Dynamic Time Warping Approach for User Authentication of Smartphones Using Single-handed Shakes

Athithyaa Selvam
Department of Computer Science and Engineering,
Sri Venkateswara College of Engineering,
Sriperumbudur Tk, India
athithyaaselvam@gmail.com

Anandrajalu R
Department of Computer Science and Engineering,
Sri Venkateswara College of Engineering,
Sriperumbudur Tk, India
arajalu@gmail.com

Bharat Chandra C
Department of Computer Science and Engineering,
Sri Venkateswara College of Engineering,
Sriperumbudur Tk, India
bharatchandra95@gmail.com

Rajeswari Natarajan
Assistant Professor,
Department of Computer Science and Engineering,
Sri Venkateswara College of Engineering,
Sriperumbudur Tk, India
raji@svce.ac.in

Abstract:-An immense amount of private information is stored in smartphones. In order to secure information from being tapped a new form of authentication mechanism is needed. Previous unlock mechanism like pattern authentication or code based authentication are vulnerable as they are not using a person's unique attribute. In this paper, we propose a method for unlocking phones based on user's handshakes. The gesture sensors and the proximity sensors help us capture the unique handshake of the person. This unlock mechanism makes it harder for the attacker to reproduce the same type of handshake even if he observes the shaking pattern.

Keywords: *Unlock Mechanism, DTW, Fast DTW, Accelerometer.*

*****

I. INTRODUCTION

The usage of smartphones is booming in the last decade. The vigorous growth is due to the powerful computing capabilities, large storage capacity and personal assistance instead of just making telephone calls or sending message. The vast functionalities and the comfort smartphones provide helped people access their personal information like bank accounts, sending/receiving emails, mobile payment, shopping, photos, stocks through phones.

Screen locker is a cardinal utility that prevents smartphones from unintentional/unauthorized operations and secures the personal information. The Android phones and the Apple iPhone can lock themselves automatically after being idle for a short period. This mechanism can protect the privacy of the users. The existing approaches are password, pattern and biometric authorization. These approaches are not well supported due to deficiency of security. IPhones generally use a four digit password which can be cracked by brute force attack. Android devices use a nine point geometric pattern. The short password or simple patterns are easy to use but they are vulnerable to shoulder surfing attacks. In addition short password and simple patterns can be guessed by the smudges left on the screen. Long passwords can be adopted to prevent these attacks but it usually give the users an awful experience every time they unlock the phone. Biometrics like fingerprint recognition, face recognition, voice recognition are being used but these unlock mechanism achieve satisfactory performance. These unlocking mechanism frequently suffer from biometric hacking attacks.

In this paper, we propose a secure smartphone authentication scheme based on user's handshake gestures. A shake cites to a 'to & fro' movement of the hand holding the smartphone and swinging/shaking it in X-axis, Y-axis and Z-axis coordinate plane of the device. Different users wave their smartphone in a different way. Some wave it gently while others do it drastically. This makes the waving speed, frequency of shakes, the waving range and the direction of shakes different from user to user. These patterns derive the user's distinctive features and styles which can hardly be reproduced by others. This prototype adopts a machine learning methodology consisting of a training and an authentication phase. The training phase collects the data from the handshakes using a small number of shakes and in the authentication phase, the shakes are verified using theDynamic Time Warping (DTW) algorithm. The data is collected from the 3D accelerometer and the Proximity sensor. The Dynamic Time Warping algorithm is used for fast and accurate classification and pattern matching. We collected the handshake traces from

volunteers using our prototype. After several experiments and tests, the results were positive with a low error rate.

The paper is organized as follows: Section 2 presents the literature survey on security threats and dynamic time warping. Section 3 describes the system architecture and section 4 details the visualizations of the dataset. Section 5 describes the system model and section 6 projects the importance of removal of gravity component. Section 7 describes the validator function followed by section 9 and 10 provides the metrics and screenshots. Section 11 shows the result of the model and draws conclusions.

