International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 07 | July - 2022 Impact Factor: 7.185 ISSN: 2582-3930

A Study of Touch Dynamics Biometrics Authentication

Ritu Agrawal[1], Dr. Pharinder Sharma[2]

[1]Research Scholar, Nirwan University Jaipur India
[1]Asst. Professor, Institute of Management & Technology, Faridabad
[2]Asst. Professor, Nirwan University Jaipur India

Abstract

A lot of recent research activities have been fulfilled in keystroke and mouse dynamics in the past three decades but the work in touch screen biometric authentication still needs to be explored. The motivation of this paper is that touch dynamics behavioral biometric authentication can be easily deployed along with user normal activities. Behavioral biometric along with machine learning algorithms and risk-assessment techniques can be efficiently and effectively used as an adaptive authentication. With the rapid usage of smart phones and touch screens in other applications, touch dynamics can be an important authentication factor in multi-factor authentication. Though a numerous studies have been done in behavioral human biometric, there is indeed much scope in the area of touch dynamics. The objective of this study is to provide the throughout survey of techniques used in this field along with the advancements for further research work.

Keywords

Biometric, touch dynamics, Behavioral authentication, multi-factor authentication, adaptive authentication

1. Introduction

The rapid advancements in technology have made our life quite easy, facilitating access to number of applications. This has raised the need of authentication and user authentication has become an issue and a challenge than ever before.

1.1 Authentication

User authentication methods can be labeled into different aspects as: something user knows (password), something user has (OTP), something user is (physiological biometric), something user exhibits (behavioral biometric). According to the result of a survey, the user's possibility as which biometric authentication process they prefer to apply on a mobile device, the top most choice to take into consideration is the usability factor [1]. Behavioral Biometric is capable of providing robust security along with speed and convenience. Every biometric authentication method has its own strengths and weaknesses so which authentication method is best depends upon the situation.

1.1.1 Knowledge-based authentication

The most popular authentication techniques for mobile users are still knowledge-based approaches like password, PIN, and pattern matching [2]. But these methods, if used solely to authenticate a user, are considered to be the weakest level of authentication as it is simply circumvented and is not considered reliable.

1.1.2 Possession-based authentication

Authentication based on what the user has, such as token or OTP when used along with password increased the security but added friction in user experience. Two-factor or multi-factor authentication also increases the cost as multiple factors are implemented to attain the security.

1.1.3 Biometric Authentication

Biometric authentication is one of the most important authentication methods than other authentication technique as it can't be duplicated, transferred, hooked, forged or forgotten [3][4]. Physiological biometric refers to user's physical attributes such as finger print, face recognition, iris pattern. Behavioral biometric refers to the behavior-based factors which are formed by user nature or habits as signature style, voice style, gait style and touch dynamics. Primarily issues in adaption of physiological biometric method are as (i) sluggish authentication rate (ii) social discomfort (iris scanning, face recognition and etc.) (iii) due to implementation costs, large-scale adoption is not feasible (DNA analysis).

Behavioral biometric solve these issues and has certain characteristics that make it easy to implement than other authentication factors. These characteristics are:

(i) By employing existing sensors in the computing devices, compared to other biometric authentication methods, it is less expensive.
(ii) It is a non-intrusive method and can be applied along-with user's normal usage activities [5].
(iii) There is no hindrance with other authentication methods.
(iv) There is no need to conceal.

The rest of the paper is closely-knit as follows: Section 2 covers the a detailed overview of touch dynamics biometrics based authentication along with its advantages and challenges, Section 3 focuses on the design and methodology used in touch dynamics authentication and evaluates the work done by different researchers during each phase of operational process, section 4 shows its importance as adaptive authentication and section 5 finally concludes.

2. Touch Dynamics

The practise of sensing and evaluating human touch rhythm on touch screen devices is known as "touch dynamics biometric." (e.g. smart phones). When people use these gadgets, a type of digital signature is produced. These signatures can be used as a personal identifier because they are distinctive and particular to each person. Each user will have a unique profile highlighting their behavioral and style details.

