Turkish Journal of Computer and Mathematics Education Vol.12 No.10 (2021), 3013-3023

Research Article

Hybrid Behavior-based Biometric Authentication Systems (HBAS)

Vasaki Ponnusamy[a,*], Leow Wei Han[a], NZ Jhanjhi[b], Najm Us Sama[c], Mamoona Humayun[d]

[a]Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman, 31900 Kampar, Perak, Malaysia;
[b]School of Computer Science and Engineering (SCE), Taylor's University, Malaysia;
[c] Deanship of Common First Year, Jouf University, Sakaka 72341, Saudi Arabia ;
[d]College of Computer and Information Sciences , Jouf university , Sakaka 72341, Saudi arabia;

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract

An idea of proposing hybrid security based on behavioural biometrics is displayed in this paper, on the two bases of tapping and swiping. Tapping and swiping are the main focus as they are the easiest actions to perform on a mobile device. Actions and mannerisms performed by either attacker and/or the user are explained alongside the results of said actions and mannerisms. An attacker will haphazardly try to brute force the motion while the owner will perform his action consistently. Then, a training set is done where an attacker and an owner's training sets are obtained and set, to determine which classifiers work best in determining the confusion matrix from a range of training set values with Hoeffiding Tree and Naïve Bayes Multinomial classifiers performing the best over the three sets of training values provided.

Keywords: Smartphone security, Mobile authentication, Password, Biometric, Machine learning, Keystroke dynamics, Touch dynamics, Tapping, Swiping.

1. Introduction

The earliest generations of security has been passwords [1], passcodes, and arguably unlock patterns in 2008[2]. While these methods of authentication are said to be the failsafe method that mobile phones fall back on when the usual authentication methods fail, their usage has been dwindling. Aviv et al has published a paper that exposes the vulnerabilities of unlock patterns in particular, with shoulder surfing being the main method of attack for this paper [3]. Other types of attacks that influenced the dwindling usage are brute force attacks, dictionary attack, and keyloggers among a few [4]. Other reasons why the usage of passcodes and unlock patterns have been reduced are that users may be worried more about the physical loss of their phone [5], users may use the same passwords for different accounts [6,7], users may forget their passwords [7], and users may find them annoying [8,9,10]. Though, [9] has recorded down that users are open to biometric solutions as a whole. Research and Development of the mobile security field had shifted to biometric authentication systems to explore on this domain. Biometrics are the traits of a unique human that is believed to be hard to spoof. More importantly, there are two types of biometrics. Physiological biometrics are the usage of recognition of a person's physical features such as the face, fingerprints, and iris. In the meanwhile, behavioral biometrics are the usage of a person's perceived behavior on the theory that different people have different habits of using their mobile devices [11,12,13,14]. While some physiological biometrics have been successfully implemented into modern society, such as fingerprint scanners and face recognition on modern smartphones, as they have received a positive reception for convenience, there has been issues with just how valid they really are, such as [15,16]. Hence, the direction of focus of research and development has now been shifted to behavioral biometrics. While different types of physiological authentication have been proposed, not much usage of physiological biometric authentication systems have been seen, for they require additional hardware [17], perform badly under suboptimal conditions [18], and are just plain inconvenient [18]. Although biometrics can be considered to be still in the early stages, its popularity and usage among the general public is considered to be on the rise [19]. Recent years of this decade have seen increase of the usage of machine learning in biometric systems, with a detailed survey recorded in [20]. Though there is a need to consider power consumption of authentication devices due to the computational power needed of machine learning, with [21] publishing a paper that suggests battery consumption as a metric for future authentication. While there have been multiple discussions in striking a balance between user acceptance and authentication systems [5,8,9,10,22], a paper reveals that user preferred gestures are the most biometrically secure [23]. Also, a combination of CA (Continuous Authentication) and IA (Implicit Authentication) can increase accuracy rates compared to standalone CA and standalone IA [24] Thus, there is an aim to find a hybrid combination that can possibly combine both CA and IA, or in other words, combine physiological biometrics with behavioral biometrics while gaining acceptance from the general public as well.

2. Motivation

The usage of mobile phones has ramped up ever since the revolution of the smartphone industry, spearheaded by Apple in 2007[25], followed by Android in 2008[26]. Some of the wide array of reasons include the development of hardware to be more compact while boosting computing power, portability and in turn being able to do more, and the implementation of sensors [27], both internal and external, for data collection. Data collection is hardly limited to sensors alone, with the majority of data compiled being personal information and imprints that would be delivered to data analytics that use said personal imprints to deliver a personalized advertisement to your mobile phone, for example Facebook with their personalized ads. However, the influx of the amount of data

collected have caused concern for potential of the abuse of data collected, not just for the use of corporations [28], but in our own mobile phones as well. A social experiment done by US-based security firm Symantec in five major cities in North America was attempted with fifty smartphones 'dropped' at public locations where the public could access them. Results have shown that 96% that found the smartphones have accessed them, while 86% of those who accessed those phones, accessed personal information, 83% read business information, 60% started up social media information and personal emails, 50% started using remote access and 43% of them have accessed online banking information [29]. It also can be said that while students and professionals were well-versed in the security of desktop computers and laptops, the same cannot be said for mobile devices. A survey done has shown that more than 30% of students' smartphones and 40% of student tablets' have no security required to access their devices, this percentage even expanding to IT professionals [8,9]. A survey census done by Redmiles et al has shown that the main reason for rejecting security advice is inconvenience [22]. [9] also supports this idea. The motivation for this project would be increased security on mobile phones on the physical layer. As passwords are seeing less usage, alongside the increased usage of physiological biometric areas, behavioral biometrics are a relatively new area that has sparked interest as of recent. Thus, it would be interesting to see whether it would truly be possible to authenticate a user based on his or her behavioral biometric action.

3. Related Works

As stated earlier, there are two known sections of biometrics, which are physiological and behavioral biometrics. Plenty of research has been done in the physiological aspect, which includes eye recognition (iris and retina) [30,31,32], facial attributes [33], and fingerprints [34]. For behavioral biometrics, meanwhile there has been considerable discussion on what counts as a behavioral biometric, although the discussions have been based on the fact that a biometric feature must be unique to the degree that it should differ from person to person [35]. To date, there have been up to six behavioral traits that have been covered in this literature review, which are tapping, swiping, keystroke dynamics, touch dynamics, gait, and touch gestures.

