LUIS: A LIGHT WEIGHT USER IDENTIFICATION SCHEME FOR SMARTPHONES

Sanju Xaviar[1], Kalyan Sasidhar [2] and Preeja Pradeep[3]

Amrita Center for Wireless Networks and Applications, Amrita Vishwa Vidyapeetham, Amritapuri, Kollam, India

ABSTRACT

Smartphone usage has reached its peak. There has been a tremendous growth in the number of people migrating from PCs to smart phones. Numerous scenarios such as loss of a phone, phone theft etc., can lead to unauthorized use of one's own smartphone. This raises the concern for securing personal and private data. This project proposes a light weight two level user identification scheme to recognize and authenticate the mobile phone based on the device holding and usage patterns. To validate the proposed scheme, an application is created which takes a gesture input characterized by time of swiping the screen, finger pressure, phone movements and location of swipe on the screen through X and Y co-ordinate. A threshold based matching scheme performs classification to find the true owner. Results show that the scheme was able to achieve 90% true positives and 10% false positives with a 0.5% of battery usage.

KEYWORDS

Smartphones, Security, User authentication, Touch screen, Sensor, Gesture

1. INTRODUCTION

According to the market research in [1], number of smartphone users worldwide will surpass 2 billion in 2016. The number of people migrating from PC to smart phones is tremendous. Smartphones are used for numerous purposes such as Google wallet, web browsing, paying bills, storing confidential documents, personal and private information. This increase in usage of smartphones makes device access control and data security very important.

In corporate business world, professionals store all their secret information on their smart phone as it is of great comfort and cost-effective. So there is a big need to protect phone being used by others. There are many ways of attacking users. For instance, shoulder surfing is a common attack where attacker can login by viewing the username password. There are some who just out of curiosity [2] does the attack in order to know business matters, co-worker details, phone call history etc. Attackers can even have the intension of knowing the financial information of the user and perform money transfers. Hence authentication has become a factor of great importance in today's era. The main purpose of authentication is to ensure that only the rightful owner of a device is granted access to it. Existing methods include PIN/password unlocking schemes. These are prone to shoulder surfing and smudge attacks. Memorizing these passwords is difficult as the user has to remember a large number of them. Hence users get motivated to go for simpler and weaker passwords which are prone to many of the basic attacks and this leads to the misuse of phone.

DOI: 10.5121/ijci.2015.4203

Modern smartphones comes with a variety of sensors that automate our daily tasks. Some of the sensors used in smartphone are accelerometer, gyroscope, compass and proximity sensor, etc. Accelerometers in mobile phones are usually used to detect the orientation of the phone. It can

also be used for identifying an activity a user performs [13] e.g. jogging, sitting etc. Gyroscope in phone is used to detect the roll, pitch and yaw motions [3]. Digital compass is based on a sensor called magnetometer which provides mobile phones with a simple orientation in relation to the Earth's magnetic field. Proximity sensor is used to detect how close the smartphones screen is to the body and based on that turns off the light of screen and saves battery. In this paper we have used sensors for the purpose of authentication in smartphones. Accelerometer sensor is used to detect the movements of the smartphone. Touch screen sensors is used to measure the finger pressure and location of swipe on screen through X and Y coordinate ,at the time of unlocking which is obtained using android APIs.

The main aim of this paper is to develop a light weight gesture based authentication scheme to detect and identify the actual user of the phone. Using any simple touch screen gesture the original user can login and this authentication scheme detects and identifies who is using the phone. The advantage of the proposed system is the two level authentication which provides additional detection of malicious user. Fine behavioral biometric information such as finger pressure, time to swipe, location of swipe etc. is collected from the user at the time of unlocking the phone, which helps in user identification. Study and evaluation of the applicability of using touch gesture inputs for authentication is done and its performance metrics are analyzed.
The rest of the paper is organized as follows: Section II describes related work that focuses on smartphone authentication schemes. The details of the proposed approach are described in Section III. In Section IV, experimental setup and methodology is been discussed. Section V describes the analysis of the collected sensor readings and Section V deals with the performance evaluation. Finally we draw conclusions and future work in Section VII.