2.1. Overview

In the 19th century, with the commencement of telegraph revolution, telegraph keys were the source of input data which were later substituted by as keyboards, mobile keypads, and etc. Today, input devices with a touch screen are widely used in the modern era. Touch screens have become the leading input medium, and in case of mobile phones, more than 78% of all phones are using a touch screen [6]. Besides smart phones, touch screens have also become common input medium from digital tablets, and ATM machines to the multimedia player on our car.

2.2 Merits

Low implementation and deployment cost
Touch dynamics can be easily captured with the existing sensors in the devices therefore it requires no external hardware to capture the data. Now- a-days, with the availability of high-resolution sensors in the devices, discriminative features can be easily extracted during authentication process. Besides this, touch dynamics remain unaffected with the external factors as light, noise etc.

Non-intrusive and non-vulnerable
Touch dynamics biometric authentication go along with the user's normal usage activities making it non-intrusive. That is, data acquisition can be done parallel to user's activities without requiring any extra or very little interaction with the user. As touch dynamics data is acquired in an explicit way, it exhibits variance with different times, so is less vulnerable to privacy risks and is most appropriate for continuous authentication.

Additional Security
Touch dynamics can be easily combined with the other authentication methods (password, PIN) to strengthen security by adding extra security layer. It can be easily used as adaptive authentication. This is to provide a balance between security and usability.

2.3 Demerits

Lower Accuracy
Behavioral biometric exhibits lower accuracy performance as compared to physiological biometric due to the variations during data acquisition process. It gets easily affected by other reasons such as fatigue, mood, stress. Therefore maximizing accuracy performance is a challenge for touch dynamics authentication.

Higher Energy Consumption
Every touch screens based electronic devices are commonly used on battery for example mobile phones, music systems and etc. Though most of the power in these devices is consumed during communication, these devices also consume power when data is captured through their embedded sensors. Therefore, how to reduce the energy consumption during biometric authentication is a challenge.

3. Touch Dynamics Operational Method

The Touch Dynamics authentication system can be used in one of two views: identification (recognition) or verification (authentication).

Verification views: In the verification, it is work to inquire a claimed identity, which means it asked to answer the question "is this person whom he/she claims to be". Authenticating a mobile user is an example of this mode.

Identification views: In the identification, it is applied to classify and identify some unknown human identity. Here, it is asked to answer the questions like "who is this person" or "is this person in the system. Typically, this is utilized in cybercrime.

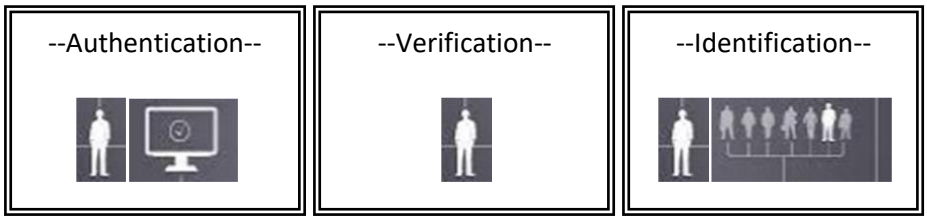

Figure 1: Verification vs. Identification

Touch dynamics design basically work in two phases: Enrolment phase and Authentication phase. Finally, the decision will be based on the evaluation criteria.

Enrolment phase: Here, touch dynamics data are grouped there after it stored as a reference template.
Authentication phase Touch dynamics test samples are matched to reference templates that have been preserved in order to calculate closeness scores that are then compared to a predetermined threshold by machine learning approach.

The working of touch dynamics model is explained in figure 2.