II. LITERATURE SURVEY

The information from European Union Agency for Network and Information Security suggest that data leakage due device loss or theft and unintentional disclosure of data has been the top two information security risks of smartphones [1]. Smudge attacks and shoulder-surfing attacks has been the common methods to take unauthorized control of mobile phones [2][3][4].The smudge attack relies on detecting the oily smudges left behind by the user's fingers when operating the device using simple cameras and image processing software. Under proper lighting and camera settings, the finger smudges can be easily detected, and the heaviest smudges can be used to infer the most frequent user input pattern. The researchers were able to break the password up to 68% of the time under proper conditions [5].Biometric spoofing is a method of confusing a biometric identification management system by presenting a counterfeit mold in front of the biometric scanner for emulating the unique biometric attributes and confusing the system between the artifact and the real biological target and gain access to sensitive data.Using the principle of pulse oximetry [6] the liveliness of the test subject is taken into account by measure of blood oxygenation and the heart rate. This reduces attacks like the one's mentioned above, although these methods aren't commercially applicable as costs of implementation are high. This reduces their real world application and hence makes biometrics insecure until these methods are commercially viable.

Dynamic time warping is an algorithm for measuring similarity between two temporal sequences which may vary in speed in a time series analysis. Any data that could be turned into linear sequence can be analyzed with DTW. The common applications of DTW are speech recognition, signature recognition and partial shape matching. Shake in authorization were done using support vector machine (SVM) classifier [7] but the error rate was high. Since the accelerometer data is continuous and the order of the sequence matters, we prefer DTW over SVM.

III. SYSTEM ARCHITECTURE

The user's handshake is taken as input in the Original Gesture Accelerometer Data phase. The user repeats the shakes three to five times and it is recorded. This recorded data is considered as the training phase. The gravity component is removed and the processed data is stored in the Internal Storage.

In the authentication phase, the gesture that is set to allow access is repeated to initiate the unlocking process. Once the user shakes the phone, the accelerometer data is recorded and the gravity component is removed. This processed data is passed through the DTW classifier. The similarity of the training phase signals and the authentication phase signals are calculated. If the distance of the signal is under the threshold values, the validator authenticates the shake and allows access to the device. Else if the distance is not under the threshold values, the access is denied.

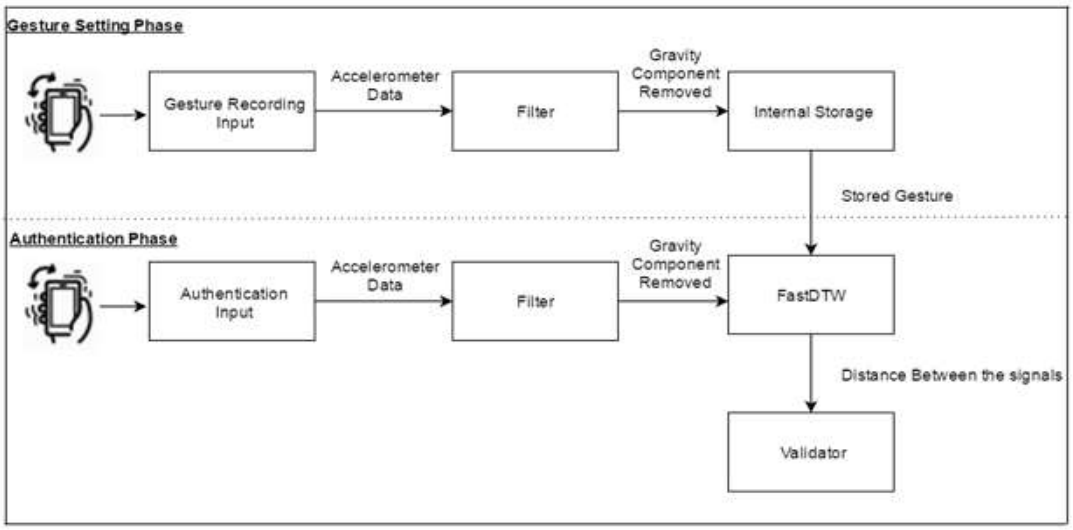

Figure 1. System Architecture

IV. DATA COLLECTION AND VISUALIZATION OF ACCELEROMETER DATA

We collect the shake data from 50 volunteers with a standard android smartphone. All the volunteers are asked to record the pattern three to five times based on the variations in their shakes. There is no restriction on the shaking action. All the raw data collected is stored in a table where the acceleration along X-axis, Y-axis and Z-axis are stored in different columns.

