SwipeAuth: Swipe-based Implicit Continuous User Authentication

Pragyan Mehrotra
Indraprastha Institute of Information Technology, Delhi
pragyan18168@iiitd.ac.in

Abstract

Dependency on electronic devices has increased exponentially in the past decade. Smartphones are extensively used for a plethora of activities ranging from social media to online banking. The nature of information being stored has become more sensitive and security-critical. Still, standard authentication techniques used in mobile phones today are limited to passwords, PINs, and swipe patterns, which are highly vulnerable to eavesdropping and smudge attacks. Hence, we propose SwipeAuth, a swipe-based implicit continuous user authentication framework. It utilizes the micro-movements and orientational deflections the smartphone undergoes while a user swipes the touch screen. We propose a novel method of combining and utilizing the contextual information provided by the consecutive swipes. We achieved an astonishing 98.18% True Acceptance rate and 99.68% True rejection rate. Moreover, the classifier used is the Random Forest Classifier, which is parallelizable and has a very low computational overhead. It can run smoothly in the background without hampering any system processes providing continuous authentication to the user.

Keywords - Implicit Authentication, Behavior-based Authentication, Swipe-based, Machine Learning, Micro Movements

1. Introduction

With the recent technological advancements and increasing communication services usage, mobile phones have become an everyday staple in billions of people's lives. As dependency on mobile phones is increasing, the nature of data being stored is becoming more sensitive. Thus, data security and privacy is a growing concern.

Typical authentication mechanisms like PIN, passwords, and lock patterns are fast and easy authentication methods commonly used in mobile phones. However, they are highly vulnerable to shoulder surfing and smudge attacks. Repeatedly putting in passwords for authentication is frustrating and inconvenient for the everyday user. Many users put simple passwords like 1234, 4321, etc., for convenience, which can be hacked easily by an adversary. Another concern with typical authentication mechanisms is that there is no guarantee that once a phone is unlocked, it is being used by a legitimate user. For ease of access, mobile users set a considerable wait time before a phone is re-locked. An adversary with unintended access to the device can cause notable damage to the privacy of the user.

Behavior-based authentication techniques depend on a user's mannerisms or actions. Nowadays, mobile devices are equipped with multiple sensors and apps to provide useful data on user behavior. The computation capabilities of computer devices are also increasing, which can be utilized for authentication.

Thus, we propose SwipeAuth, a framework that can efficiently authenticate a user based on their micro-movements. We utilize the user's swipe patterns to provide continuous user authentication in integration with the sensor data. The paper's main contribution is utilizing the contextual information achieved by consecutive swipes using machine learning classification models. Upon evaluation, we observe that the Random Forest classifier achieves the best performance and is an extremely efficient classifier for SwipeAuth. It is parallelizable and can be easily incorporated into mobile devices, making our solution scalable to the real world.

We discuss the related literature briefly in Section 2. Section 3 provides an overview of the traditional authentication mechanisms and some of the latest categories used in continuous mobile authentication. A detailed explanation of our methodology and highlights our contribution through the paper is mentioned in Section 4. We report our results in Section 5 and conclude the paper in Section 6.

2. Related Work

Many implicit authentication techniques have been proposed in the related literature. [1] proposed a mechanism using the UMDAA-02 dataset for multi-modal user authentication. They utilized the front camera, touch sensor, and the location service to perform continuous user authentication. They achieved an equal error rate (EER) of 22.1% with 10-fold cross-validation using Random Forest.

[2] proposed a method using touch analytics, which employed around 30 useful features extracted from a user's swipe. Utilizing the proposed features and SVM and K-NN, they achieved an EER of 2% to 3% with 5-fold Cross-validation on the training data. [3] proposed a model (Random Forest Classifier) utilizing X-Y coordinates, speed of motion, and pressure and achieved a False Acceptance Rate (FAR) of 4.66% and a False Rejection Rate (FRR) of 0.13%.

A context-aware implicit authentication mechanism utilizing touch, accelerometer, gyroscope, and magnetometer data to classify users while they are inputting there PIN/passwords [4]. They utilize the orientation deflections and micro-movements of the phone to build a classifier. They used a One-Class SVM (OC-SVM) to fuse the different features' results and obtain a fascinating 0.00071% (EER). However, they consider the authentication only when the user is inputting the PIN/password of the device.