2. RELATED WORK

There is considerable work done in this field. A few of the works are listed below:

In [2], the author highlights the importance of smart phone and its growing popularity due to which users store their sensitive information (E.g. confidential documents) more on phone. Passwords can be used only for on time authentication but they are highly unreliable. The solution to this problem is Continuous authentication. The authors introduced FAST (finger gesture authentication system using touch screen) an authentication scheme which extracts touch data features such as finger pressure, trajectory, speed, acceleration and X and Y coordinates. This method hasn't completely reduced the False accept rate and False reject rate to 0; hence it is not possible to completely mitigate the unauthorized use. These schemes take a large amount of time and are not suitable for instantaneous authentication, which is the main focus of this paper.

Jakobsson et.al [3] discusses about M-Commerce (Mobile) and its rapid growth. Mobile internet devices give rise to authentication without user involvement. Implicit authentication can replace passwords and the burden of remembering it. Implicit authentication is needed in order to authenticate users based on users behavior. High security can be maintained by implicitly authenticating a person and logging off a person, if it is an invalid user. Implicit authentication can replace passwords and the burden of remembering it. An Authentication score can be calculated based on the recent activities of the user. Negative score indicates an attack, positive score indicates that the true user is using. If the score falls below a threshold, then the user can't access the system. The main limitation of this paper is that they haven't mentioned about the accuracy of the system and how the unauthorized users can be denied access. In the proposed

system identification of users is done based on the performance metrics i.e. True positive and false positive.

In [5], mechanisms are used to collect the user's patterns and based on that the network and power management has been done. Collection of phone usage details is done for two months and a case study is done to show how this usage pattern information can be applied to power management system. The authors [6], implement a tapping based authentication scheme that uses a combination of four features such as acceleration, pressure, size and time in order to substantiate whether the authenticated user is the true owner of the smartphone. In this paper a gesture based scheme is implemented along with pattern based unlocking as the second level authentication, which provides extra security and there is no need for memorizing pin/password.

In [7], the author brings about a new concept called Tap songs which helps to enable user authentication on a binary sensor. It is implemented by matching rhythm of tap down/up events to jingle timing model. The matching algorithm uses absolute match criteria which learn from the successful login. Tap songs memorability hasn't been checked if the tap songs haven't been entered for more than1 week. The number of taps needs to be memorized by the user; the proposed system takes away this problem by using a gesture based mechanism.

In [8], a tapping detection technique is proposed which uses Hamming distance matching approach which compares the two patterns based on the key presses and key releases. As a part of pattern matching, the time between the taps and within the taps is noted. Memorability of tapping pattern is not considered. There are problems due to capturing sound such as tapping and observations through video camera. They haven't mentioned about its accuracy.

The author explains about context aware implicit identification scheme using touch screen gestures in [9] uncontrolled environments. User identification schemes used here is dynamic time wrapping and one nearest neighbor classifier. A touch based identity protection service was implemented that implicitly authenticated the user in the background by analyzing touch screen gestures continuously in a running application. Other than usual biometric features such as swipe speed, click gap, contact size, other behavioral features such as touch location, swipe length and swipe curvature is also taken into account. In [10], a gesture based user authentication scheme is implemented for secure unlocking of touch screen devices. They used features such as finger velocity, device acceleration and stroke time for authentication. Luca et al [11] used dynamic time warping algorithm to compute the distance between gesture traces. This scheme was of low accuracy, they hadn't extracted any behavioral feature from user's gesture.

In [12] they utilized accelerometer in smartphones to authenticate user based on their gaits. This scheme has low true positive rate as gaits of people are different on different surfaces. Jennifer R. Kwapisz et.al [13] had conducted analysis of activity recognition using available accelerometer data by just placing smartphone in pocket. For the implementation of the system, data was collected from 29 users performing daily activities like walking, jogging, climbing stairs, sitting and standing. In our paper we are using more than one sensor to authenticate the user based on the unlocking pattern.

In [14], Shi et al had designed and evaluated an implicit mobile user identification system. It is based on four different smartphone sensors such as microphone, GPS, touch screen and accelerometer. One sensor is activated to continuously authenticate the user in one out of four usages conditions. For example, accelerometer is used while the user is walking, and the touch screen sensor is used to monitor user's touching activities while he/she is engaged in some applications. In our system we use the combined performance of all the sensor data together. In [15], it is said that users have a unique way to hold and operate his smartphone while using applications and these behavioral biometrics can be captured from the readings of the orientation

sensor. The non-intrusive mechanism is been used with existing mechanisms such as password or fingerprint to build a robust authentication framework for smartphone users.