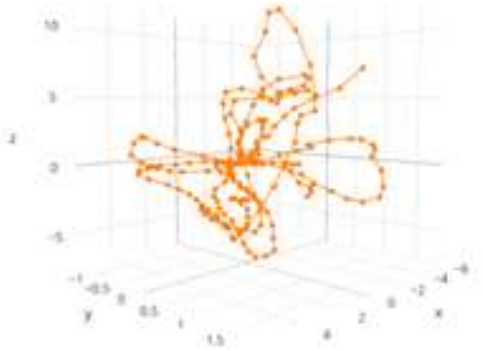

Figure 2. User 1 accelerometer data visualization

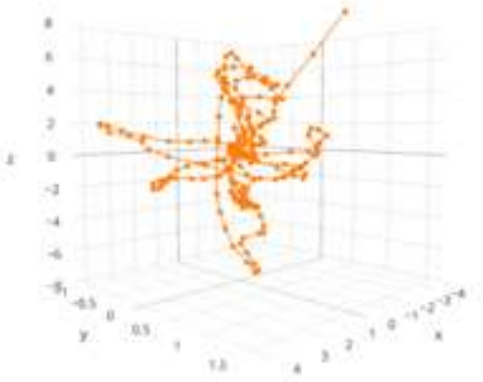

Figure 3. User 2 accelerometer data visualization

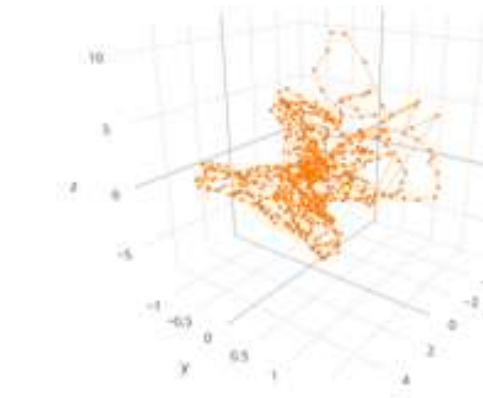

Figure 4. User 3 accelerometer data visualization

V. SYSTEM MODEL

5.1 Dynamic Time Warping

The Dynamic Time Warpping (DTW) is a well-established technique which is used to measure the similarity between two temporal sequences which may vary in time or speed. The aim of DTW is to find the best mapping with the minimum distance by the use of Dynamic Programming. The advantage of DTW is that it can well deal with the misalignment of points in the temporal sequences. DTW is suitable as the user waves his/her smart phone along a fixed, secrete and pre-defined movement.

Given two time series X and Y of lengths $|X|$ and $|Y|$ such that,

$X = x_1, x_2, x_3\ldots\ldots, x_i, \ldots\ldots, x_{|X|}$

$Y = y_1, y_2, y_3\ldots\ldots, y_i, \ldots\ldots, y_{|y|}$

Construct a warp path W,

$W = w_1, w_2, w_3, \ldots\ldots, w_k \qquad max(|X|,|Y|) \leq K < |X| + |Y|$

Where K is the length of the warp path and the k^{th} element of the warp path is:

$w_k = (i,j)$ *{ i -> index from time series X, j -> index from time series Y}*

The warp path must start at the beginning of each time series at $w_1 = (1, 1)$ and finish at the end of both time series at $w_K = (|X|,|Y|)$.

Every index of each time series must be used in the warp path. There is a constraint on the warp path that forces i and j to be monotonically increasing functions in the warp path.

$w_k = (i, j), w_{k+1} = (i', j') \quad where\ \{ i \leq i' \leq i+1, j \leq j' \leq j+1\}$

The optimal warp path is the minimum distance warp path. The distance of the warp path W is:

$$Dist(W) = \sum_{k=1}^{k=K} Dist(w_{ki}, w_{kj})$$

DTW Algorithm:

A dynamic programming approach is used to find this minimum-distance warp path. The methodology involves finding solutions to sub-problems and these solutions are used repeatedly to find solutions to a slightly larger problem until the solution is foundfor the entire time series. Each and every cell of the cost matrix must be filled to find the minimum distance warp path.

STEP 1: Construct a two dimensional |X| by |Y| cost matrix D, where the value D(i, j) is the minimum distance warp path that can be constructed from two time series X and Y.

