**Smartphone Authentication using Soft Biometrics**

By Radhika Bailurkar (2019430003)

Faculty Incharge: Prof. Nataasha Raul

INTRODUCTION

Today, smartphones are being used widely in professional as well as personal life. These devices contain almost every data required for our daily life. The increasing use of access to sensitive and privacy data has given rise to the need of secure authentication techniques. To prevent unauthorized use of their mobile phones, most users typically rely on a feature that allows them to “lock” their smartphones using PINs, swipe patterns or passwords. These popular authentication mechanisms are susceptible to guessing, spoofing and side channel attacks such as smudge. Additionally, a fundamental limitation of PINs, passwords, and fingerprint scans is that they are well suited for one-time authentication, and therefore are commonly used to authenticate users at login. This renders them ineffective when the smartphone is accessed by an adversary after login. Continuous or active authentication addresses these challenges by frequently and unobtrusively authenticating the user via behavioral biometric signals, such as touchscreen interactions, hand movements and gait, voice and phone location. Let us look at biometrics for authentication.

BASICS OF BIOMETRICS

Biometric is the scientific field of study related to human characteristics. Biometric characteristics are unique, personal characteristics that can be used to establish a person’s identity. Unlike pass cards, keys and passwords, for example, the physical characteristics that can be used for biometric solutions cannot be transferred, or cannot be transferred easily, from one person to another. They are also not susceptible to fraud like photos and signatures. It is impossible for them to be removed. Biometrics can be classified below as:

* **Physical Biometrics**

Physical Biometrics focuses upon examining the biological and the physiological features of the human being.  These unique features include the shape of the hand, finger, and face, and the structure of the eye.

1. Hand geometry: The actual shape and dimensions of your hand are sometimes used for access control and time-and-attendance operations in the workplace. However, they are not as unique as fingerprints, so aren’t viable in high-security applications.

### Finger vein patterns: Fingerprints, while totally unique, can be at risk of being copied. A similar but more advanced technique looks instead at the veins underneath the fingerprint, which are virtually impossible to copy.

### The eye: The unique and complex characteristics of the iris or the retina of your eye can also be used for biometric ID. Eye biometrics are commonly used for automated passport controls and national ID programmes, and are also now starting to appear in smartphones, such as the Samsung Galaxy S8.

### Face shape: Analyzing the shape of your face, as well as its specific features (e.g. distance between the eyes or the height of your ears), is used in CCTV security systems, but can also be used as a commercial identification and marketing tool. With the huge and enduring popularity of selfies, it’s something that we may see more of in low-security smartphone apps.

* **Behavioral Biometrics**

Behavioral Biometrics focuses upon examining the non-biological or the non-physiological features of the human being.  This realm of Biometrics studies the unique, psychological aspects of humans.  This is the way we type on the computer keyboard, the way we sign our name, even the way we walk.

1. Signature dynamics: This takes it beyond just what your signature looks like, and instead looks at how you sign. It includes analysis of the direction and pressure of your pen stroke, and combines it with the overall shape of the signature to verify your ID.

### Voice: The unique patterns in your voice can be analyzed and compared to an example voiceprint to confirm your ID. This is already used to access some online banking services and automated customer service phonelines.

### Keystroke dynamics: As well as how you write with a pen, biometric data can also come from the manner and rhythm in which you type on a keyboard.

### Gait: Gait analysis looks at the unique way you walk, which is determined by a set of personal characteristics including your age, height and weight. Special cameras can be set up to analyze people’s walking style and identify them.

### Gestures: Other physical human gestures, usually from the face or hands, can also be used to identify you. Some smartphones today use facial or smile recognition to control unlocking the device.

### Soft Biometrics

Soft biometrics provide ancillary information but are not fully distinctive and permanent, so these features cannot provide a reliable person recognition. However, such ancillary information still can be used as a secondary information to complement the primary biometric traits (face, iris, etc.), and these features can be classified to physique (e.g., color skin, gender, ethnic origin), clothing (e.g., clothes’ color), or accessories (e.g., glasses, hat).