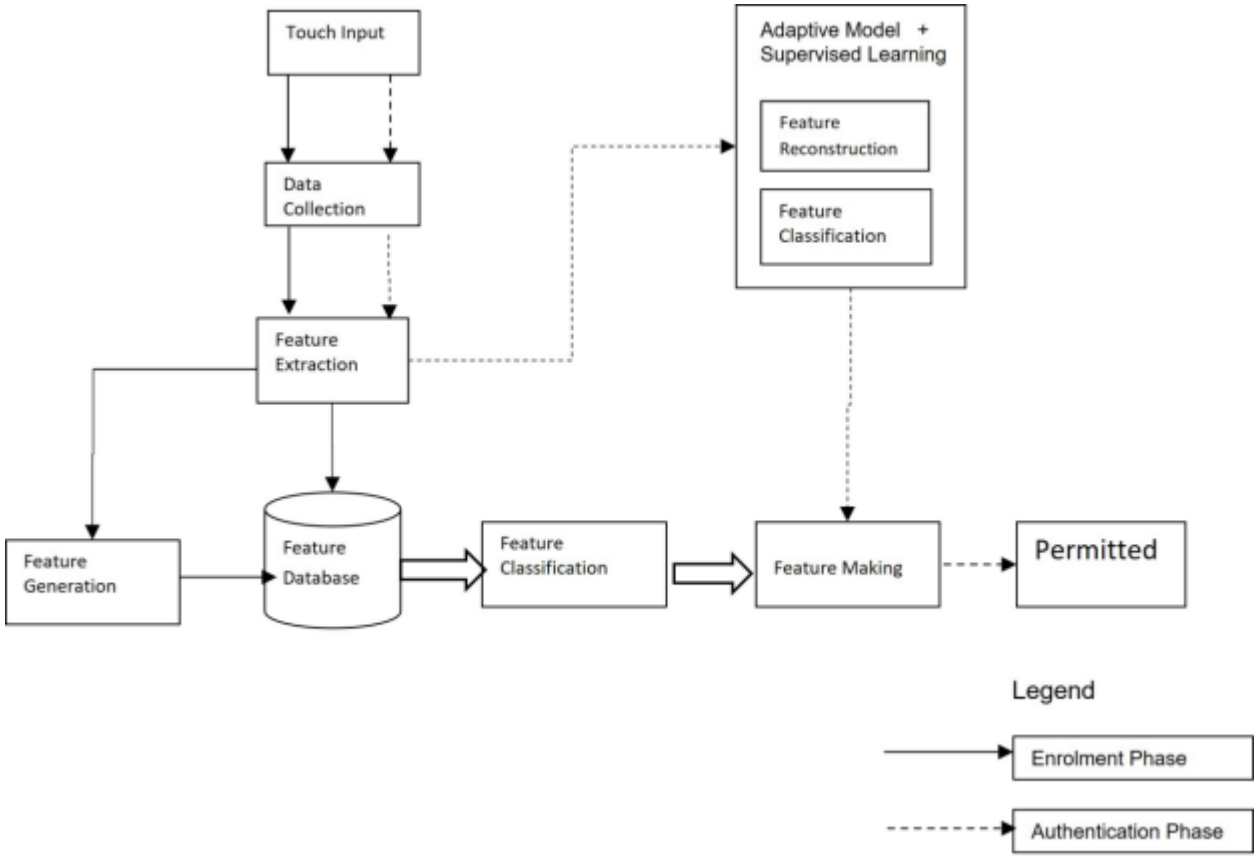

Figure 2: Diagram of Touch Dynamics Model

Each of the phases of biometric authentication is represented by a block in the flow diagram and each block performs a specialized function which is described below.

3.1 Data Collection

The data collection component as known as fundamental component, that it is employed for collecting raw data through a touch screen device and transforming them into a well significant information.

3.2 Feature Extraction

This is one of the fundamental operations that are carried out both in enrollment and authentication phase. This may include feature generation component if required. Touch dynamics patterns have unique characteristics that can be used to distinguish one to another. These unique characteristics are collected as a template and are stored in the one of feature database for further reference. The common features of touch dynamics include (i) Timing, (ii) Spatial, (iii) Motion along with others. The following categories can be used to group the various functionalities that can be used with touch screen inputs [7]:
Single-Touch (ST): This involves touch press down, followed by a touch press up that is touching a single point.