The authors in [5] explored a mechanism to utilize consecutive swipes for authentication of the user. They proposed a framework to aggregate the scores of successive swipes by averaging the score and returning the class with the closest score. Their mechanism was only limited to the swipes recorded during the swiping of the screen lock of the phone. Using this technique and the RF classifier, they could bring down 4% EER of a single swipe to 0.2% EER with consecutive swipes.

Our study aims to provide a classifier able to utilize the swipe gesture and the micro-movements the phone encounters when the user swipes the mobile phone to authenticate the user continuously. We also explore the classification metrics using consecutive swipes. Our model focuses on authenticating the user throughout their usage session.

3. Authentication Mechanisms

There are three fundamental behavior-based authentication mechanisms categorized on the type of information they extract and use. Of course, there are multiple hybrid models of the following categories; however, we just brief on the type of behavioral information that we can extract from a smartphone device being utilized by a user.

A. Event-Based User Authentication

Users perform various activities on their phones, such as accessing apps, making a phone call, messaging a friend, browsing a webpage, etc. These activities generate multiple events, contributing a good chunk to the user's mobile usage pattern. These events are a crucial feature while considering a user behavior model. Users develop particular mannerisms concerning when they perform an event, frequency of their usage, and duration for the event. It acts as an identifier to mark suspicious activity if an illegitimate user accesses their phone [6]. This is known as event-based mobile authentication.

B. Sensor-Based User Authentication

Modern smartphone devices are equipped with sensors capable of tracking the device's motion and orientation, along with some surrounding traits like ambient noise and light. These sensors are precise and provide reliable data that can be utilized for continuous authentication [7]. Using this data, a user can be verified (sensor-based mobile authentication).

C. Gesture-Based User Authentication

Touch screens are the most common and user-friendly feature of smartphones today. They have revolutionized the way humans interact with technology, providing an interface adopted by most electronic devices [8]. When the user interacts with the touch screen using their fingers in a swiping, pinching, dragging, or spreading motion, it is known as a gesture. Gesture-based mobile authentication utilizes it as a feature to distinguish between a legitimate and an illegitimate feature.

We propose a hybrid sensor-based and gesture-based mobile authentication mechanism to propose a reliable and robust verification technique.

4. Methodology

4.1. Framework Overview

Figure 1 represents the overall framework of the proposed authentication mechanism. While a user is interacting with the smartphone, the phone continuously collects data, cleans it, and extracts relevant features described in the next few subsections. Afterward, a pre-trained classifier is applied, determining if a user is legitimate or not and takes action accordingly.

4.2. Dataset Description and Preprocessing

We utilized the hand movement, orientation, and grasp dataset (H-MOG), which consists of 100 users spanning through 24 sessions. Each session was of 5-15 minutes where a user could either (i) sit or (ii) walk. When using the phone, our actions and micro-movements are much different while performing these activities [9]. Thus, the dataset was divided into two parts based on the position (sitting or walking), and the evaluation was done separately.

A phone can have three different types of orientation (i) 0: Portrait and no rotate, (ii) 1: device rotated 90 degrees counter-clockwise, and (iii) 3: device rotated 90 degrees clockwise. For our data, we only consisted of instances with orientation 0. The sessions were split into three categories, (i) reading, (ii) writing, and (iii) map navigation

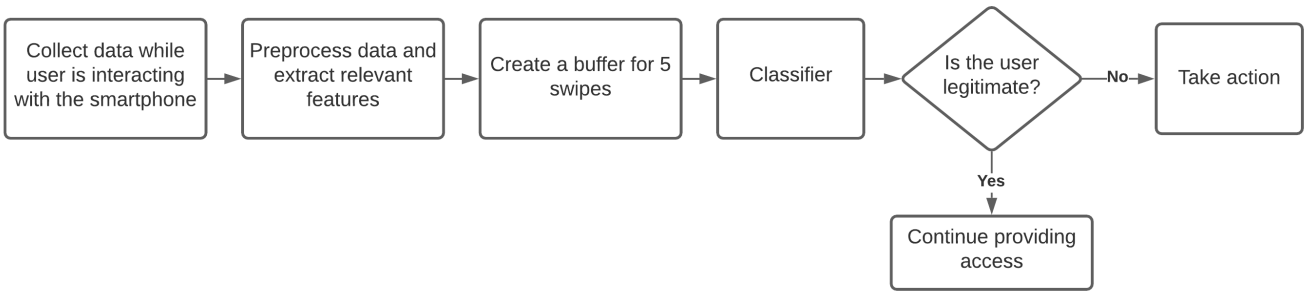


Figure 1: Authentication Mechanism Framework

(eight each). The data collection app could capture the slightest micro-movements essential for continuous mobile authentication. It collected nine major categories of data:

1. Accelerometer
2. Gyroscope
3. Magnetometer
4. Raw touch event
5. Tap gesture
6. Scale gesture
7. Scroll gesture
8. Fling gesture
9. Keypress on the virtual keyboard

Since our project focuses on swipe-based mobile authentication, we shortlisted four categories to extract features: Raw touch event, Accelerometer, Gyroscope, and Magnetometer.

4.2.1 Raw touch event

For our problem, we considered the single-touch events. It had attributes like action (UP, DOWN, or MOVE), X and Y coordinate of the touch location, touch pressure, and contact size.

4.2.2 Accelerometer

It measures the acceleration forces of the phone in the 3-D space. Thus, it provides a mapping of the acceleration across the X, Y, and Z-axis. This value varies from person to person, acting as a unique identifier in user authentication.

4.2.3 Gyroscope

It helps in determining the orientation of the phone by measuring the angular rotational velocity. It measures the rate of change of rotational velocity across the X, Y, and Z-axis using the same coordinate system as the accelerometer.

4.2.4 Magnetometer

It is used for measuring the magnetic field across the X, Y, and Z-axis. Usually, compass applications in smartphones utilize this sensor to provide accurate results.

4.3. Feature Extraction

4.3.1 Raw Touch Event

Each swipe S_i is a culmination of N touch events. It can be represented as a tuple given below.

$$S_i = (X, Y, P, C, T)$$

where X, Y, P, C, T are arrays of size N representing pressure values, contact size values, X-coordinate, Y-coordinate, and time of the touch events respectively. Figure 2 visualizes the swipes of two users while performing different activities. Using a swipe S_i, we can extract the Pairwise X-axis Velocity V_X defined as:

$$V_X = \frac{X_i - X_{i-1}}{T_i - T_{i-1}} \forall i \in [0, 1, 2, ...N)$$

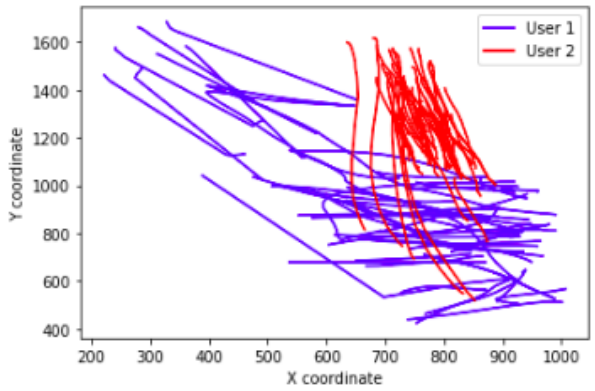
where V_X is an array of size $N - 1$. V_Y can be extracted similarly. We can get the Pairwise X-axis accelerations as follows:

$$A_X = \frac{V_i - V_{i-1}}{T_i - T_{i-1}} \forall i \in [0, 1, 2, ...N - 1)$$

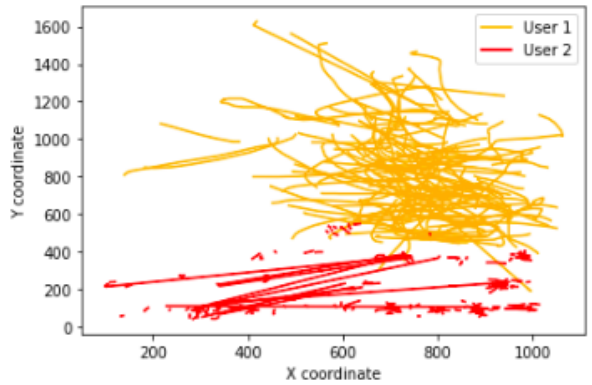
where A_X is an array of size $N - 2$. A_Y can be defined similarly. We can also define the length of the swipe, l, as follows:

$$l = \sum_{i=1}^{N-1} \sqrt{(X_{i-1} - X_i)^2 + (Y_{i-1} - Y_i)^2}$$

We used raw touch events to extract 37 features describing each swipe. We omitted swipes with extremely small length ($l < 0.01$) or very few data points describing the swipe ($N \leq 7$) as they could potentially be representing



(a) Swipe patterns of two users while Sitting



(b) Swipe patterns of two users while Walking

Figure 2: Distinction in Swipe Patterns of different users

a tap event rather than a swipe event. Table 1 provides a brief description of the extracted touch features. We used the touch features given in [9] in culmination with few additional features to improve performance.