These soft biometrics can be used to study the continuous authentication of the smart phone users. In this paper, we lay foundational work for continuous authentication schemes that rely on touchscreen input as a datasource. We investigate if it is possible to authenticate users while they perform basic navigation steps on a touchscreen device and without any dedicated and explicit security action that requires attention from the user. Our goal is to analyze how robustly such schemes operate and if they are sufficiently reliable to be used on commodity devices.

LITERATURE SURVEY

Table: Literature Review

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sr No | Year | Title of Paper | Author | Content |
| 1 | 2013 | Unobservable Reauthentication for Smartphones | L Li,X Zhao and G Xue | Gesture Movements |
| 2 | 2012 | Exploring touch-screen biometrics for user identification on smart phones | J. Angulo and E. W’astlund | Lock Pattern Dynamics |
| 3 | 2011 | Implicit Authentication through Learning User Behavior | E Shi,Y Niu, M Jakobson and R Chow | Behavior Patterns |
| 4 | 2014 | Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones | H Xu, Y Zhou and M Lyu | Touch Gesture Evaluation |
| 5 | 2013 | Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication | M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song | Learning the touch behaviour of User |
| 6 | 2015 | Biometric authentication based on touchscreen swipe patterns | M Antal and L Szabo | Touch Gesture Evaluation |
| 7 | 2019 | Continuous User Authentication by the Classification Method Based on the Dynamic Touchscreen Biometrics | K Leyfer and A Spivak | Dynamic Touch Movements |
| 8 | 2015 | Touch-Interaction Behavior for Continuous User Authentication on Smartphones | C Shen, Y Zhang,Z Cai, T Yu and X Guan | Continuous Authentication |
| 9 | 2014 | LatentGesture: Active User Authentication through Background Touch Analysis | P Saravanan, S Clarke | Touch Analysis |
| 10 | 2012 | Continuous Mobile Authentication using Touchscreen Gestures | T Feng, Z Liu, K Kwon, W Shi, B Carbunar, Y Jiang and N Nguyen | FAST = Touchscreen Authentication |

MOTIVATION

As the number of smartphone users have raised, there arises a need for secure authentication. These smartphone companies provide various authentication techniques like PIN, password, fingerprint scanner and face scanning. But there was no mention of continuous authentication of smartphones. Some research papers have proposed the idea of continuous authentication of users using biometrics which deal with behavioral characteristics of user like the tapping, scrolling and swiping on the touch screen. This study focuses on continuous authentication of smartphone user on touch screen medium.

ASSUMPTION

A commodity smartphone can be used or a simulation tool. We can design a workflow model where inputs are users actions on touch screen which are captured and stored as a particular pattern. We can do analysis on the pattern stored and produce results.