3. PROPOSED APPROACH

The common methods used for authentication are based on user location, finger print reader, pass codes and face recognition schemes [4]. The main problem with location based is when a user travels outside the regular scope. Finger print readers can be a problem when there are injuries on the finger. In case of pass codes, the main attacks are shoulder surfing and smudge attack. In case of face recognition schemes, lighting and face make up can reduce the chances of authenticating a true user.

In the proposed system there are no problems due to shoulder surfing and smudge attacks as the thief even after knowing the unlocking pattern will not be able to unlock the phone ,*as behavioral features applied by each user vary from person to person*. By using touch screen gestures based on behavioral biometrics increases the chances for authenticating a true user. Training samples are collected from users for n number of trials, where n=10, 30, 50, 70 and 100 trials. Then extraction and selection of behavioral features are done from those samples, and finally users are classified using a threshold based matching scheme. Compared to the existing methods such as PIN/Password schemes, the proposed method does not need any memorizing skill to remember the touch screen patterns.

3.2. System Architecture

Figure1 shows the different components in an authentication system. An application is created that recognizes a touch screen gesture of a user based on input parameters such as time, pressure, X and Y coordinate and phone movements. A two factor authentication scheme is been introduced here. In the first level, a gesture based authentication scheme is implemented. The second level is a pattern unlocking scheme which is a technique usually used in smartphones.

In the gesture based authentication scheme there are two phases: Training phase and Verification phase. In training phase, feature extraction and classification takes place of the original user. In verification phase, a test input is given; it is compared with the data in the database and based on that detection takes place. The database consists of learnt patterns of the original users. Using a threshold based matching scheme, the patterns formed by user is learnt and classified. MATLAB offline analysis is been done in order to detect the actual user. If this level is satisfied then it follows the next stage i.e. pattern unlock. If the user is successful in satisfying these two levels of authentication then he can access the phone. If an intruder gets in then alarm is triggered.

3.3. Touch Screen-Data features

When a user presses the touch screen, there are several different features of touch behavior biometrics that can be used. The following parameters are used in the proposed system:

3.3.1. X and Y coordinate: X coordinate is a sequence of numbers which stores the finger position [4] on x axis on the touch screen while unlocking a phone using a gesture. Y coordinate refers to finger position on y axis on the touch screen.

3.3.2. Finger pressure: Pressure [6] is obtained by using the Android API MotionEvent.getpressure ( ).The returned pressure measurements are of abstract units

ranging from 0(no pressure at all) to 1(normal pressure). There can be chances to have a value higher than 1 depending on the calibration of the device.

3.3.3. Time*:* Time can be obtained by using Android API MotionEvent.getEventTime ( ). It helps in retrieving the time this event occurred.

3.3.4. Phone Movements: When a device is held in its default orientation X axis point's horizontal, Y axis points vertical and Z axis points outside of the screen surface. Linear acceleration sensor provides with a 3D vector representing acceleration along each device axis, excluding gravity. Magnitude of acceleration/Vector sum is taken as the phone coordinate system is sensitive to location changes.

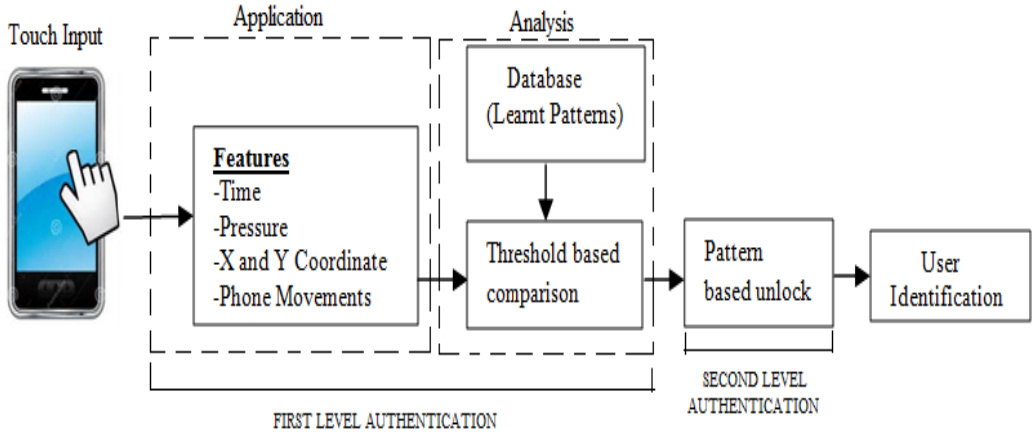

Figure 1. System Architecture

4. EXPERIMENTAL SETUP AND METHODOLOGY

The experimental setup and the methods deployed are explained in the following section.