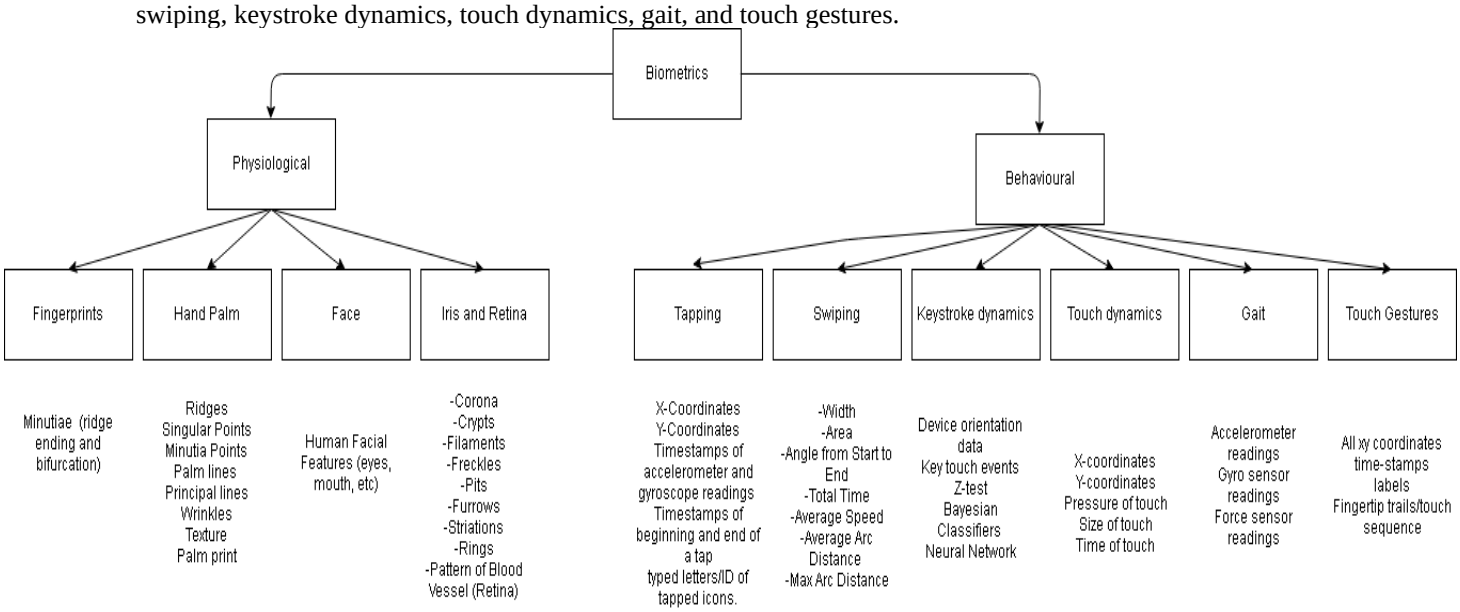


Fig.1. Different types of common biometric features recorded by sensors for mobile systems

2.1 Tapping

A tapping motion can be defined as softly pressing down onto the touch screen or the keyboard. In this scenario, the main features can be said to include XY coordinates, accelerometer and gyroscope readings if available, timestamps of a beginning and at the end of the tap, and possible the typed letter/ID of the tapped icon. [36] has implemented a hybrid authentication system with the usage of tapping and phone holding movements while holding the phone while doing so. [37]'s work looks into the usage of UI buttons for feature obtaining.

2.2 Swiping

A swiping motion is said to be a movement over a certain direction on a screen. In modern devices, this can be attributed to having certain actions done with certain points swiped on the device's screen. The main features for this behavioral biometric can include width and area of the swipe done, the angle from the start to the end of the swipe, total time taken to swipe, the average speed and the average arc of the swipe done, and the distance and the max distance of the swipe done. [38] 's work has attempted relying on obtaining swiping features via a questionnaire that forced the users to use a horizontal slider in order to answer the questionnaires, which show that sensor data is highly involved in obtaining reliable feature data. [39] brings a combined approach with the

involvement of swiping, pickup and vocal features, with the conclusion that swiping is a much more robust modality than pickup, due to the external factors of the user's actions while registering test data for the pickup modality.

For the dataset, a theory as to why the data has such a high correct rate of the data is via the area of where the user taps versus where an intruder taps. The user would concentrate his or her action at certain areas, while an intruder would be haphazardly performing the action at a random area to try and determine how the user performs the action. In the figure below, the user's data, colored in blue, is concentrated in one area, while the imposter's data, colored in red, is spread about the graph.

2.3 Keystroke

The modality of keystroke dynamics is said to be the exact timing of when a key was pressed and released while a person is typing at a computer keyboard. It could be said to be similar to tapping and touch dynamics in the features gained for the training model, as the actions done are relatively similar which is tapping on a screen, since mobile devices use a virtual keyboard for data input. [40] has noted that keystroke dynamics can be a possible method of mobile authentication even with an overly simplified password such as 1111, as the field of keystroke dynamics was limited to the computer keyboard before. [41] showed that sensor-based features mostly outperform keystroke-based features. [42] had implemented Deep Learning to a mobile authentication system to analyze the keystroke features. [43] has attempted to create an application with an overly simplistic approach of static keystroke dynamics with no machine learning involved. [44] has also used Deep Learning in their mobile authentication system for continuous authentication approach.

2.4 Gait

Gait is defined as the manner of walking of a person. In the case of behavioral biometrics, the features that gait provides are mostly obtained from sensor readings, such as the accelerometer, the gyroscope, and the force sensor. The basis on using gait as a behavioral biometric is that humans have different methods of gait, and this can be used as features. [45] has implemented the usage of three different classifiers for the data of three different gait-related actions. [46] has shown the potential of gait to be combined with other behavioral biometrics for a higher accuracy factor.

2.5 Touch Dynamics

Touch dynamics are could be said to be similar to keystroke dynamics, though it could be argued that touch dynamics work on a more continuous authentication-based framework, as it does not actively prompt the user, but rather, obtain the user's details while he is using the mobile device. [46] has developed an application that works as a framework to focus on continuous authentication of the user's touch dynamics while using his phone. [47] shows the potential of a hybrid continuous authentication and implicit authentication system using the touch dynamic features.