STEP 2: The distance of the optimal warp path D(i,j) is calculated.

$$D(i,j) = Dist(i,j) + min\begin{cases} D(i-1,j), \\ D(i,j-1), \\ D(i-1,j-1) \end{cases}$$

STEP 3: After the entire matrix is filled, a warp path is found from $D(1, 1)$ to $D(|X|, |Y|)$. The warp path is calculated in reverse order starting at $D(|X|, |Y|)$. A greedy search is performed that evaluates cells to the left, down, and diagonally to the bottom-left. The adjacent cell which has the smallest value is added to the beginning of the warp path found sofar,and the search continues from that cell. The search stops when $D(1, 1)$ is reached.

```
1   path[] ← new array
2   i = rows(dtw)
3   j = columns(dtw)
4   while (i > 1) & (j > 1) do
5           if i == 1 then
6                   j = j - 1
7           else if j == 1 then
8                   i = i - 1
9           else
10                  if dtw(i-1, j) == min {dtw(i - 1, j);
    dtw(i, j - 1); dtw(i - 1, j - 1)}
11                  then
12                          i = i - 1
13                  else if dtw(i, j-1) == min {dtw(i - 1,
    j); {dtw(i, j - 1); dtw(i - 1, j - 1)}
14                  then
15                          j = j - 1
16                  else
17                          i = i - 1; j = j - 1
18                  end if
19                  path.add((i, j))
20          end if
21  end while
22  return path
```

5.2 FAST DTW

Standard dynamic time warping (DTW) is an $O(N^2)$ algorithm as every cell in the cost matrix must be filled to obtain an optimal answer. The size of the cost matrix grows quadratically with respect to the size of the time series. In the Fast dynamic time warping approach (multilevel approach), the cost matrix is only filled in the neighborhood of the path projected from the previous resolution. Since the length of the warp path grows *linearly* with the size of the input time series, the multilevel approach is an $O(N)$ algorithm[8]. Due to these advantages of Fast DTW over standard DTW we switch to Fast DTW approach.

ALGORITHM

Function FastDTW()
Input: *X* – A TimeSeries of length |*X*|
Y – A TimeSeries of length |*Y*|
Radius– distance to search outside of the projected warp path from the previous resolution when refining the warp path.

// the min size of the coarsest resolution.
Integer *minTSsize* = *radius*+2
IF (|*X*| ≤ *minTSsize* OR |*Y*| ≤ *minTSsize*)
{
/ Base Case: for a very small time series run the full DTW algorithm.*/*
RETURN DTW(*X*, *Y*)
}
ELSE
{
/ Recursive Case: Project the warp path from a coarser resolution onto the current resolution. Run DTW //only along the projected path (and also 'radius' cells from the projected path). */*
TimeSeries *shrunkX* = *X*.reduceByHalf()
TimeSeries *shrunkY* = *Y*.reduceByHalf()

WarpPath *lowResPath* = FastDTW(*shrunkX*,*shrunkY*, *radius*)
SearchWindow *window* = ExpandedResWindow(*lowResPath*, X, Y,*radius*)

RETURN DTW(*X*, *Y*, *window*)
}

Output:1) A min. distance warp path between *X* and *Y*
2) The warped path distance between *X* and *Y*

VI. REMOVAL OF GRAVITY COMPONENT

The coordinate-system is defined relative to the screen of the phone in its default orientation. The axes are not swapped when the device's screen orientation changes. The X axis is horizontal and points to the right, the Y axis is vertical and points up and the Z axis points towards the outside of the front face of the screen. In this system, coordinates behind the screen have negative Z values.

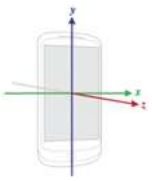

Figure 5. Sensors coordinate-system diagram.

The accelerometer measures the acceleration applied to the device ($\mathbf{A_d}$). The acceleration is found using the relation:

$$\mathbf{Ad = - \sum F_s / mass}$$

Where $\mathbf{F_s}$is the force applied to the sensors.

The force of gravity is always influencing the measured acceleration:

$$\mathbf{Ad = -g - \sum F / mass}$$

In order to measure the real acceleration of the device, the contribution of the force of gravity must be eliminated. **That is** when the device is sitting on a table, the accelerometershould read a magnitude of approximatelyg=0 m/s^2 instead of g = 9.81 m/s^2.

This is achieved by a *low-pass* filter which is used to isolate the force of gravity and the alpha constant used for removal of gravity component is found to be 0.8 with experimentation.

VII. VALIDATOR

Using the DTW algorithm we find the average relative distance between the three gestures that is the distance between gesture one and two, gesture two and three, gesture one and three and finally store their average.