Touch Movement (TM): This involves a touch point moved (also called drag) and then finally touch press up.

Multi-Touch (MT): This involves two or more cumulatively, distinct touch press down events at multiple position of the touch screen display (rotation), either with or without any operation before a touch press-up.

3.3 Feature Database

All this extracted data which contains the unique features are gathered as a template and is saved in the feature database for further reference.

3.4 Feature Classification

Feature classification component is the core of biometric user authentication system. Generally, the feature classification model will select the machine learning algorithm to form the training samples. Supervised machine learning algorithms can be used to classify data more accurately.

3.5 Feature Matching

The feature matching component works to match the current user's with the predefined database and is then verified as a legitimate user (permitted) or illegitimate one. In the later case, adaptive model will be invoked.

3.6 Feature Adaption

This component will help us in real-time authentication with newly feature generation process.

3.7 Evaluation Criteria

The quantify the performance of biometrics verification system, the metrics that are commonly used are the False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER). False Acceptance Rate (FAR) is the proportion of the number of illegitimate users who are accepted by the biometric system. Certain other terms such as miss alarm rate, false positive rate, etc are also used for FAR. False Rejection Rate (FRR) is the proportion of the number of legitimate users who are rejected. Other terms used for FRR are false alarm rate, false negative rate, etc. Equal Error Rate (EER) is used to measure and compare different biometrics authentication methods. It is also known as Crossover Error Rate (CER) which is a compromise between FAR and FRR. This is a trade-off between FAR(security) and FRR(usability). Both FAR and FRR should be low. EER is to equalize FAR and FRR.

3.8 Review of Related Work

Feng et.al[8] in 2012 in their work on touch based user authentication, used smart phone's sensors along with sensor gloves to record touch data. They named their mechanism as FAST. The study was conducted on 40 participants. Three distinct gestures such as swiping, pinching and spreading, and dragging or drawing shapes were carried out by each participant. For each touch gesture, 53 features were extracted. Their result showed a False Accept Rate (FAR) of 4.66 % and False Reject Rate of 0.13 % in the login phase.

Meng et al. [9] again in 2012, did the work on the concept of touch dynamics and particularly extracted 21 different features using SVM classifier. They did their study on 20 participants. They proposed a hybrid classifier called PSORBFN(decision tree, Bayes Net). Through imitation of operations, they got success in reducing the average error rate down to 2.92% (FAR of 2.5% and FRR of 3.34%).

Frank et al. [10] collected 30 features from the touch screen input using a nearest neighbor classifier (KNN) and support vector machine (SVM), with a Gaussian RBF kernel. Their results were authentic and robust, with equal error rates (EERs) between 0 and 4 %, depending on the conditions.

Li et al. [11] used user's finger move as touch feature. Touch-data collection was done using logs from Android based system. Depending upon the rights of the user on the operating system, these logs can record data from the touch screen device. The raw data collected were grouped into different gesture types. In particular, they used 13 metrics to measure a sliding gesture which includes first touch point, first touch pressure, first touch movement and all. They then conducted a study with 75 users. SVM classifier gave the best result for sliding up gesture with accuracy as 95.78 %.

Meng et al. [9,12] then proposed an adaptive authentication mechanism so that appropriate classifiers can be used at different times depending upon situation, so that accuracy can be maintained during user authentication process. They have found that the performance depends upon the selected classifier. Their study evaluated 50 participant and the result depicted an average error rate of 2.46 %.