2.6 Touch Gestures

Touch gestures are a more widely defined variant of touch dynamics, using a variety of gestures to perform implicit authentication via a gesture done, and authentication based on how the gesture is done. [48] introduces the framework for touch gestures in uncontrollable scenarios, [49] implements a hybrid of both physiological and behavioral biometric features, and [50] has introduced a novel way of obtaining touch gestures via a signature done with the user's finger.

Table 1. Review of Behaviour Authentication System

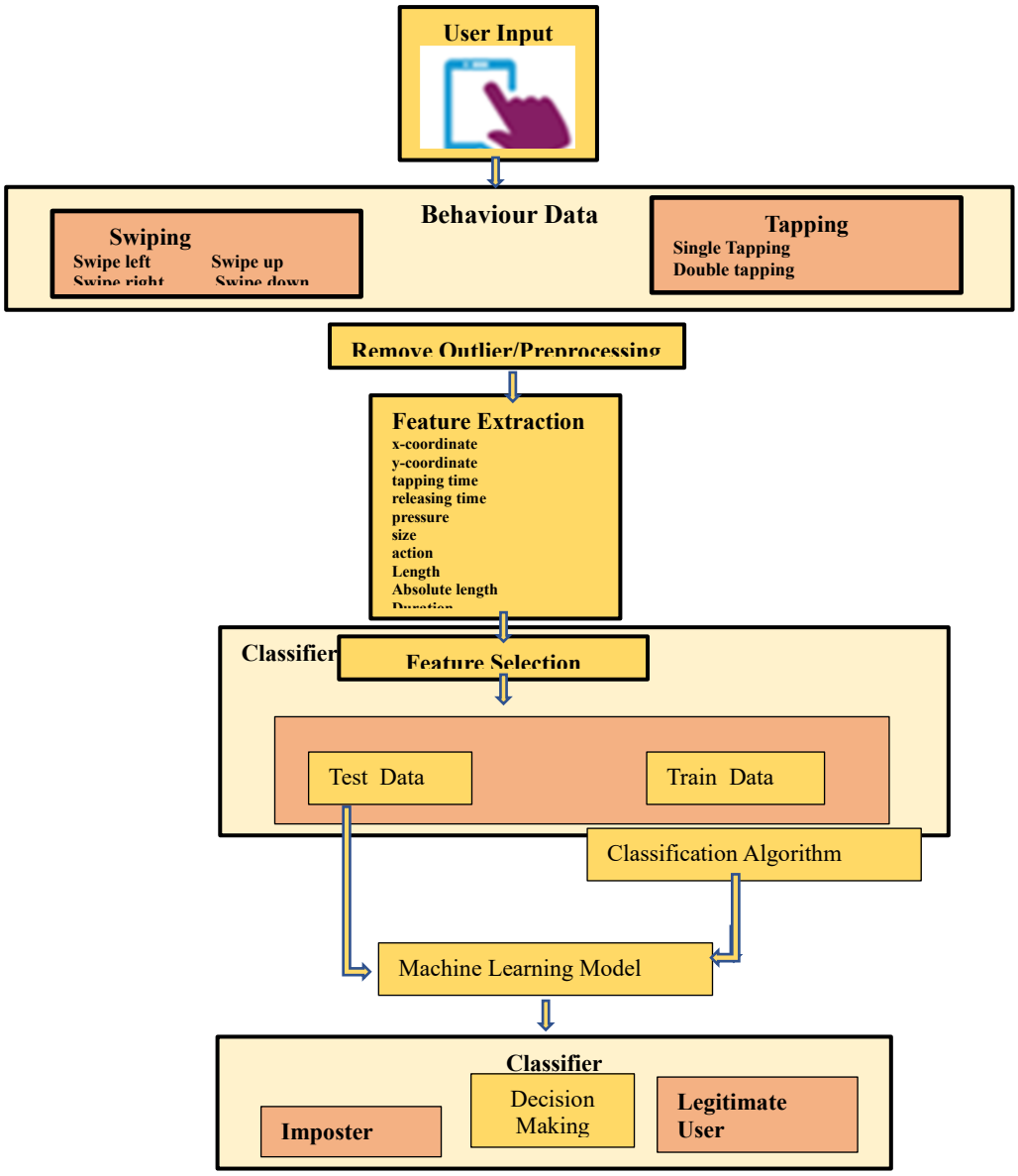
Type of Behavioral Biometric Investigated	Papers	Machine Learning involved? If yes, what classifiers?	Advantages/Results	Disadvantages
Tapping	[36]	BN	Attempts a fusion of touch data with other sensory data with solid results.	Only uses 4-digit pins, low numbers of participants
	[37]	LibSVM, BN, RF	Shows the potential of UI elements (buttons, etc) in feature gathering	Low number of participants numbers.
Swiping	[38]	BN, KNN, RF	Method used to capture straight swipe motions, results show a heavy emphasis on sensors factor	EER of using sliders as authentication not within implementable range
	[39]	BN, RF, SVM	Showed validity of a hybrid authentication system	Open source library used was not up to par for voice models, no user study conducted
Keystroke Dynamics	[40]	MD, RF, GDA, SVM	Shows that keystroke dynamics can work as an authentication	Only used rough statistics

			method even with simple password like 1111	
	[41]	SVM, BN, KNN, "mean algorithm"	Shows that accuracy of sensor-based features outperforms keystroke dynamic features.	Low number of participants (20)
	[42]	SVM, DNN	Applied Deep Learning to a mobile authentication system	Small subject pool, simple use cases, no mention of energy usage from Deep Learning computational power
	[43]	N/A	Focuses on getting an overview on static keystroke dynamics, simplistic approach.	Registration process a chore, overly simplistic data obtained, no user study.
	[44]	CNN, RNN	Attempts a continuous authentication with usage of Deep Learning.	No details on the user study done (only noted experiments done on 75 users)
Gait	[45]	BN, NB, SVM, KNN, J48, RF	A more complete paper that shows abilities of different classifiers to read data from three actions	Training problem in not getting transparent data
	[46]	SVM	Shows that gait is able to be combined with other behavioral biometrics as a factor	No indication as to why only SVM is used as a classifier
Touch Dynamics	[46]	SVM	Develops a framework that runs as a background application to read user touch dynamics more transparently.	No indication as to why only SVM is used as a classifier
	[47]	J48, NB, JRip, BPNN, RBFN, PSO-RBFN	Shows the usage of different classifiers and the potential of a hybrid CA+IA system	Low number of participants, only one device used, framework based on surfing the internet instead of working with device.
Touch Gestures	[48]	1NN-DTW	Introduces framework for uncontrollable scenarios, recorded low energy consumption	Recorded accuracy rate not on par for industry standards, low number of participants.
	[49]	KNN	Presents a hybrid of physiological and behavioral biometric authentication without extra hardware.	EER not as expected, only using one type of device for an application designed for general usage.
	[50]	SVDE	Detailed paper on how features are collected and trained, introduces recording biometric of signatures with finger.	No reasoning as to why SVDE is used.
Others	[51] – application usage	N/A	Shows that behavioral usage of applications can be used as a behavioral biometric.	Static apps used, low participant count (2)
	[52] – phone placement recognition	KNN, J48, RF, MLP	A survey on the problems of phone placement/position recognition, and the potential of an accelerometer-only solution.	Self-compiled dataset is not generalized (i.e only for his problem statement)
	[53] – Wi-FI BSSID	N/A	Introduced the theory that Wi-Fi information captured by sensors could be used as a behavioral biometric.	Low participant count(17)