OBJECTIVES

1. To study basics of continuous authentication on smart-phone touch screen.

2. To do comparative analysis of different methodologies.

3. To provide solution, to design more efficient authentication system for user using smartphone touch screen.

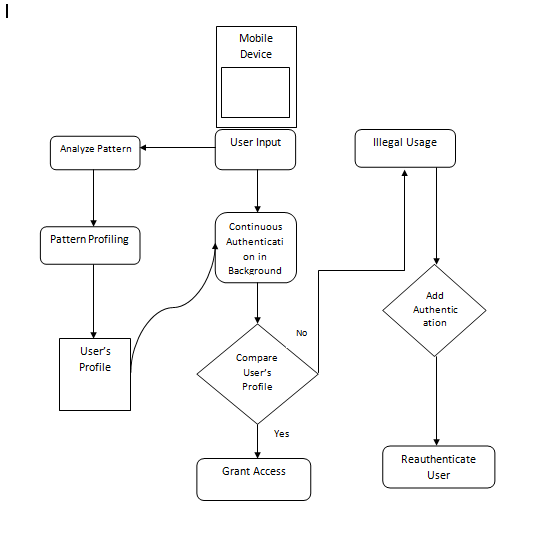
COMPARATIVE ANALYSIS

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sr No | Year | Method | No of Participants | Performance | Features |
| 1 | 2013 | SVM(kernel fn = Gaussian Radial Basid Function) | 75 CSE grad students in Arizona State University | FAR,FRR,ROC(for block size of ns = 14, ns = 20)  Sliding up = 95% | Potrait Mode(8)  Landscape Mode(8) |
| 2 | 2012 | Euclidean, Manhattan, Mahalanobis, R Part, SVM, Random Forest | 32 participants were asked to draw 3 patterns 50 times | ERR = 10.37%  FAR = 85.32% - 86.35%  FRR = 13% - 14%  ROC :  y = 0.05(0.051 +- 0.002) | 3 Different Lock Patterns(Finger-in-dot time, Finger-in-between-dot time) |
| 3 | 2011 | Gaussian Mixture Model(GMM) | 50 users over the span of 2 weeks | X, Y  Median, 75, 90,95 percentile | GPhone, GBrowser, GSMS, BPhone, BBrowser, BSMS and GPS Location |
| 4 | 2014 | SVM(Radial Basis Function kernel) | 32 users | Distinctiveness, Permanence, Avg ERR = lower than 10% | KeyStroke, Slide, Handwriting and Pinch |
| 5 | 2013 | kNN, SVM(Radial Basis Function kernel) | 41 participants | ERR = 0% – 4%  SVM achieves a lower error rate than kNN | Stroke(30):  Mid stroke area covered, mid stroke pressure, dir of end to end line, avg dir, avg vel,length of trajectory,mean resultant length, phone orientation |
| 6 | 2015 | Bayes Net, kNN, Random Forest | 40 subjects(Hungarian 58-question Eysenck Personality Questionnaire) | ERR,DET curves  ERR(RF) = 0.004 ± 0.001  ERR(knnd) = 0.024±0.020  ERR(parzendd) = 0.023±0.019 | Swipe(11):  Duration, length of trajectory, avg vel, mid stroke press, acceleration start, mean press, |
| 7 | 2019 | kNN, RF,GB,Linear SVM | 14 participants | AUC for GB = 0.97 with SD = 0.0002 | User Gestures are distributed in classes(texting, feed,browser, other,system,launcher,game,  video) each having sub divided fields |
| 8 | 2015 | SVM(linear kernel) | 51 students(each subject  contributed around 800 touch-interaction operations) | FAR = 4.68%  FRR = 1.17%  Based on application | Position, Length, Angle, Temporal Features, Linear velocity, Linear Acceleration,Angular velocity, Pressure |
| 9 | 2014 | LibSVM(unary class) and BayesNet(multi class) | 20 participants from Georgia Institute of Technology | MultiUser(Accuracy = 97.78%)  SingleUser(Accuracy = 96.79%) | Radio Buttons, Checkboxes and Sliders |
| 10 | 2012 | Decision Tree, Random Forest, Bayes Net Classifier, FAST | 40 users | FAR = 4.66%  FRR = 0.13% | Touch Gestures, Virtual Typing and Touch Based Drawing |

GAPS IDENTIFIED

* It was observed that traditional smartphone authentication techniques were applicable only during the initial process of security. Once they authenticated the user by checking his/her credentials and comparing them with the database server these techniques did not check for the user’s approval till the time he/she logged out of the system. This provided a back door for the attackers to access the users system once some time has passed by. The attacker can manipulate user credentials and have access to sensitive information of the organization.
* In this study, we report that combining multiple features gives better results than using each single feature alone.
* Touch based results vary for different Mobile Model. For instance, the screen of different phones have slightly different dimensions.
* Sometimes an impersonator might mimic the touch behaviour of another user.(For example, he can be a friend, coworker or a family member)
* Increase the feature space by including a categorical variable that records values like ‘read e-mail’, ‘write e-mail’, ‘browse’, ‘control music player’.
* Influence of sample size

WORKFLOW MODEL



IMPLEMENTATION

A Dataset consisting of various features such as inter stroke time, stroke duration, mean length,etc, with their respective values on the touch screen recorded by a set of actions performed by the user or the participants. The Dataset was taken in CSV format. Exploratory Data Analysis was performed on the data set to identify any missing or duplicate values and replace them with legitimate data. Followed by training and testing of the dataset to give accuracy. kNN and SVM Algorithm were the used to give the results.

* **kNN Algorithm**

The k-nearest neighbors (KNN) algorithm is a simple, easy-to-implement supervised machine learning algorithm that can be used to solve both classification and regression problems.

