposed KDSmart system, it has been developed to use continuous authentication through keystroke dynamics and touch dynamics for smart devices. This system developed to make strong authentication process and secure mobile data. Both the technology keystroke dynamics and touch dynamics used in KDSmart system, are very secure, efficient and trustworthy. Author designed an algorithm to improvise the authentication process, this algorithm can be apply in any android based application. Author implemented *Pared T test* for result analysis to check the KDSmart system authenticity and FAR, FRR and EER method also applied to check the validity of the system. Test results proved that designed algorithm is working efficiently KDSmart system is capable to identify the identity of the genuine user and intruders because FAR result was 1.6% and after login the application user can be identified through their touch behavior on smartphone.

References

[1] A. Buchoux and N. L. Clarke,(2008) "Deployment of keystroke analysis on a smartphone," in Australian Information Security Management Conference.
[2] Arwa Alsultan1 and Kevin Warwick2. (2013) "A Survey of Free-text Methods", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 1, July.
[3] Arwa Alsultan1, Kevin Warwick2. (2016) "Free-text keystroke dynamics authentication for Arabic language", 1School of Systems Engineering, University of Reading, Reading RG6 6AH, UK 2Vice Chancellors Office, Coventry University, Priory Street, Coventry CV1 5FB, UK. ISSN 2047-4938 Received on 29th October 2015 Revised on 11th January 2016 Accepted on 8th February doi: 10.1049/iet-bmt.2015.0101.
[4] Asma Salem Dema Zaidan Andraws Swidan Ramzi Saifan. (2016) " Analysis of Strong Password Using Keystroke Dynamics Authentication in Touch Screen Devices", Amman, Jordan , Cybersecurity and Cyberforensics Conference.
[5] B. Draffin, J. Zhu, and J. Zhang, (2014) "Keysens: Passive user authentication through micro-behavior modeling of soft keyboard interaction," in Mobile Computing, Applications, and Services, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer International Publishing, vol. 130, pp. 184–201.
[6] G. Forsen , M. Nelson and R. Staron. "Personal attributrs authentication techniques," Tech. Rep. RADC-TR-77-333, Rome Air Development Center.
[7] Bhawna Mathur, Manju Kaushik, (2018), "Data Analysis utilizing principal component analysis", , paper published in International journal of engineering research and technology. (ISSN 0974-3154). Vol. 11, Number 2, pp. 333-348 (Scopus Indexed)
[8] Bhawna Mathur, Manju Kaushik, " Comparing different classification techniques using Data mining tools", in intenational Journal of Management, IT & Engineering , (IJMIE), ISSN: 2249-0558, Volume8, Issue 9, pp273-284.
[9] Bhawna Mathur, Manju Kaushik, (2018), "Data Analysis utilizing principal component analysis", paper published in International journal of engineering research and technology. (ISSN 0974-3154). Vol. 11, Number 2, pp. 333-348 (Scopus Indexed).
[10] Bhawna Mathur, Manju Kaushik, "Empirical Analysis of Metrics Using UML Class Diagram", International Journal of Advanced Computer Science and Applications, 7(5), 2016. 10.14569/IJACSA.2016.070506.
[11] Chandrasekar Venko Vivekanandha Educational Institutions, Krishna Sankar P 3Edge Solutions, "Biometric Authentication Based on Keystroke Dynamics for Realistic User" Chennai See discussions, stats.
[12] Darren Cilia Frankie Inguanez. (2014) "Multi-Model authentication using keystroke dynamics for Smartphones", Information and Communication Technology Institute, University College, Malta College of Arts, Science and Technology Corradino Hill, Paola PLA 9032, Malta.
[13] https://saucelabs.com/blog/how-smartphones- and-mobile-internet-have-changed-our- lives
[14] Jain M., Kaushik, M. and Kumar, G. (2015) "Reliability Analysis for Embedded System with Two Types of Faults and Common Cause Failure Using Markov process", Published in Proceeding of the International Conference on Computer and Communication technology, ACM New York USA, pp. 271-275.
[15] Jong-hyuk Roh, Sung-Hun Lee, Soohyung Kim "Keystroke dynamics for authentication in smartphone" Cyber Security Research Division ETRI Daejeon, KOREA.
[16] Kaushik M., Kumar G., Preeti, Sharma R. (2015) "Availability Analysis for Embedded System with N-version Programming using Fuzzy Approach", Published in International Journal of Software Engineering, Technology and Applications. Vol.1, No.1, pp 90-101. (UGC Journal).
[17] Kaushik, M. and Kumar, G. (2015) "Markovian Reliability Analysis for Software using Error Generation and Imperfect Debugging", Published in Proceeding of the International Multi Conference of Engineers and Computer Scientists 2015, vol. 1, pp. 507-510.