4. Hybrid Behavior-based Biometric Authentication Systems (HBAS)

Figure 2 shows HBAS system architecture flow of mobile user authentication system. The authentication process is run on the background without user acknowledgement. At the beginning, when the user taps the screen, the system will automatically collect tapping and swiping raw data of user. The out of range data are filtered from the collected raw data. From the collected tapping and swiping raw data, several features were obtained such as x-coordinate, y-coordinate, tapping time, releasing time, pressure, touched size and action. The feature results are stored into a database system and used to perform classification. The decision maker makes a final decision, label

whether the user is a legitimate user or an imposter based on the decision score. Figure 3 and Figure 4 shows how the tapping and swiping action is performed and the results are obtained.



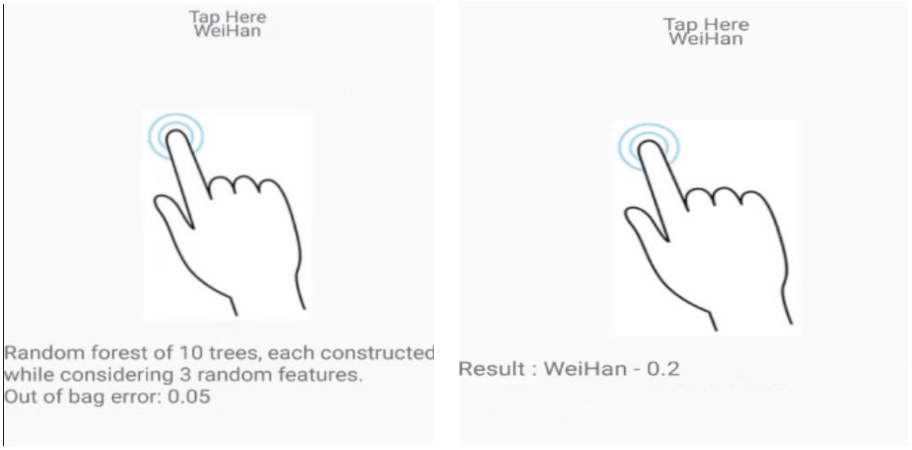


Fig. 3. Tapping action and Results.

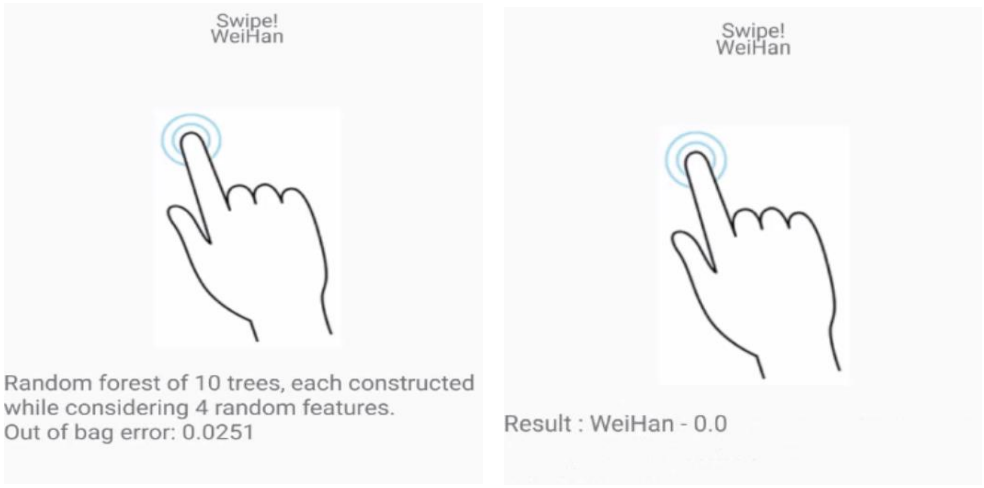


Fig. 4. Swiping action and Results.

For the dataset, a theory as to why the data has such a high correct rate of the data is via the area of where the user taps versus where an intruder taps. The user would concentrate his or her action at certain areas, while an intruder would be haphazardly performing the action at a random area to try and determine how the user performs the action. In the Figure 5, the user's data, colored in blue, is concentrated in one area, while the imposter's data, colored in red, is spread about the graph.