1. Load the data
2. Initialize K to your chosen number of neighbors

3. For each example in the data

3.1 Calculate the distance between the query example and the current example from the data.

3.2 Add the distance and the index of the example to an ordered collection

4. Sort the ordered collection of distances and indices from smallest to largest (in ascending order) by the distances

5. Pick the first K entries from the sorted collection

6. Get the labels of the selected K entries

7. If regression, return the mean of the K labels

8. If classification, return the mode of the K labels

How to select the k?

In KNN, K is the number of nearest neighbors. The number of neighbors is the core deciding factor. K is generally an odd number if the number of classes is 2. Suppose P1 is the point, for which label needs to predict. First, you find the k closest point to P1 and then classify points by majority vote of its k neighbors. Each object votes for their class and the class with the most votes is taken as the prediction. For finding closest similar points, you find the distance between points using distance measures such as Euclidean distance, Hamming distance, Manhattan distance and Minkowski distance.

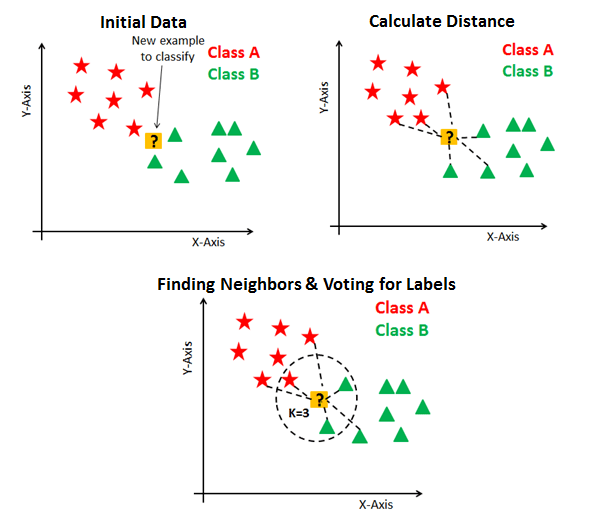


Fig: kNN Algorithm working

* **SVM Algorithm**

The objective of the support vector machine algorithm is to find a hyperplane in an N-dimensional space(N = the number of features) that distinctly classifies the data points. So the task is to find an ideal line that separates this dataset in two classes (say red and blue). According to the SVM algorithm we find the points closest to the line from both the classes. These points are called support vectors. Now, we compute the distance between the line and the support vectors. This distance is called the margin. Our goal is to maximize the margin. The hyperplane for which the margin is maximum is the optimal hyperplane. Thus SVM tries to make a decision boundary in such a way that the separation between the two classes is as wide as possible.