Feng et al.[13] named their authentication scheme TIPS. It was a novel, continuous,context-based user authentication system for uncontrolled environment. They implemented TIPS on the Android operating system and evaluated with 123 participants (23 owners and 100 guests) and over 23 different phones as Galaxy S3, Galaxy S4, Nexus 4. Classifiers which were used to gather data at varying times were One Nearest Neighbor (1NN) and Dynamic Time Warping (DTW). Their system reached 90% accuracy in real time. There was an issue of privacy as there is a need of installing different forms of Android operating system.

Meng et al. [14] further took the authentication system to a good level by developing a TMGuard, touch-based authentication mechanism. They evaluated 75 participants. They conducted their study on 9-dot patterns and found that the successful rate is decreased from 97.8 % to 91.1 % for males and from 97.8 % to 88.9 % for females, respectively.

Stefania Budulan et al.[15] gathered data from 5 Android phones screens and extracted features based on 41 user's data sets. Touch-down and touch-up is considered as an input sequence action. That is, records for clicks span from action 0 to action 1, without any movement in-between. AdaBoostClassifier (also known as an Adaptive Boost classifier) is used as an ensemble method by adjusting the performances of incorrectly classified instances. GridSearchCV , a tool of Scikit-learn[5] was used for fitting the specific estimator(model) onto the data set. They achieved an accuracy of 83% approximately.

Above stated touch dynamics-based user authentication schemes is summarized in the tabular form.

Study	Data Collection	Classifiers	No. of users	Mechanism with features	Performance
Feng et al. [8]	digital	Random forest,	40	FAST with 53 features	FAR: 4.66 %

in 2012	sensor glove	Bayes Net			FRR: 0.13%
Meng et al. [9] in 2012		SVM	20	PSORBFN with 21 features	FAR: 2.5% FRR: 3.34%
Frank et al. [10] in 2013		SVM	41	Touchalytics with 30 features	ERR: nearly 4%
Li et al. [11] in 2013	Device logs	SVM	75	Sliding gesture with 13features	Best Acc.: 95.78 % for sliding up
Meng et al. [9, 12] in 2014			50	Adaptive authentication scheme With 8 features	FAR: 2.55% FRR: 2.37%
Feng et al. [13] in 2014	Multi-touch driver and running application	1NN DTW	123 (23 device owners 100 guests)	TIPS-Touch gestures and adaptive sequential identification	90% accuracy
Meng et al. [14] in 2016			75	TMGuard	EER: 1–3 %
Stefania et .al [15] in 2016	5 Android phones	AdaBoost classifier GridSearchCV Tool	41	64 features	83% accuracy approax.

4. Behavioral Biometrics for adaptive authentication

Adaptive authentication is a way for selecting the appropriate authentication elements based on a user's risk profile and scenarios — that is, for adapting the type of authentication according to the situation. There are different ways of deploying Adaptive Authentication procedure:

✓ Static: Defining risk levels for different factors, such as user role, resource importance, and location, time of day or day of week.

✓ Dynamic: This is the learning mode in which system can learn the typical activities of users based on their tendencies over time. This learned form of adaptive authentication is similar to behavioral correlation.

✓ Hybrid: A combination of both.

But considering the dynamic nature as a challenge, a machine learning-based model could be recognized as an appropriate mechanism for implementation. Machine learning model analyses risk scores based on behavior and context and determines the most effective security response for a certain situation to make the process more salient. The various inputs which are examined for adaptive authentication are environmental factors, device-based factors, attribute-based factors, behavior-based factors as shown in figure 3.