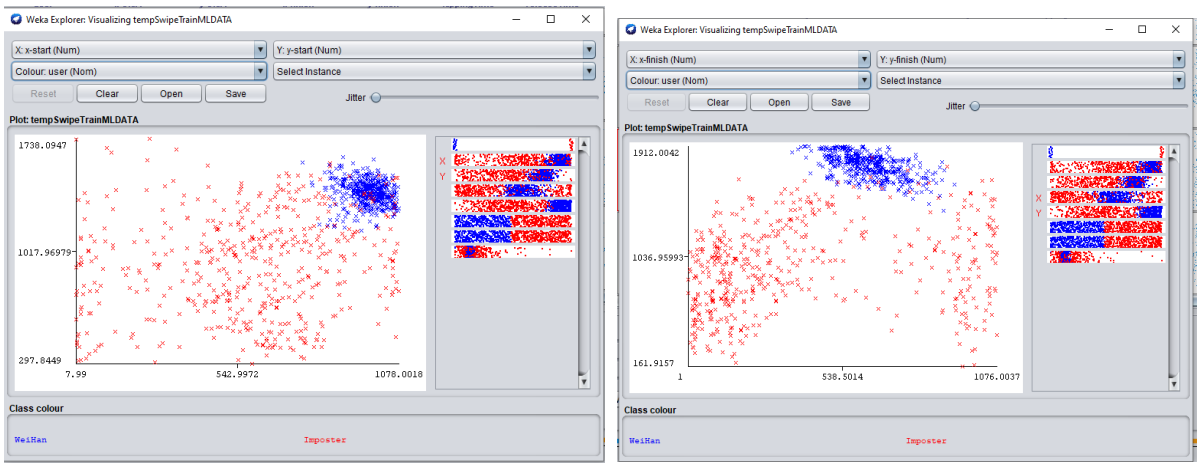


Fig. 5. Visualization of the user's Swipe Action

5. Results

Different amounts of classifiers are analyzed based on the application used to perform visualization of the dataset earlier. For the purpose of this section, three different datasets were made at fifty instances, one hundred instances, and two hundred instances for the training dataset, while a dataset of ten instances was to be used as the test dataset to compare against the training dataset. All four of these datasets will contain half the instances of the user's, while the other half are an intruder's.

Table 2: The dataset used for 10 test instances.

user	x-start	y-start	x-finish	y-finish	tappingTime	releaseTime	key_interval
WeiHan	1028.048	1422.259	630.4163	1900.01	1.59E+12	1.59E+12	142
WeiHan	969.1027	1446.247	632.4144	1801.062	1.59E+12	1.59E+12	138
WeiHan	1042.035	1386.278	694.3571	1827.048	1.59E+12	1.59E+12	180
WeiHan	995.0786	1350.297	567.4746	1849.037	1.59E+12	1.59E+12	149
WeiHan	1016.059	1411.265	641.4061	1833.045	1.59E+12	1.59E+12	193

Imposter	963.1082	1399.271	559.4819	1875.023	1.59E+12	1.59E+12	127
Imposter	722.3312	511.7335	178.8344	1504.217	1.59E+12	1.59E+12	170
Imposter	790.2683	199.8959	479.556	1689.12	1.59E+12	1.59E+12	190
Imposter	133.876	415.7835	835.2266	1454.243	1.59E+12	1.59E+12	191
Imposter	314.7086	328.8287	1044.033	1056.45	1.59E+12	1.59E+12	160

Eight classifiers will be used for this testing program, which are: Naive Bayes Updatable, Naive Bayes Multinomial, Hoeffding Tree, Random Forest, Decision Stump, Multilayer Perceptron, Naive Bayes and KStar.

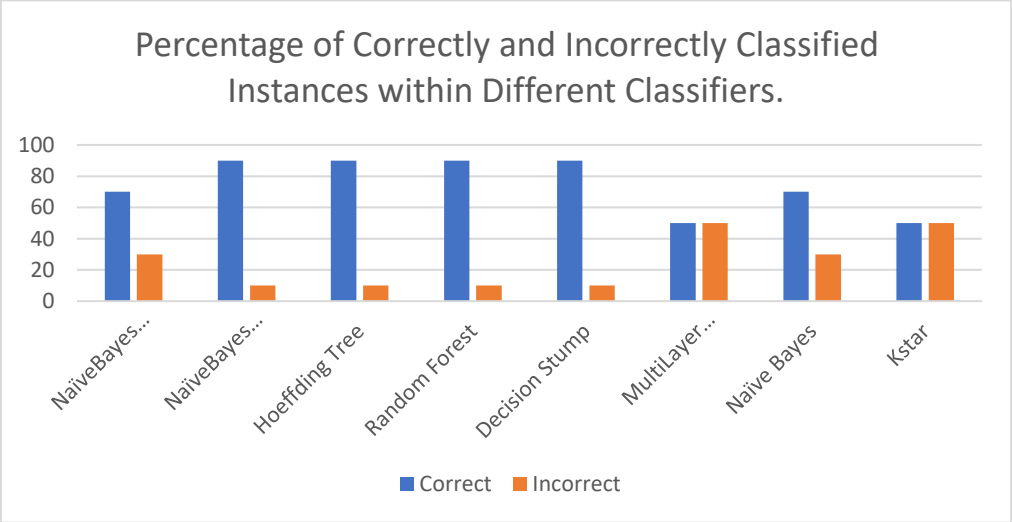


Fig. 6. The graph showing for 50 training data tested with 10 test data.

Here, we are able to see four classifiers at the top with a 90% in correctly classified instances, which are Naïve Bayes Multinomial, Hoeffding Tree, Random Forest, and Decision Stump. The second best are 70% correctly classified, which are Naïve Bayes Updatable, and Naïve Bayes. Finally, the worst performing are MultiLayer Perceptron and Kstar classifiers at 50% correctly classified.

The dataset used for 10 test instances.

Table 3 : The confusion matrix of 50 training data.

Classifier	**True Positive**	**True Negative**	**False Positive**	**False Negative**
Naïve Bayes Updatable	5	2	3	0
Naïve Bayes MultiNomial	5	4	1	0
Hoeffding Tree	5	4	1	0
Random Forest	5	4	1	0
Decision Stump	5	4	1	0
Multilayer Perceptron	0	5	5	0
Naïve Bayes	5	2	3	0
KStar	5	0	5	0

As of this table, again, the same classifiers with 90% correct classifying are to be of note here. Their only incorrectly classified is one false positive, which means that an intruder can enter.