[18] Kumar G., Kaushik M. and Purohit R. (2018) "Reliability Analysis of Software with Three Types of Errors and Imperfect Debugging using Markov Model" , Published in International Journal of Computer Applications in Technology, Vol 58, No. 3, pp. 241-249. (Scopus).
[19] Kumar G., Kaushik M., Preeti (2016) "Maintenance Policies for Improving the Availability of a Software- Hardware System", Published in proceedings of the "11th International Conference on Reliability, Maintainability and Safety", ISBN: 978-1-5090-2714-9, pp. 1-5. IEEE xplore,DOI: 10.1109/ICRMS.2016.8050058, (Available online: 28 September 2017). (Scopus Indexed)
[20] Kyle R. Corpus, Ralph Joseph DL. Gonzales,Larry A. Vea, Alvin Scott Morada. (2016) "Mobile User Identification through Authentication using Keystroke Dynamics and Accelerometer Biometrics" IEEE/ACM International Conference on Mobile Software Engineering and Systems.
[21] Marlies Temper, Simon Tjoa "The Applicability of Fuzzy Rough Classifier for Continuous Person Authentication" St. P¨olten University of Applied Sciences St. P¨olten, Austria.
[22] Mudhafar M. Al-Jarrah. (2012) "An Anomaly Detector for Keystroke Dynamics Based on Medians Vector Proximity", Department of Computer Information Systems Faculty of Information Technology, Middle East University, Amman, Jordan. VOL. 3, NO. 6, June ISSN 2079-8407 Journal of Emerging Trends in Computing and Information Sciences ©2009-2012 CIS Journal. All rights reserved. http://www.cisjournal.org 988.
[23] Nareerat Benjapatanamongkol; Pattarasinee Bhattarakosol, (2019) " A Preliminary Study of Finger Area and Keystroke Dynamics Using Numeric Keypad With Random Numbers on Android Phones", Conference: 2019 23rd International Computer Science and Engineering Conference (ICSEC) Phuket, Thailand, 30 Oct.-1 Nov. 2019, DOI**:** 10.1109/ICSEC47112.2019.8974686 ,
[24] N. Zheng, K. Bai, H. Huang, and H. Wang, (2014) "You are how you touch: User verification on smartphones via tapping behaviors", IEEE 22nd International Conference on Network Protocols.
[25] Pragya Vaishnav1, ManjuKaushik2 and Linesh Raja3, (2021), "Survey on Smartphone Securities", IOP Conf. Series: Materials Science and Engineering 1099 012067 IOP Publishing, doi:10.1088/1757-899X/1099/1/012067
[26] Sharma, R., Kaushik, M. and Kumar, G. (2015) "Reliability analysis of an embedded system with multiple vacations and standby", Published in International Journal of Reliability and Applications, Vol. 16, No. 1, pp. 35-53, 2015
[27] Sung-Hoon Lee1, Jong-Hyuk Roh2, Soohyung Kim2, and Seung-Hun Jin2. " A Study on Feature of Keystroke Dynamics for Improving Accuracy in Mobile Environment", 1 Informaion Security Engineering, University of Science and Technology, 217 Gajeong-ro, Yuseong-gu, Daejeon 34113, Korea.
[28] Tanapat Anusas-amornkul. (2000) "Strengthening Password Authentication using Keystroke Dynamics and Smartphone Sensors"
[29] Zde˘nka Sitov´ay Jaroslav ˇSed˘enkay Qing Yangz* Ge Pengz Gang Zhouz Paolo Gastiy Kiran S. Balaganiy["HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users" yNew York Institute of Technology.
[30] Zheng, K. Bai, H. Huang, and H. Wang, (2014) "You are how you touch: User verification on smartphones via tapping behaviors", IEEE 22nd International Conference on Network Protocols.

Authors Profile

Name: Ms. Pragya Vaishnav
Pragya Vaishnav is PhD Scholar in Amity University Jaipur, Rajasthan, completed MSC in Information Technology from Makhanlal Chaturvedi University Bhopal, Madhya Pradesh. Currently working as an Assistant Professor in Nagindas Khandwala College, Mumbai, Maharastra. She has more than 11 years of experience in teaching. She has published papers in the field of smartphone securities National and International Journals.

Name: Dr. Manju Kaushik
Dr. Manju Kaushik is an Associate Professor, Head Amity Innovation Incubator Centre, E-Cell, IEEE & ACM Branch Counsellor and Coordinator Technical Clubs – Amit University Rajasthan. She was awarded Ph.D. from the Mohan Lal Sukhadia, Udaipur. Her research papers have been published in various journals and conferences of National and International repute like IEEE, Springer, Elsvier and other SCI, Scopus indexed. She is an active reviewer of different indexed journals. Presently she is the executive member of Rajasthan sub-section of IEEE & Member of ACM, life member of ISTE and CSI. She is editor of Scopus index JCIT
Journal (IGI Globe). She has published 02 Patents. She is editor of 02 Books .

Name: Dr. Linesh Raja
Linesh Raja is currently working as Assistant Professor at Manipal University Jaipur, Rajasthan, India. He earned a Ph.D. in computer science in the year 2015. Before that, he has completed his Master's and Bachelor's degrees from Birla Institute of Technology, India. Dr. Linesh has published several research papers in the field of wireless communication, mobile network security, and the internet of things in various reputed national and international journals. He is recently appointed as managing editor of the Taru Journal of Sustainable Technologies and Communication. He has edited the Handbook of Research on Smart Farming Technologies for Sustainable Development, IGI Global. At the same time, he is also acting as a guest editor of the various reputed journal publishing houses, such as Taylor and Francis, Inderscience, and founder member of the ACM Jaipur chapter.