4.1. Experimental setup

An android application is implemented that collects the input parameters such as time to swipe, finger pressure, phone movements and location on phone where swipe takes place. The application was installed in two smartphones (Sony Xperia J and Samsung S3 Mini). Training was conducted for two users, first inferences were made of the data collected from the android app in MATLAB, after which analyses is done in order to identify users based on the performance metrics discussed in the next section. The data is collected from 2 phones for 4 weeks. Two Users two weeks of touch data was used as training templates and the subsequent 2 weeks of data was employed as testing data. The main assumptions for this experiment are that user behavior is consistent and user identification is done in a controlled environment. Variations among two users are analyzed based on the given input parameters for the same pattern.

4.2. Methodology

The following methodology is adopted in order to detect and identify the actual user:

4.2.1. "TimeAuthenticate" application

A gesture based android application "TimeAuthenticate" is implemented which takes input from the user such as time to swipe, pressure applied by the finger and the location where the swipe is performed.

Step1: Start Activity
Step2: When finger is pressed on screen, start the timer ta.
Step3*:* When the finger is moved across the screen, get the X and Y coordinates (xi, yi), time ti and pressure pi during action move, Where 1<=i<=n (number of trials).
Step4: When the finger is picked up from screen, find the gesture duration and stop the timer ta.
Step5: If the gesture duration tg is less than the minimum touch duration tm or if the touched distance dg is less than minimum distance dm, give a simple message to user to "make gesture properly".

Input parameters are displayed on the screen when the user swipes on the screen using USB debugging, logcat is used to get input values when a user unlocks the phone.

4.2.2. Threshold based matching scheme

A threshold based matching scheme is been implemented in MATLAB. For each user there are four datasets i.e. for time, pressure, phone movement and X and Y Coordinates. Readings are taken from user for N trials, where N=10, 30, 50, 70 and 100. When the threshold t is too large then it is difficult to correctly identify users as large range of values will be selected and there are chances for an invalid user to be recognized as a true user. It can be seen that when more number of readings is collected the threshold can be set more precisely. Finer the threshold less is the chances for an unauthorized user to gain access to the device. Based on the threshold set performance is analyzed when the sensor data are used individually and when multiple sensor data are combined. Data is collected and analyzed and the outliers are filtered as there are fluctuations in user's phone usage behavior.

From the dataset features such as mean, minimum, maximum are computed. Those values are used to define the upper bound or the threshold for which the unlock pattern is considered as valid. Raising the threshold by 5%, 10% and 15% was also analyzed to find which combination performs better. The analysis was performed using different thresholds and different parameter combinations. Any combinations of multiple sensor data can be combined.

Figure 2 illustrates a combination of four inputs i.e. Time, pressure, X and Y coordinate and phone acceleration. It explains a threshold based matching scheme. There are N number of trials, and two data sets for each user1 and user2. Each data set consists of four database each for input parameters such as time, pressure, X and Y coordinates and acceleration. Upper and lower bound is set for each data base parameters based on the readings obtained from the users. Upper bound is denoted by i, k, m and o. Lower bound is denoted by j, l, n and p. x is the count for successful authentication, if the true positive C0 is greater than x then the original user is said to be authenticated. Study is done to check the performance when a single sensor data is used and the variations in performance when more than one sensor data is used. Performance is analyzed for different combinations of input parameters and the true positive and true negative is calculated which is discussed in Section VI.

5. DATA ANALYSIS

After the input parameters such as finger pressure, phone movements, time and location of swipe are measured using the application it is then given to MATLAB tool for analysis. The inferences obtained from the graphs are given below: A user's phone movement while unlocking a phone is recorded using accelerometer sensor. Both users are asked to do the same pattern to unlock the phone.

Figure 3 shows (a) accelerometer readings for different trials by user1, (b) accelerometer readings for different trials by user2, (c) combined readings of both user1 and user2 .The variation is seen in the time taken to swipe. User1 takes more time to swipe than user2. For user1 the variations in vector sum is in the range of 0.7 to 0.8. Whereas for user2 it can be seen that the vector sum is in the range of 0.5 to 0.6. The variations can be observed when both user1 and user2 readings are plotted together. The accelerometer readings of user1 and user2 are consistent within themselves and when both the users readings are plotted together the variations can be clearly seen.