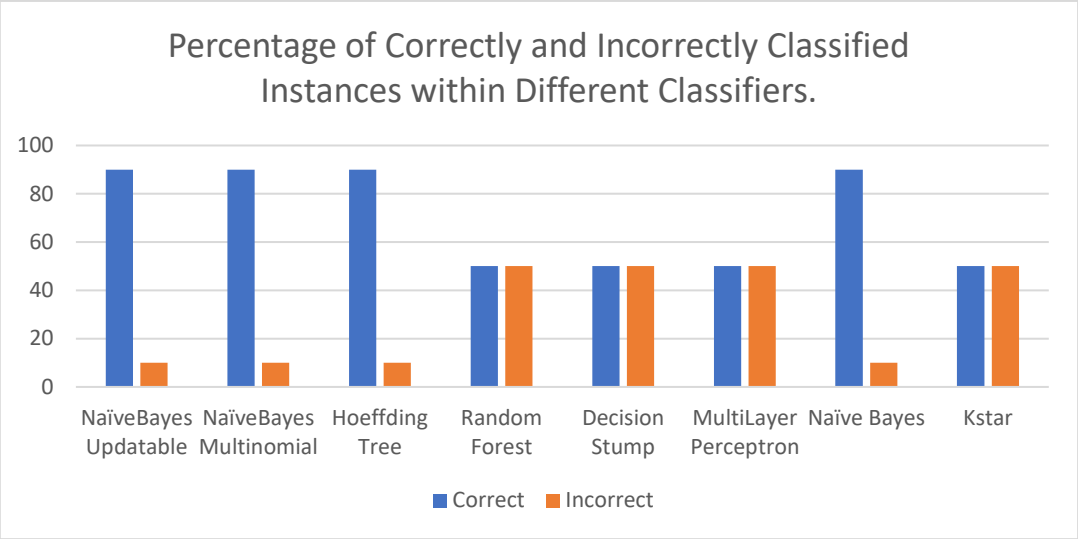


Fig.7. 100 training data tested with 10 test data.

An important thing to note here is that some classifiers either performed better (Naïve Bayes Updatable and Naïve Bayes went from 70% correctly classified to 90%) or went worse (Random Forest and Decision Stump went from 90% correctly classified to 50% correctly classified). Kstar and MultiLayer Perceptron classifiers showed no change, alongside Naïve Bayes Multinomial and Hoeffding Tree.

Table 4: Confusion matrix of one hundred training data alongside ten test data.

Classifier	True Positive	True Negative	False Positive	False Negative
Naïve Bayes Updatable	5	4	1	0
Naïve Bayes MultiNomial	5	4	1	0
Hoeffding Tree	5	4	1	0
Random Forest	5	0	5	0
Decision Stump	5	0	5	0
Multilayer Perceptron	5	0	5	0
Naïve Bayes	5	4	1	0
KStar	5	0	5	0

Here, the changes are reflected that the 90% correctly classified instances can now somewhat detect whenever it is an user or intruder. However, all of the 90% classifiers still have an 10% correct rate, that an intruder can still be marked as a false positive.

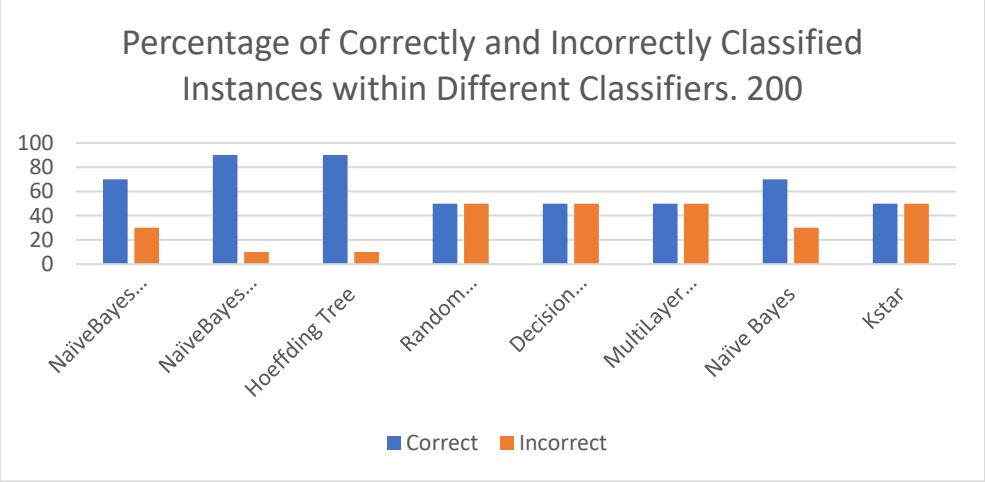


Fig. 8. 200 training data tested alongside 10 test data.

In two hundred training data, there would be seen to have little to no changes, only in decreasing correctly classifying instances. Both Naïve Bayes Updatable and Naïve Bayes, earlier both at 90% correctly classifying rate, have been decreased to 70%.

Table 4 : Confusion matrix of two hundred training data alongside 10 test data

Classifier	**True Positive**	**True Negative**	**False Positive**	**False Negative**
Naïve Bayes Updatable	5	2	3	0
Naïve Bayes MultiNomial	5	4	1	0
Hoeffding Tree	5	4	1	0
Random Forest	5	0	5	0
Decision Stump	5	0	5	0
Multilayer Perceptron	5	0	5	0
Naïve Bayes	5	2	3	0
KStar	5	0	5	0

Alongside what was explained earlier, Naïve Bayes Updatable and Naïve Bayes have both now began to accept more false positives from their true negatives, thus decreasing their correctly classified rate, from 1 to 3. As a result, from these tests performed on classifiers, the most consistent classifiers by far in all three of these tests would be Naïve Bayes Multinomial and Hoeffding Tree, consistently clocking in a 90% correctly classified rate. Naïve Bayes Updatable and Naïve Bayes went down in correct classifier rate from 90% to 70%, Random Forest and Decision Stump went from 90% to 50%, and KStar and MultiLayer Perceptron were the worst performers at a constant 50% correctly classified rate.

6. Conclusion

While the original planned features or actions had been deviated, an intended result had been achieved, which would be the testing process for determining the user. However, a major concern would be the somewhat inconsistent results in the confusion matrix testing. In theory, the confusion matrix should work better the more the amount of instances being fed into the classifier. To the lack of extensive knowledge in Machine Learning, perhaps a more experienced researcher would be able to pick this project up and further improve it. The novelty and contribution done by this project would be the implementation of two separate behavioral biometric features to be used as an authentication process. From the results shown, it is indeed possible to assume that behavioral biometrics could be considered a contender as an authentication method alongside physiological biometrics. Future work for this project has a wide variety of directions that are able to be approached from. As this project has the basic graphical user interface, it would be possible to improve the user experience to make it more attractive to users. It would also be possible to authenticate the user based on a behavioral biometric feature right after the user logs into the application, and allow or denies access based on the results of the testing. Other behavioral features could be explored, and other classifiers could be tested to further refine the accuracy and the confusion matrix of the testing model.

References:

[1]T. A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman and Y. Nam, "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," in IEEE Access, vol. 8, pp. 60539-60551, 2020, doi: 10.1109/ACCESS.2020.2983117.