4.3.2 Sensor Data

The inertial sensors' orientation sensitivity affects the classification performance [10]. Thus, we add another dimension M for all the sensors, i.e., accelerometer, gyroscope, and magnetometer, to avoid the interference caused by sensitivity. M is simply the magnitude of the vector representing the X, Y, Z readings of the inertial sensors.

$$M = \sqrt{X^2 + Y^2 + Z^2}$$

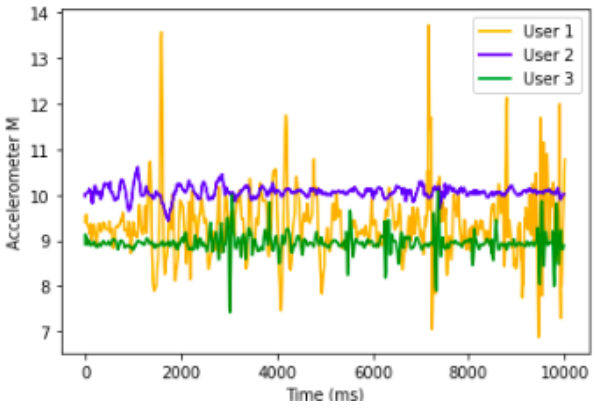
We extract the sensor readings only during the interval of the swipes. Meaning, for each swipe S_i, we consider the sensor readings belonging to only the time interval the swipe lasted i.e. from $S_i[T_0]$ till $S_i[T_{N-1}]$. We calculated 16 features from each of the sensors [9]. Table 2 provides a brief description of the extracted features. Figure 3 visualizes the calculated M values from different users, highlighting the difference and reiterating authentication feasibility using sensor data.

Feature	Description
swipe_duration	$T_{end} - T_{start}$
startX	X_0
startY	Y_0
endX	X_{N-1}
endY	Y_{N-1}
minVx	$min(V_x)$
maxVx	$max(V_x)$
minVy	$min(V_y)$
maxVy	$max(V_y)$
meanVx	Average of V_x
meanVy	Average of V_y
stdVx	Standard deviation of V_x
stdVy	Standard deviation of V_y
varVx	Variance of V_x
varVy	Variance of V_y
minAx	$min(A_x)$
minAy	$min(A_y)$
maxAx	$max(A_x)$
maxAy	$max(A_y)$
meanAx	Average of A_x
meanAy	Average of A_y
stdAx	Standard deviation of A_x
stdAy	Standard deviation of A_y
varAx	Variance of A_x
varAy	Variance of A_y
minP	$min(P)$
maxP	$max(P)$
meanP	Average of P
stdP	Standard deviation of P
varP	Variance of P
minC	$min(C)$
maxC	$max(C)$
meanC	Average of C
stdC	Standard deviation of C
varC	Variance of C
l	Length of the swipe
d	Direct end-to-end distance of swipe

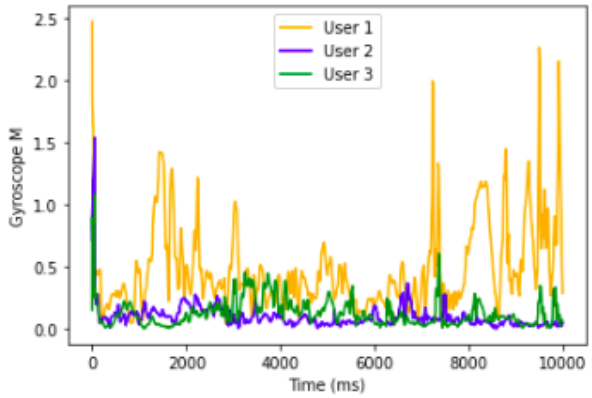
Table 1: Raw Touch Event Features

Indices	Features	Features	Features	Features
$1-4$	meanX	meanY	meanZ	meanM
$5-9$	stdX	stdY	stdZ	stdM
$10-13$	skewX	skewY	skewZ	skewM
$13-16$	kurtX	kurtY	kurtZ	kurtM