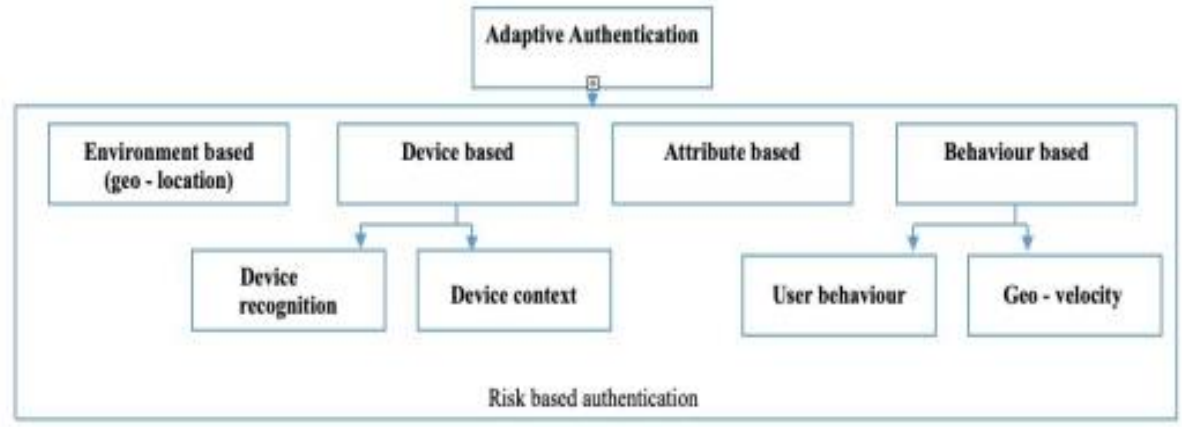

Figure 3: Adaptive authentication Scenarios

Behavior-based factors are behavioral biometrics which is acquired from user normal behavior or habits like signature, voice, gait, and touch dynamics. This can be easily implemented in real-time applications such as online transaction systems, air-traffic control systems and all to go one step ahead of fraudsters. Behavioral Biometric is to provide security without causing friction in user experience along with adaptability.

5. Conclusion

The work of different researchers in touch dynamics has been summarized here. This will indeed be helpful for new researchers to have the knowledge of behavioral biometric authentication.
It has been suggested here that touch dynamics can be an important biometric for continuous and adaptive authentication. The adaptive capability in touch dynamics makes the process cumbersome but considering the security as main criteria, it can be neglected. User involvement is very important in this type of study so it requires large user study with more number of users. The limitations of touch dynamics authentication can be bypassed since this authentication method is often used as an additional biometric in multi-factor authentication.

Another scope in this research is to build a model that analyses time-stamped data with the deep learning algorithms. Feature extraction can also be done with different types of auto-encoders, which will help in reducing feature engineering time and will improve overall accuracy.

6. References

[1] De Luca, A., Hang, A., von Zezschwitz, E., Hussmann, H., 2015. I Feel Like I'M Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones, in: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI '15. ACM, New York, NY, USA, pp. 1411–1414.

[2] Khan, H., Atwater, A., Hengartner, U., 2014. Itus: An Implicit Authentication Framework for Android, in: Proceedings of the 20th Annual International Conference on Mobile Computing and Networking, MobiCom '14 ACM, New York, NY, USA, pp. 507–518. doi:10.1145/2639108.2639141

[3] W. Meng, D.S. Wong, S. Furnell, J. Zhou, Surveying the development of biometric user authentication on mobile phones. IEEE Commun. Surv. Tutorials 17(3), 1268–1293 (2015).

[4] Jain, A.K., Flynn, P., Ross, A.A. (Eds.), 2008. Handbook of Biometrics. Springer US, Boston, MA.

[5] Shen, C., Zhang, Y., Guan, X., Maxion, R.A., 2016. Performance Analysis of Touch-Interaction Behavior for Active Smartphone Authentication. IEEE Trans. Inf. Forensics Secur. 11, 498–513.

[6] W. Meng, D.S. Wong, S. Furnell, J. Zhou, Surveying the development of biometric user authentication on mobile phones. IEEE Commun. Surv. Tutorials 17(3), 1268–1293 (2015).

[7] Y. Meng, D.S. Wong, R. Schlegel, L.-F. Kwok, Touch gestures based biometric authentication scheme for touchscreen mobile phones, in Proceedings of the 8th China International Conference on Information Security and Cryptology (INSCRYPT). Lecture Notes in Computer Science, vol. 7763 (Springer, 2012), pp. 331–350, Beijing.