Input: N=number of trials, N= {10, 50,100}
Dataset user1 D1= {d11, d12, d13, d14}
Dataset user2 D2= {d22, d23, d24, d25}
d11=d22=Time, d12=d23=Pressure
d13=d23=X and Y Coordinate
d14=d24=Accelerometer
Threshold T user1= {T1, T2, T3, T4}
T1={i,j},T2={k,l},T3={m,n},T4={o,p}
x= count for successful authentication

Output: Count C= {C0, C1, C2, C3}
C0- True positive, C1-False positive, C2-False negative,C3-True negative.

```
1. C is initialized to 0
2. for t=0 to N
        If(d11(t)>=i || d11(t)<=j)
            If(d12(t)>=k && d12(t)<=l)
            If(d13(t)>=m && d13(t)<=n)
              If(d14(t)>=o && d14(t)<=p)

3. C0=C0+1
4. C1=N-C0
5. for t=0 to N
        If(d22(t)>=i || d22(t)<=j)
            If(d23(t)>=k && d23(t)<=l)
               If(d24(t)>=m && d24(t)<=n)
                 If(d25(t)>=o && d25(t)<=p)
6. C2=C2+1
7. C3=N-C3
8. If(C0>x)
9. display 'User A/B authenticated'
```

Figure 2. Description of the Threshold based scheme

To find the location on screen where a user swiped, we can use X and Y coordinates for it. Figure 3 Shows (d) X and Y coordinates of user1 with different trials (e) shows X and Y coordinates of user2 with different trials, shows(f) both user1 and user2 combined. By using X and Y coordinate we can get the shape of the swipe and the location in the phone where the swipe was performed.

In case of user1, swipes is performed on left most of the screen so the X coordinates range from 50 to 150 and Y coordinates from 150 to 250.In case of user2, swipe is

performed on the right most of the screen so his coordinate values are from 310 to 400 and Y coordinates from 300 to 400.

Figure 4 shows (a) Finger pressure of user1 with different trials, (b) shows finger pressure of user2 with different trials, and (c) shows user1 and user2 trials combined. In case of user 1 it is being seen that while unlocking the phone, the pressure of the finger increases from 0.6 to 0.8 to 1 and then decreases during the swipe. In case of user 2 the pressure applied by user2 increases from 0.6 to 0.8 to 1, stays at 1 for some time and then decreases. It can be seen that user2 average is more than user1's average. Moreover it is been noticed that each user shows consistent and unique behavior which helps in differentiating itself from other users.

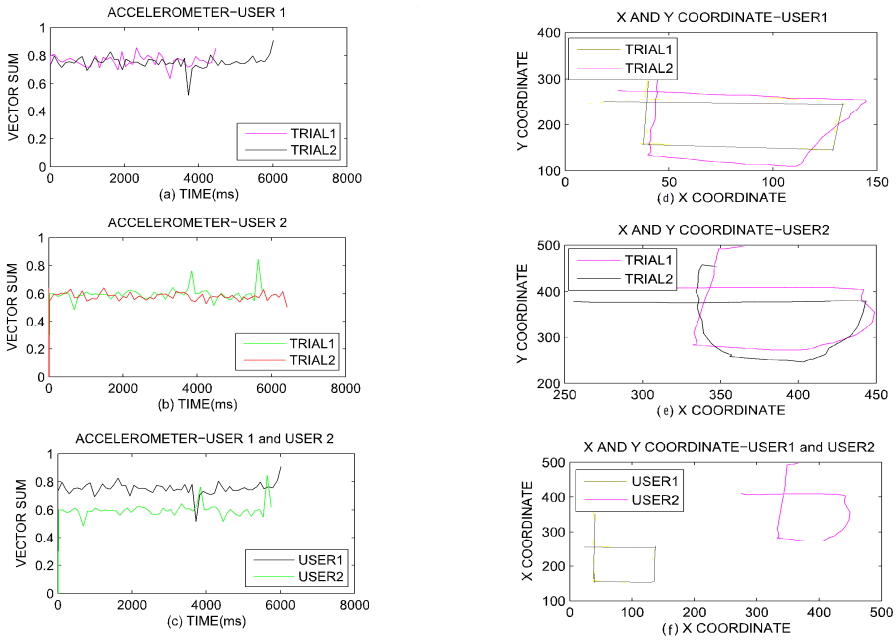

Figure3. Illustrates the variations in phone accelerometer and X and Y Coordinate readings of user1 and user2.