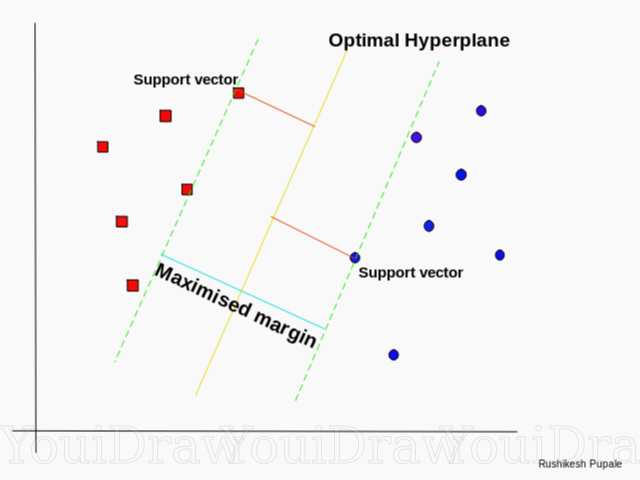


Fig: Optimal Hyperplane using the SVM algorithm

RESULTS

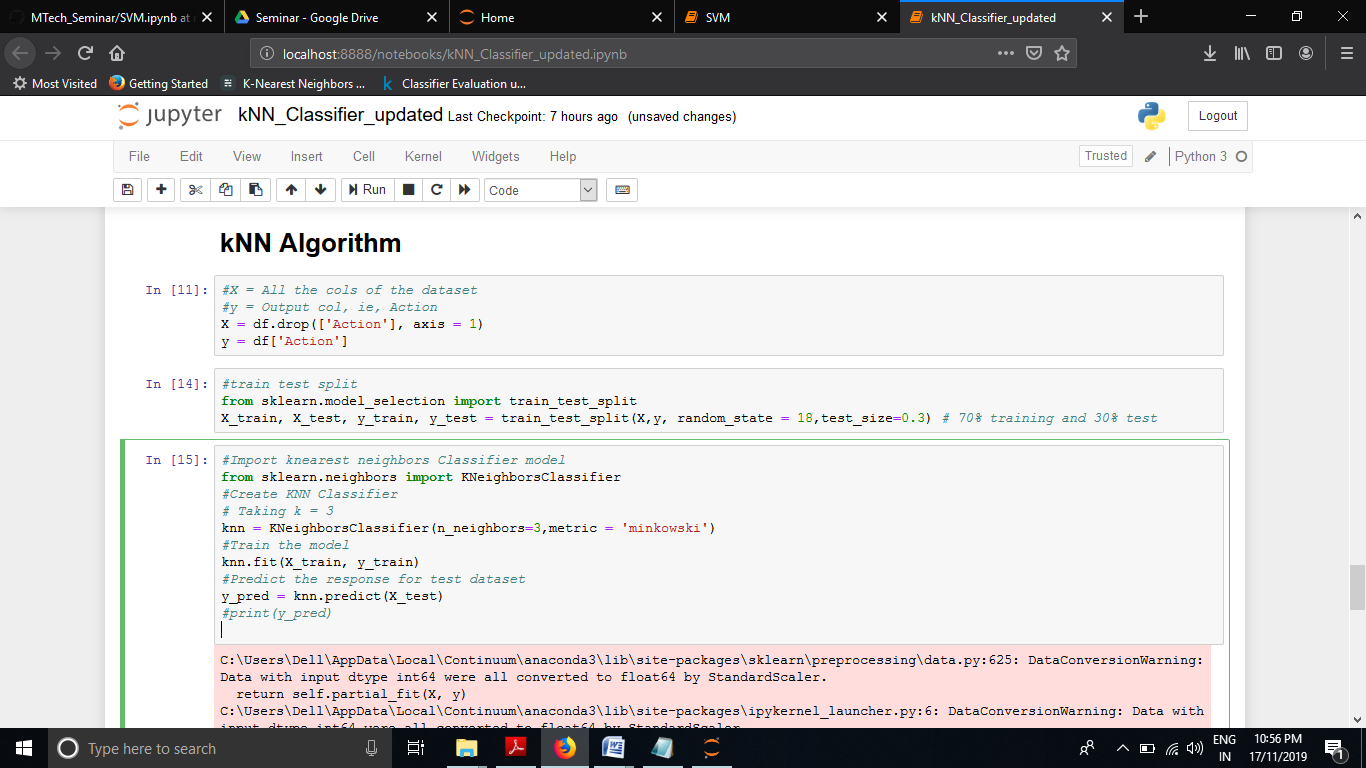


Fig: Implementation of kNN

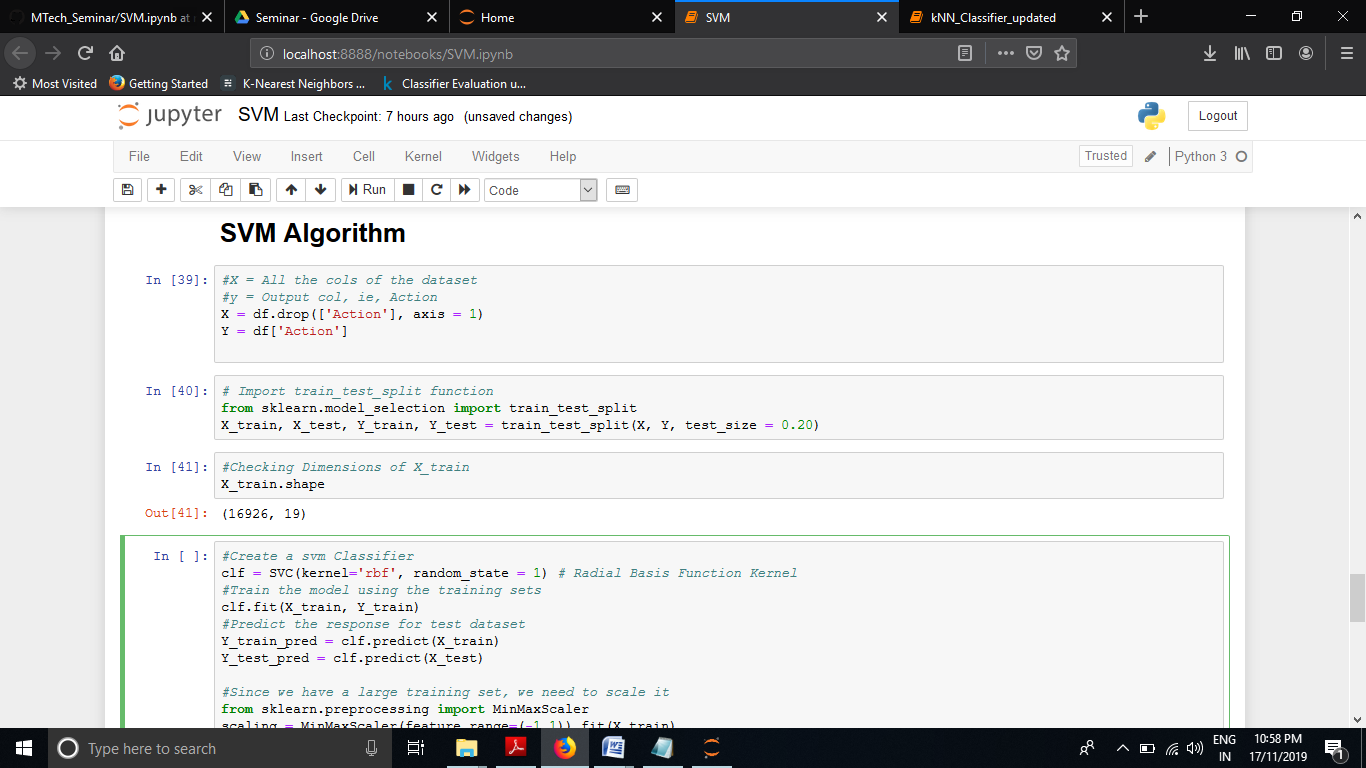


Fig: Implementation of SVM

* **Accuracy**

|  |  |  |
| --- | --- | --- |
|  | kNN(k = 5) | SVM(kernel = rbf) |
| Dataset with 21158 rows and 20 columns | 92.407% | 91.918% |

CONCLUSION

I have studied various methods of Smartphone Authentication from traditional methods like passwords and pins to behavioral techniques like voice, sign, gait,etc. As we delve further it was seen that these traditional techniques has major trap doors that intruders could exploit. So soft techniques were proposed as for authentication of the user. It was observed that we can use simple touch screen movements, which are usually the part of any navigation activity, are sufficient to authenticate the user. For this, I have collected a dataset of 20 different behavioral features from the raw touchscreen data. kNN and SVM classifier were used to train and test the dataset to give accurate results.

FUTURE WORK

The aim of the study was to use touch features for authentication.

1. One way to further improve accuracy could be the use of multistroke based features.
2. Try to implement this model on tablet computer and smart watches
3. Combining this model with other modalities such as, for instance, location, accelerometer data, images from the front-facing camera, and application usage patterns to improve accuracy.