[2]"Lock patterns are more predictable than we thought", Android Authority, 2020. [Online]. Available: https://www.androidauthority.com/lock-pattern-predictable-636267/.

[3]A. Aviv, F. Wolf and R. Kuber, "Comparing Video Based Shoulder Surfing with Live Simulation", Proceedings of the 34th Annual Computer Security Applications Conference, 2018. Available: 10.1145/3274694.3274702.

[4]M. Raza, M. Iqbal, M. Sharif and W. Haider, "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication", World Applied Sciences, vol. 19, no. 4, pp. 439-444, 2012.

[5]E. Chin, A. Felt, V. Sekar and D. Wagner, "Measuring user confidence in smartphone security and privacy", Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12, 2012. Available: 10.1145/2335356.2335358.

[6]"SplashData's Top 100 Worst Passwords of 2018 | TeamsID - Password Manager for Teams", TeamsID - Password Manager for Teams, 2018. [Online]. Available: https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018/.

[7]"Password Security Report: 83% of Users Surveyed Use the Same Password for Multiple Sites - Cyclonis", Cyclonis. [Online]. Available: https://www.cyclonis.com/report-83-percent-users-surveyed-use-same-password-multiple-sites/.

[8]M. Harris, S. Furnell and K. Patten, "Comparing the Mobile Device Security Behavior of College Students and Information Technology Professionals", Journal of Information Privacy and Security, vol. 10, no. 4, pp. 186-

202, 2014. Available: 10.1080/15536548.2014.974429.

[9]H. Crawford and K. Renaud, "Understanding user perceptions of transparent authentication on a mobile device", Journal of Trust Management, vol. 1, no. 1, p. 7, 2014. Available: 10.1186/2196-064x-1-7.

[10]H. Khan, U. Hengartner and D. Vogel, "Usability and Security Perceptions of Implicit Authentication: Convenient, Secure, Sometimes Annoying", Eleventh Symposium On Usable Privacy and Security, pp. 225-239, 2015.

[11]C. Bevan and D. Fraser, "Different strokes for different folks? Revealing the physical characteristics of smartphone users from their swipe gestures", International Journal of Human-Computer Studies, vol. 88, pp. 51-61, 2016. Available: 10.1016/j.ijhcs.2016.01.001.

[12]N. Zheng, K. Bai, H. Huang and H. Wang, "You Are How You Touch: User Verification on Smartphones via Tapping Behaviors", 2014 IEEE 22nd International Conference on Network Protocols, pp. 221-232, 2012.

[13]E. Miluzzo, A. Varshavsky, S. Balakrishnan and R. Choudhury, "Tapprints", Proceedings of the 10th international conference on Mobile systems, applications, and services - MobiSys '12, 2012. Available: 10.1145/2307636.2307666

[14]M. Li, H. Wang, B. Guo and Z. Yu, "Extraction of Human Social Behavior from Mobile Phone Sensing", Active Media Technology, pp. 63-72, 2012. Available: 10.1007/978-3-642-35236-2_7

[15]S. McGlaun, "Apple Face ID Epic Fail Allows Two Unrelated Chinese Women Access To iPhone X", HotHardware, 2020. [Online]. Available: https://hothardware.com/news/apple-face-id-epic-fail-allows-two-unrelated-chinese-women-access-to-iphone-x. [Accessed: 28- May- 2020].

[16]A. Greenberg, "Watch a 10-Year-Old Beat Apple's Face ID on His Mom's iPhone X", Wired, 2017. [Online]. Available: https://www.wired.com/story/10-year-old-face-id-unlocks-mothers-iphone-x/. [Accessed: 28- May- 2020].

[17] W. Meng, D. Wong, S. Furnell and J. Zhou, "Surveying the Development of Biometric User Authentication on Mobile Phones", IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1268-1293, 2015. Available: 10.1109/comst.2014.2386915.

[18]C. Bhagavatula, B. Ur, K. Iacovino, S. Kywe, L. Cranor and M. Savvides, "Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption", Proceedings 2015 Workshop on Usable Security, 2015. Available: 10.14722/usec.2015.23003 [Accessed 28 May 2020].

[19] Almulhim, M., Islam, N., & Zaman, N. (2019). A lightweight and secure authentication scheme for IoT based e-health applications. International Journal of Computer Science and Network Security, 19(1), 107-120.

[20]K. Sundararajan and D. Woodard, "Deep Learning for Biometrics", ACM Computing Surveys, vol. 51, no. 3, pp. 1-34, 2018. Available: 10.1145/3190618 [Accessed 28 May 2020].

[21]J. Spooren, D. Preuveneers and W. Joosen, "Leveraging Battery Usage from Mobile Devices for Active Authentication", Mobile Information Systems, vol. 2017, pp. 1-14, 2017. Available: 10.1155/2017/1367064 [Accessed 28 May 2020].

[22]E. Redmiles, S. Kross and M. Mazurek, "How I Learned to be Secure", Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016. Available: 10.1145/2976749.2978307 [Accessed 28 May 2020].

[23]K. Isbister, N. Memon and N. Sae-Bae, "BOMETRIC-RCH GESTURES FOR AUTHENTICATION ON MULTI-TOUCH DEVICES", US 9,147,059 B2, 2015.

[24]J. Nader, A. Alsadoon, P. Prasad, A. Singh and A. Elchouemi, "Designing Touch-Based Hybrid Authentication Method for Smartphones", Procedia Computer Science, vol. 70, pp. 198-204, 2015. Available: 10.1016/j.procs.2015.10.072 [Accessed 28 May 2020].

[25] P. Cohen, "Macworld Expo Keynote Live Update: Introducing the iPhone", Macworld, 2007. [Online]. Available: https://www.macworld.com/article/1054764/liveupdate.html. [Accessed: 28- May- 2020].

[26] "Announcing the Android 1.0 SDK, release 1", Android Developers Blog, 2008. [Online]. Available: https://android-developers.googleblog.com/2008/09/announcing-android-10-sdk-release-1.html. [Accessed: 28- May- 2020].

[27] N. Zaman and F. A. Almusalli, "Review: Smartphones power consumption & energy saving techniques," 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT), Karachi, 2017, pp. 1-7, doi: 10.1109/ICIEECT.2017.7916593.

[28] "Hard Questions: What Data Does Facebook Collect When I'm Not Using Facebook, and Why? - About Facebook", About Facebook, 2018. [Online]. Available: https://newsroom.fb.com/news/2018/04/data-off-facebook/. [Accessed: 28- May- 2020].