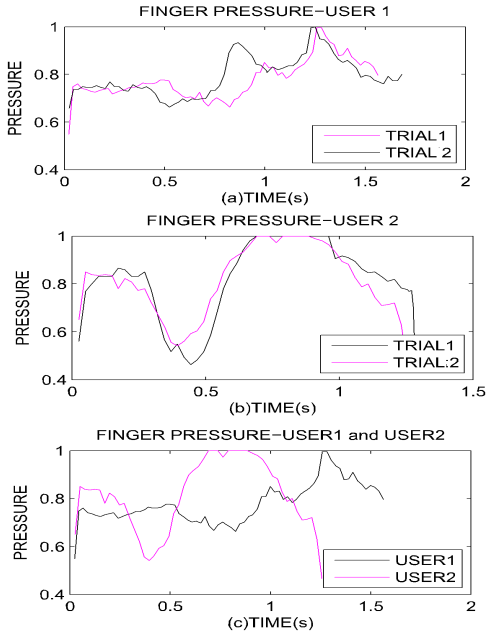

Figure 4. Illustrates the variations in pressure sensor readings of user1 and user2.

6. PERFORMANCE EVALUATION

In this experiment, performance of our simple threshold based authentication is evaluated. We evaluate based on True positive and False positive. True positive is defined as those who test positive and are positive. False positive is defined as those who test positive and are negative. As the number of trials increases the accuracy also increases but with delay as a constraint.

In Figure 5, when number of trials=10, touch data features such as Time, Pressure and X and Y coordinate achieves an accuracy of 40% and Accelerometer an accuracy of 30%.Hence combined sensor data can achieve an accuracy of 50% when compared to single sensor data which give an average accuracy of 40%. When the number of trials=50, touch data features such as Time, Pressure, X and Y coordinate and Accelerometer achieves an accuracy of 52%,68%,72% and 60% respectively. Hence combined sensor data can achieve an accuracy of 76% when compared to single sensor data which gives an average accuracy of 63 %. When the number of trials=100, touch data features such as Time, Pressure, X and Y coordinate and Accelerometer achieves an accuracy of 80%,78%,80% and 70% respectively. Hence combined sensor data can achieve an accuracy of 90% when compared to single sensor data which gives an average accuracy of 77%.

In Figure 6, When number of trials=10, touch data features such as Time, Pressure, X and Y coordinate and Accelerometer can reduce the error rate to 60%,60%,60% and 70% respectively .Hence combined sensor data can reduce the error rate to 50% when compared to single sensor data which can reduce it to 62.5%. When number of trials=50, touch data features such as Time, Pressure, X and Y coordinate and Accelerometer can reduce the error rate to 48%,32%,28% and 40% respectively. Hence combined sensor data can reduce the error rate to 24% when compared to single sensor data which can reduce it to an average of 37%.When number of trials=100, touch data features such as Time, Pressure, X and Y coordinate and Accelerometer can reduce the error rate to 20%,22%,20% and 30% respectively. Hence combined sensor data can reduce the error rate to average of 10% when compared to single sensor data which can reduce it to an average of 23%.

The power consumption for the android application "TimeAuthenticate" is only 0.5%. Hence it is an efficient light weight application. It can be seen if a user satisfies all the levels i.e. Time to swipe, finger pressure, location of the swipe through X and Y coordinates etc then the user can enter in as an authenticated user. Based on the performance different combinations of sensor data are taken by which we can improve the accuracy and authentication.