[8] T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, "Continuous mobile authentication using touchscreen gestures," in IEEE Conference on Technologies for Homeland Security, Nov 2012, pp. 451–456.

[9] Y. Meng, D.S. Wong, L.F. Kwok, Design of touch dynamics based user authentication with an adaptive mechanism on mobile phones, in Proceedings of the 29th Annual ACM Symposium on Applied Computing (ACM SAC), Gyeongju (2014), pp. 1680–1687.

[10] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touch analytic: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 136–148, Jan 2013

[11] L. Li, X. Zhao, and G. Xue, "Unobservable reauthentication for smart phones," in Proceedings of the 20th Network and Distributed System Security Symposium, 2014.

[12] W. Meng, D.S. Wong, L.F. Kwok, The effect of adaptive mechanism on behavioural biometric based mobile phone authentication. Inf. Manage. Comput. Secur. 22(2), 155–166 (2014).

[13] Feng, Tao; Yang, J., Yan, Z., Tapia, E.M., Shi, W.: Tips: Context-aware implicit user identification using touch screen in uncontrolled environments (2014)

[14] W. Meng, W. Li, D.S. Wong, J. Zhou, TMGuard: a touch movement-based security mechanism for screen unlock patterns on smartphones, in Proceedings of the 14th International Conference on Applied Cryptography and Network Security (ACNS 2016), Guildford (2016), pp. 629–647.

[15] Budulan, Stefania, Burceanu, Elena, Rebedea, Traian, Chiru, Costin Continuous User Authentication Using Machine Learning on Touch Dynamics DOI - 10.1007/978-3-319-26532-2_65.

[16] H. L. S. R. P. De Silva, D. C. Wittebron, A. M. R. Lahiru, K. L. Madumadhavi, L. Rupasinghe and K. Y. Abeywardena, "AuthDNA: An Adaptive Authentication Service for any Identity Server," 2019 International Conference on Advancements in Computing (ICAC), 2019.

[17] I. Traore, I. Woungang, M. S. Obaidat, Y. Nakkabi, and I. Lai, “Online risk-based authentication using behavioral biometrics,” in Multimedia Tools and Applications, 2014.

[18] V. M. Patel, R. Chellappa, D. Chandra and B. Barbello, "Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges," in IEEE Signal Processing Magazine, vol. 33, no. 4, pp. 49-61, July 2016.

[19] T. Neal, D. Woodard, and A. Striegel, “Mobile device application, bluetooth, and wi-fi usage data as behavioral biometric traits,” in IEEE International Conference on Biometrics Theory, Applications and Systems, Sept 2015, pp. 1–6.

[20] Crawford, H., Renaud, K., Storer, T., 2013. A framework for continuous, transparent mobile device authentication.Comput. Secur. 39, Part B, 127–136.

[21] A. Sethi, O. Manzoor, and T. Sethi, “User authentication on mobile devices,” tech. rep., Cigital, 2012.

[22] L. Zhou, Y. Kang, D. Zhang, and J. Lai, “Harmonized authentication based on ThumbStroke dynamics on touch screen mobile phones,” Decision Support Systems, vol. 92, pp. 14–24, Dec. 2016.

[23] A. Buriro, S. Gupta, and B. Crispo, “Evaluation of motion-based touchtyping biometrics for online banking,” in Proceedings of the International Conference of the Biometrics Special Interest Group, BIOSIG ’17, pp. 1–5,Sept. 2017.

[24] Jiang Lijun, Meng Weizhi “Smartphone User Authentication Using Touch Dynamics in the Big Data Era: Challenges and Opportunities” in book Biometric Security and Privacy (pp.163-178) Springer International Publishing,2017.

[25] Kanlun Wang, Lina Zhou, Dongsong Zhang, Zhihui Liu “What is More Important for Touch Dynamics based Mobile User Authentication?” in Proceedings Pacifc Asia Conference on Information Systems (PACIS) 2020.