[29] "Endpoint Protection - Symantec Enterprise", Symantec.com, 2012. [Online]. Available: https://www.symantec.com/connect/blogs/introducing-symantec-smartphone-honey-stick-project. [Accessed: 28- May- 2020].

[30] C. Song, A. Wang, K. Ren and W. Xu, "EyeVeri: A secure and usable approach for smartphone user authentication", IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, 2016. Available: 10.1109/infocom.2016.7524367 [Accessed 28 May 2020].

[31] L. Birgale and M. Kokare, "Iris Recognition Using Ridgelets", Journal of Information Processing Systems, vol. 8, no. 3, pp. 445-458, 2012. Available: 10.3745/jips.2012.8.3.445 [Accessed 28 May 2020].

[32] C. Galdi, M. Nappi, D. Riccio and H. Wechsler, "Eye movement analysis for human authentication: a critical survey", Pattern Recognition Letters, vol. 84, pp. 272-283, 2016. Available: 10.1016/j.patrec.2016.11.002 .

[33] P. Samangouei, V. Patel and R. Chellappa, "Facial attributes for active authentication on mobile devices", Image and Vision Computing, vol. 58, pp. 181-192, 2017. Available: 10.1016/j.imavis.2016.05.004.

[34] A. Jain, S. Prabhakar and S. Chen, "Combining multiple matchers for a high security fingerprint verification system", Pattern Recognition Letters, vol. 20, no. 11-13, pp. 1371-1379, 1999. Available: 10.1016/s0167-8655(99)00108-7 .

[35] A. Jain, A. Ross and K. Nandakumar, Introduction to biometrics. New York: Springer, 2011.

[36] A. Buriro, B. Crispo, F. Del Frari and K. Wrona, "Touchstroke: Smartphone User Authentication Based on Touch-Typing Biometrics", New Trends in Image Analysis and Processing -- ICIAP 2015 Workshops, pp. 27-34, 2015. Available: 10.1007/978-3-319-23222-5_4

[37]P. Saravanan, S. Clarke, D. Chau and H. Zha, "LatentGesture", Proceedings of the Second International Symposium of Chinese CHI on - Chinese CHI '14, 2014. Available: 10.1145/2592235.2592252.

[38] M. Antal and L. Szabó, "Biometric Authentication Based on Touchscreen Swipe Patterns", Procedia Technology, vol. 22, pp. 862-869, 2016. Available: 10.1016/j.protcy.2016.01.061.

[39] A. Buriro, B. Crispo, F. Del Frari, J. Klardie and K. Wrona, "ITSME: Multi-modal and Unobtrusive Behavioural User Authentication for Smartphones", Technology and Practice of Passwords, pp. 45-61, 2016. Available: 10.1007/978-3-319-29938-9_4 .

[40] G. Ho, "Tapdynamics: strengthening user authentication on mobile phones with keystroke dynamics", Technicalreport, StanfordUniversity, 2014.

[41] C. Giuffrida, K. Majdanik, M. Conti and H. Bos, "I Sensed It Was You: Authenticating Mobile Users with Sensor-Enhanced Keystroke Dynamics", Detection of Intrusions and Malware, and Vulnerability Assessment, pp. 92-111, 2014. Available: 10.1007/978-3-319-08509-8_6 .

[42] M. Almulhim and N. Zaman, "Proposing secure and lightweight authentication scheme for IoT based E-health applications," 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon-si Gangwon-do, Korea (South), 2018, pp. 481-487, doi: 10.23919/ICACT.2018.8323802.

[43] J. Miya, M. Bhatt, M. Gupta and M. Anas, "A Two Factor Authentication System for Touchscreen Mobile Devices Using Static Keystroke Dynamics and Password", 2017.

[44] L. Xiaofeng, Z. Shengfei and Y. Shengwei, "Continuous authentication by free-text keystroke based on CNN plus RNN", Procedia Computer Science, vol. 147, pp. 314-318, 2019. Available: 10.1016/j.procs.2019.01.270.

[45] A. Buriro, B. Crispo and M. Conti, "AnswerAuth: A bimodal behavioral biometric-based user authentication scheme for smartphones", Journal of Information Security and Applications, vol. 44, pp. 89-103, 2019. Available: 10.1016/j.jisa.2018.11.008.

[46] C. Bo, L. Zhang, T. Jung, J. Han, X. Li and Y. Wang, "Continuous user identification via touch and movement behavioral biometrics", 2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC), 2014. Available: 10.1109/pccc.2014.7017067.

[47]J. Nader, A. Alsadoon, P. Prasad, A. Singh and A. Elchouemi, "Designing Touch-Based Hybrid Authentication Method for Smartphones", Procedia Computer Science, vol. 70, pp. 198-204, 2015. Available: 10.1016/j.procs.2015.10.072.

[48] Zaman, N., & Ahmad, M. (2017). Towards the evaluation of authentication protocols for mobile command and control unit in healthcare. Journal of Medical Imaging and Health Informatics, 7(3), 739-742.

[49] C. Koong, T. Yang and C. Tseng, "A User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices", The Scientific World Journal, vol. 2014, pp. 1-12, 2014. Available: 10.1155/2014/781234.

[50] M. Shahzad, A. Liu and A. Samuel, "Behavior Based Human Authentication on Touch Screen Devices Using Gestures and Signatures", IEEE Transactions on Mobile Computing, vol. 16, no. 10, pp. 2726-2741, 2017. Available: 10.1109/tmc.2016.2635643.

[51] S. Mohammed, A. Mohd and M. Singh, "A Secure Mobile App Solution Using Human Behavioral Context and Analytic Hierarchy Process", Procedia Computer Science, vol. 72, pp. 434-445, 2015. Available: 10.1016/j.procs.2015.12.124

[52] O. Incel, "Analysis of Movement, Orientation and Rotation-Based Sensing for Phone Placement Recognition", Sensors, vol. 15, no. 10, pp. 25474-25506, 2015. Available: 10.3390/s151025474

[53] R. Kobayashi and R. Yamaguchi, "A Behavior Authentication Method Using Wi-Fi BSSIDs around Smartphone Carried by a User", 2015 Third International Symposium on Computing and Networking (CANDAR), 2015. Available: 10.1109/candar.2015.45.