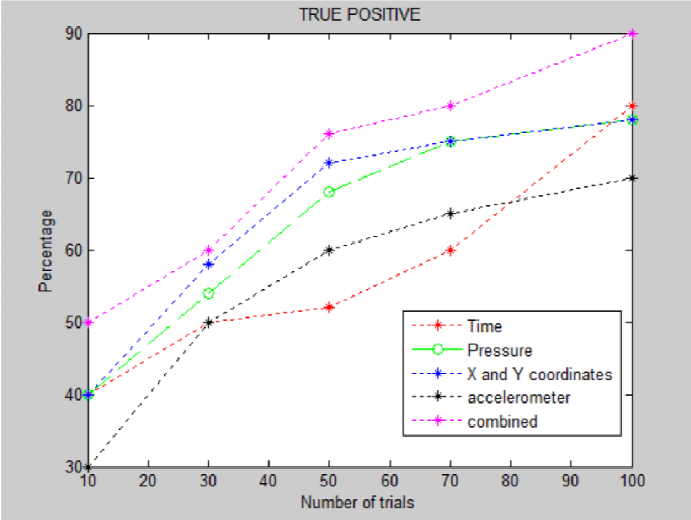

Figure 5. True Positive under different number of trials

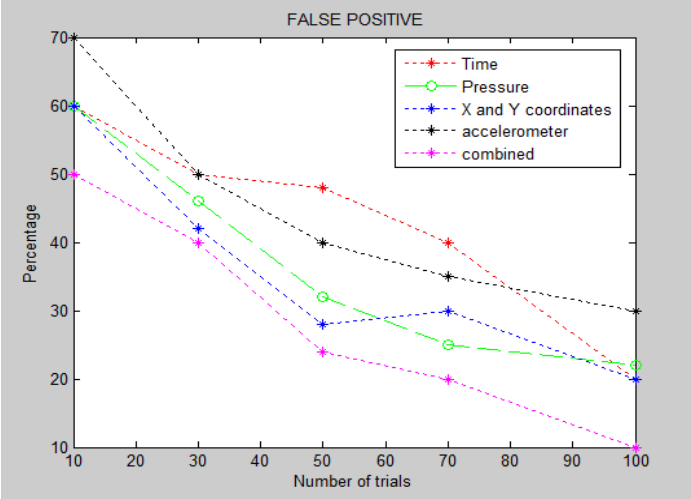

Figure 6. False Positive under different number of trials

7. COMPARISON WITH EXISTING SCHEME

We have compared the performance with the works done in this direction reported in [11] where Luca et al, has used the following gestures: swipe left with one finger, swipe down with one finger, swipe down with two fingers, and swipe diagonally up from bottom left of the screen to

top right. The highest false positive when the true positive is 94%, that they achieved is 43%, but we were able to achieve false positive of 10%, with 90% true positive.

Table1 reports the True positive and False positive achieved by our method and the scheme in [11].We do not use more than 1 gesture as error rates are large and less user convenient. The proposed method has an advantage as any touch screen gesture can be performed to unlock the phone and is not limited to a few gestures as done in the existing schemes. This paper is able to achieve 10% false positive when compared to [11] which has high false positive rates. Luca et al used dynamic time warping which is more power consuming when compared to the 'TimeAuthenticate' application implemented in this paper which consumes only 0.5% power.

Table 1. Comparison of Proposed method with [11]

	Luca et al [11] (%)			**Proposed method (%)**
	Swipe left	**Swipe down**	**Swipe diagonal**	**Any gesture**
True positive	85.11	94	90	90
False positive	48	50	43	10

8. CONCLUSIONS AND FUTURE WORK

The increasing popularity of smart phones devices necessitates the need to bring in intense authentication methods to users that can't be replicated by intruders as it is the biometric information that is taken into account. Compared with the existing methods the proposed method provides more security and usability as it is free from shoulder surfing and smudge attacks. In this proposed method a gesture based user authentication scheme is been implemented. Real time touch data is analyzed for two users and their classification is done based on threshold based matching scheme. By increasing the password length, positive effects on accuracies might be observed. However, this would come at the costs of decreased usability and memorability. This method showed its effectiveness in offline experimental results. This system attains accuracy around 90%.

Future work is to do the implementation and testing on device. The system is to be made scalable so that the system works among large number of users. More touch features can be gathered so that a robust system can be achieved. The accuracy for true positive and false positive can be further increased so that the system can be more reliable.

ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to our beloved Chancellor Sri. Mata Amritanandamayi Devi (AMMA) for the immeasurable motivation and guidance for doing this work.

REFERENCES

[1] "Usage of smartphones", [Online] Available: http:// www.ema- rketer.com/Article/2-Billion-Consumers- Worldwide-Smart- phones-by-2016/1011694

[2] Stockinger, Tobias. "Implicit Authentication On Mobile Devices." In *Ubiquitous Computing*, p. 75. 2011.