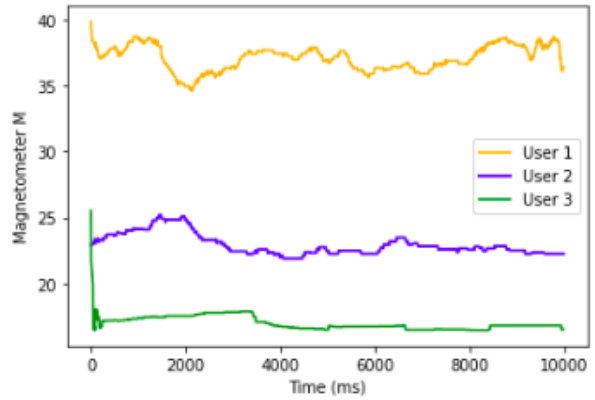
Table 2: Sensor Features



(a) Accelerometer Plot



(b) Gyroscope Plot



(c) Magnetometer Plot

Figure 3: Distinction in sensor values of different users

4.3.3 Activity

We one-hot encoded the activities (reading, writing, and map navigation) and used them in our final feature vector. One feature corresponding to each activity, 0 and 1 describing the absence and presence of the activity, respectively.

4.3.4 Final feature vector

The final feature vector for each swipe consists of 88 dimensions. It directly concatenates the 37 dimension feature vector from the raw touch events, 16 dimension feature vector from each of the three sensors (Accelerometer, Gyroscope, and Magnetometer), and three dimensions from the one-hot encoded activities. Considering multiple consecutive swipes increases the context of the information, improving the performance. We consider the data of five consecutive swipes as our input vector (swipes 1-5, 2-6, and so on) for our classification model. Thus, the feature vector size for the classification model becomes $88 * 5 = 440$.

4.4. Classifier Training

In this section, we describe our authentication mechanism. As described in the previous section, the final feature vector of 88 dimensions was used to train five classification models. K-Nearest Neighbors (KNN), Random Forest (RF), Gaussian Naive Bayes (GNB), Support vector machine classifier (SVC), and Multi-layer perceptron (MLP) were applied for classifying the user. We split the dataset into walking and sitting (discussed in section 4.2) and trained the classifier on each type of data separately. We picked up one random user from the dataset as the legitimate user (class 1), which were around 2000 samples, and from the other 49 users, we picked up 40 random swipes (class 0) from each user to avoid class imbalance. We also trained the above models for the consecutive swipes vectors and compared the following section results. We evaluate the performance of the mentioned algorithms on the training set in section 5.

4.5. Evaluation Metric

True Acceptance Rate: The fraction of times the legitimate user was authenticated out of the total times it authenticated.

True Rejection Rate: The fraction of times the adversary was locked out or correctly identified.

False Acceptance Rate: The fraction of times the adversary was granted access.

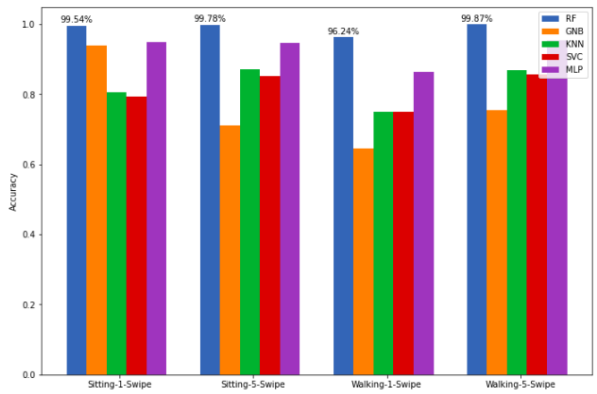
False Rejection Rate: The fraction of times the legitimate user was locked out of the device.

Accuracy: The fraction of correct predictions upon the total predictions made.