REFERENCES

1. L Li,X Zhao and G Xue,”Unobservable Reauthentication for Smartphones”,NDSS Symposium 2013
2. J. Angulo and E. W’astlund,”Exploring touch-screen biometrics for user identification on smart phones”, In Privacy and Identity Management for Life, pages 130–143. Springer, 2012
3. E Shi,Y Niu, M Jakobson and R Chow,”Implicit Authentication through Learning User Behavior”,Springer,2011
4. H Xu, Y Zhou and M Lyu,“Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones”,Proceeding SOUPS '14 Proceedings of the Tenth USENIX Conference on Usable Privacy and Security,10th Symposium,USENIX,2014
5. M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song.,”Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication,”IEEE Trans. on Information Forensics and Security, 8(1), Jan. 2013.
6. M Antal and L Szabo,”Biometric authentication based on touchscreen swipe patterns”, 9th International Conference Interdisciplinarity in Engineering, INTER-ENG 2015, 8-9 October,2015
7. K Leyfer and A Spivak,“Continuous User Authentication by the Classification Method Based on the Dynamic Touchscreen Biometrics”, PROCEEDING OF THE 24TH CONFERENCE OF FRUCT ASSOCIATION, 2019
8. C Shen, Y Zhang,Z Cai, T Yu and X Guan,“Touch-Interaction Behavior for Continuous User Authentication on Smartphones”,IEEE,2015
9. P Saravanan, S Clarke,“LatentGesture: Active User Authentication through Background Touch Analysis”,Proceeding Chinese CHI '14 Proceedings of the Second International Symposium of Chinese CHI,2014
10. T Feng, Z Liu, K Kwon, W Shi, B Carbunar, Y Jiang and N Nguyen,”Continuous Mobile Authentication using Touchscreen Gestures”,2012 IEEE Conference on Technologies for Homeland Security (HST), 15 Nov. 2012
11. A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, “Touch me once and I know it’s you!: implicit authentication based on touch screen patterns,” in ACM Conference on Human Factors in Computing Systems, 2012
12. N. SaeBae,K. Ahmed, K. Isbister, and N. Memon,”Biometric Rich Gestures: a novel approach to authentication on multitouch devices”,In Proc. of the SIGCHI Conf. on Human Factors in Computing Systems, 2012.
13. H. Seo, E. Kim, and H. K. Kim, “A novel biometric identification based on a users input pattern analysis for intelligent mobile devices,” 2012
14. Z Ali, J Payton and Sritapan,”At Your Fingertips: Considering Finger Distinctness in Continuous Touch-Based Authentication for Mobile Devices”, IEEE Security and Privacy Workshop,2016
15. C Bo, L Zhang, X Li, “SilentSense: Silent User Identification via Dynamics of Touch and Movement Behavioral Biometrics”, MobiCom '13: Proceedings of the 19th annual international conference on Mobile computing & networking, 2013
16. K Niinuma, U Park and A K Jain, “Soft Biometric Traits for Continuous User Authentication”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 4, DECEMBER 2010
17. Z Sitova, J Sedenka, Q Yang, G Peng, G Zhou, P Gasti, K Balagani, “HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users”, DARPA, IEEE, 2013
18. S. Thomas,”Touchscreen handsets dominanting uk mobile market!” http://www.3g.co.uk/PR/Nov2012/touchscreen-handsets-dominanting-uk-mobile-market.html, 2012
19. I. Fischer, C. Kuo, L. Huang, and M. Frank, “Smartphones: Not smart enough?,” in Proc. 2nd ACM CCS Workshop on Security and Privacy in Mobile Devices (SPSM ’12), New York, 2012.
20. R. Yampolskiy and V. Govindaraju,”Behavioural biometrics: a survey and classification”, International Journal of Biometrics, 1(1):81–113, 2008
21. Neil Zhenqiang Gong, Mathias Payer, Reza Moazzezi, Mario Frank, “Forgery-Resistant Touch-based Authentication on Mobile Devices”, In *ASIACCS '16: 11th ACM Asia Conference on Computer and Communications Security* , pages 499-510, ACM 2016
22. M. S. Obaidat and B. Sadoun, “Keystroke dynamics based authentication,” in Biometrics, A. K. Jain, R. Bolle, and S. Pankanti, Eds. New York: Springer, 2002, pp. 213–229.
23. N. Clarke and S. Furnell, “Advanced user authentication for mobile devices,” Comput. Security, vol. 26, no. 2, pp. 109–119, 2007
24. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, “Smudge attacks on smartphone touch screens,” in 4th USENIX Workshop on Offensive Technologies, WOOT ’10, Washington, D.C.,USA, August 9, 2010, 2010.
25. S. Azenkot and S. Zhai, “Touch behavior with different postures on soft smartphone keyboards,” in MobileHCI, 2012.