[3] Feng, Tao,Z. Liu, K.A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen. "Continuous mobile authentication using touchscreen gestures." In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, pp. 451-456. IEEE, 2012.

[4] M. Jakobsson, E. Shi, P. Golle, and R. Chow, "Implicit authentication for mobile devices," in Proceedings of the 4th USENIX Conference on Hot Topics in Security, ser. HotSec'09. Berkeley,CA, USA: USENIX Association, 2009, pp. 9–9. [Online]. Available: http:///dl.acm.org/citation.cfm

[5] J. M. Kang,_ S. S. Seo, and J. K. Hong, "Usage pattern analysis of smart-phones," in Network Operations and Management Symposium (APNOMS),2011 13th Asia-Pacific, Sept 2011, pp. 1–8.

[6] N. Zheng, K. Bai, H. Huang, and H. Wang, "You are how you touch: User verification on smartphones via tapping behaviors," Tech. Rep., 2012.

[7] J. O. Wobbrock, "Tapsongs: Tapping rhythm-based passwords on a single binary sensor," in Proceedings of the 22Nd Annual ACM Symposium on User Interface Software and Technology, ser. UIST '09. New York, NY, USA: ACM, 2009, pp. 93–96. [Online]. Available: http://doi.acm.org

[8] D. Marques, T. Guerreiro, L. Duarte, and L. Carri¸ co, "Under the table: Tap authentication for smartphones," in Proceedings of the 27th International BCS Human Computer Interaction Conference, ser. BCS-HCI '13. Swinton, UK, UK: British Computer Society, 2013, pp. 33:1–33:6. [Online]. Available: http://dl.acm.org/citation.cfm

[9] T. Feng, J_. Yang, Z. Yan, E. M. Tapia, and W. Shi, "Tips: Context-aware implicit user identification using touch screen in uncontrolled nvironments," in Proceedings of the 15th Workshop on Mobile Computing Systems and Applications, ser. HotMobile '14. New York, NY, USA: ACM, 2014, pp.9:1–9:6 [Online] Available: http://doi.acm.org

[10] Shahzad, Muhammad_, A. X. Liu, and A. Samuel. "Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you cannot do it." In *Proceedings of the 19th annual international conference on Mobile computing & networking*, pp. 39-50. AC M, 2013.

[11] D. Luca, _Alexander, A. Hang, F. Brudy, C. Lindner, and H. Hussmann. "Touch me once and i know it's you!: implicit authentication based on touch screen patterns." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 987-996. ACM, 2012.

[12] Gafurov, Davrondzhon, K. Helkala, and T. Søndrol. "Biometric gait authentication using accelerometer sensor." *Journal of computers* 1.7 (2006): 51-59.

[13] J. R. Kwapisz, G. M.Weiss, and S. A. Moore, "Activity recognition using cell phone accelerometers," in Proceedings of the Fourth International Workshop on Knowledge Discovery from Sensor Data, 2010, pp. 10–18. 5

[14] Shi, W., Yang_, J., Jiang, Y., Yang, F., & Xiong, Y. (2011, October). Senguard: Passive user identification on smartphones using multiple sensors. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2011 IEEE 7th International Conference on* (pp. 141-148). IEEE.

[15] Lin, C. C., Liang, D., Chang, C. C., & Yang, C. H. (2012, June). A new non-intrusive authentication method based on the orientation sensor for smartphone users. In *Software Security and Reliability (SERE), 2012 IEEE Sixth International Conference on* (pp. 245-252). IEEE.

Authors

Sanju Xaviar received BTech degree in Electronics and Communication from Federal Institute of science and Technology, Kerala, India in July 2013. She is currently pursuing MTech in Wireless Networks and Applications from Amrita University, Kerala, India.

Kalyan Sasidhar received his Ph.D. from the University of North Texas, Denton, TX, USA in 2011. From 2012-2013 he worked as a post-doctoral researcher in the School of Computer Engineering, Nanyang Technological University, Singapore. In 2013 he joined the Center for Wireless Networks and Applications, Amrita University, Kerala, India, where he is currently an assistant professor. His research interests include mobile and pervasive computing, applied machine learning, and wireless sensor networks.

Preeja Pradeep received MTech in Wireless Network and Applications from Amrita University, Kerala, India in July 2010. She serves as a Research Associate at the Amrita Center for Wireless Networks & Applications (Amrita WNA), Amrita University, Kerala, India. Her research interests include body area networks and location tracking.