In the authentication module, raw data of the 3 axial accelerometer is obtained from the user when a gesture is made. The gravity component is removed from the raw data. Using the DTW algorithm, we find the distance between the authentication gesture and the stored 3 gestures. Now the average is found and stored as $\text{Average}_{\text{authentication}}$. We find the ratio between the two averages ($\text{Average}_{\text{original}}$ and $\text{Average}_{\text{authentication}}$). If the ratio is below a threshold, then the user is authenticated else the user is not authenticated. The threshold value is adjusted based on experimentation so that the false positive and false negative rates are optimal.Based on the experiments carried out we found that the optimal threshold value is 1.35. Anything above this threshold value is considered as a false authentication and the access is denied.

VIII. METRICS

FALSE POSITIVE RATE:

False positive is defined as a test result which shows that a particular condition or an attribute is present when it is not. In our case an unauthorized user is treated as authorized user and access is provided. The rate is determined by the ratio of number of incorrect authentications of an unauthorized user to the total number of authentication attempts. The false positive rate derived from the experiments is 0.05.

TRUE POSITIVE RATE:

The probability that an authorized user is successfully verified. This rate is derived from the ratio of number of correct authentications of an authorized user to the total number of authentication attempts. The true positive rate derived from the experiments is 0.87

FALSE NEGATIVE RATE:

False negative is defined as a test result which indicates that a particular condition or attribute is absent when it actually exists. In this case an authorized user is treated as unauthorized user and the access is denied. The rate is determined by the ratio of number of incorrect authentications of an authorized user to the total number of authentication attempts.The false negative rate derived from the experiments is 0.13.

IX. SCREENSHOTS

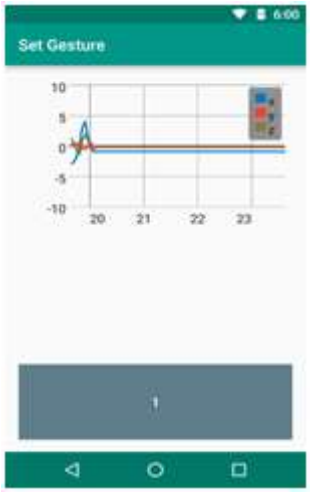

Figure 6. Set gesture Screen Figure 7. Recording Trails

Figure 8. Rejection ScreenFigure 9. Authentication screen

X. RESULTS AND CONCLUSION

The prototype is resilient to shoulder-surfing, smudge and biometrics hacking attacks as it adopts both physiological and behavioral characteristics to profile users. It is handy as it allows customized shakes and single-hand operations.It is

likely to be quite reliable with low false positive rate of 0.05. A secondary authentication mechanism can be used as a backup in case this fails.

REFERENCES

[1] European Union Agency for Network and Information Security, "Top Ten Smartphone Risks," https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks.

[2] F. Tari, A. Ozok, and S. H. Holden, "A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords," in Proceedings of the second ACM Symposium on Usable privacy and security, 2006, pp. 56–66.

[3] F. Schaub, R. Deyhle, and M. Weber, "Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone Platforms," in Proceedings of the 11th ACM International Conference on Mobile and Ubiquitous Multimedia, 2012.

[4] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge Attacks on Smartphone Touch Screens," WOOT, vol. 10, pp. 1–7, 2010.

[5] *Aviv, Adam J.; Gibson, Katherine; Mossop, Evan; Blaze, Matt; Smith, Jonathan M.* Smudge Attacks on Smartphone Touch Screens *(PDF)*. 4th USENIX Workshop on Offensive Technologies.

[6] Reddy, P.V; Kumar, A; Rahman, S; Mundra, T.S. "A New Antispoofing Approach for Biometric Devices". *EEE TRANSACTIONS ON BIOMEDICAL CIRCUITS AND SYSTEMS*. **2** (4): 328–337. doi:10.1109/tbcas.2008.2003432

[7] Hongzi Zhu, Member, IEEE, Jingmei Hu, Shan Chang, Member, IEEE, and Li Lu. "ShakeIn: Secure User Authentication of Smartphones with Habitual Single-handed Shakes" 10.1109/TMC.2017.2651820, IEEE Transactions on Mobile Computing

[8] Stan Salvador & Philip Chan, FastDTW: Toward Accurate Dynamic Time Warping in Linear Time and Space. KDD Workshop on Mining Temporal and Sequential Data, pp. 70-80, 2004

[9] **https://developer.android.com/reference/android/hardware/SensorEvent.html android developer documentation.**