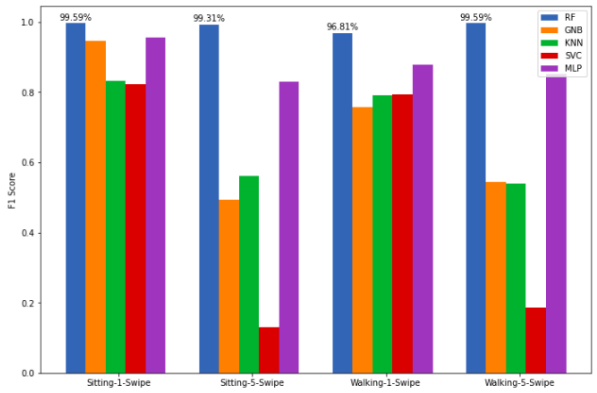
Macro F1 score: It's a measure of how good is the classification of each class. It's the harmonic mean of precision and recall.

5. Results

In this section, we evaluate our proposed framework. We train and compare the performance of the algorithms mentioned in Section 4.4. Random Forest achieved the best



(a) Accuracy Plot



(b) F1 Score Plot

Figure 4: Classifiers Evalaluation

scores out of all the models in all the cases as visible in Figure 4 and Table 3. It is imperative from the scores obtained that RF outperforms all the other classifiers in question. Since Random Forest is parallelizable, it can provide an efficient solution for continuous user authentication as it can run in the background with minimal computational costs. We can observe that the consecutive swipe performed much better than a single swipe. Thus, the RF can detect an intrusion very effectively with five consecutive swipes of the adversary. Also, the Random Forest has an extremely high true acceptance rate-making SwipeAuth feasible for deployment and used on a larger scale.

Models	Accuracy	TAR	TRR	F1
RF	99.87	99.18	99.68	99.59
GNB	75.36	93.22	72.00	54.51
KNN	86.90	48.23	94.18	53.85
SVC	85.66	10.29	99.84	18.53
MLP	95.45	83.19	97.75	85.27

Table 3: Walking-5-swipe

6. Conclusion

Mobile Phones are ubiquitous in a user's everyday life. The unreliability and tediousness of typical authentication methods like Passwords, PINs, and Patterns make it imperative to introduce a novel, secure, and robust continuous authentication techniques. Behavioral traits unique to the individual present themselves as essential tools in realizing this goal.

In this paper, we propose SwipeAuth, which utilizes the swipe, accelerometer, gyroscope, and magnetometer data for classifying the users based on their micro gestures observed while swiping. We used the HMOG dataset to perform binary classification with the data of 50 users. We consider consecutive swipes to capture more contextual information than a single swipe model and see a performance improvement.

We wish to add more contextual information to the classifier in the future. In this case, we considered only three activities. However, we want to extend this model to have higher contextual information by adding compatibility for more activities. A user may use it for other tasks in an uncontrolled environment and in many more complex positions than sitting or walking. Thus, we wish to increase the context and robustness of SwipeAuth in our future work.

References

[1] U. Mahbub, S. Sarkar, V. M. Patel, and R. Chellappa, "Active user authentication for smartphones: A challenge data set and benchmark results," pp. 1–8, 2016.

[2] 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 Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 136–148, 2013.

[3] T. Feng, Z. Liu, K. A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, "Continuous mobile authentication using touchscreen gestures," 2012.

[4] R. Wang and D. Tao, "Context-aware implicit authentication of smartphone users based on multi-sensor behavior," *IEEE Access*, vol. 7, pp. 119654–119667, 2019.

[5] M. Antal and L. Z. Szabó, "Biometric authentication based on touchscreen swipe patterns," *Procedia Technology*, vol. 22, pp. 862 – 869, 2016. 9th International Conference Interdisciplinarity in Engineering, INTER-ENG 2015, 8-9 October 2015, Tirgu Mures, Romania.

[6] Y. Ashibani and Q. H. Mahmoud, "A Behavior-Based Proactive User Authentication Model Utilizing Mobile Application Usage Patterns," vol. 11489 LNAI, 2019.

[7] A. Acien, A. Morales, R. Vera-Rodriguez, J. Fierrez, and R. Tolosana, "Multi lock: Mobile active authentication based on multiple biometric and behavioral patterns," 2019.

[8] M. Shahzad, A. X. 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, 2017.

[9] "Answerauth: A bimodal behavioral biometric-based user authentication scheme for smartphones," *Journal of Information Security and Applications*, vol. 44, pp. 89 – 103, 2019.

[10] M. Ehatisham-ul Haq, M. A. Azam, J. Loo, K. Shuang, S. Islam, U. Naeem, and Y. Amin, "Authentication of smartphone users based on activity recognition and mobile sensing," *Sensors*, vol. 17, p. 2043, Sep 2017.