Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Enhancing the Intellect to the Mobile Device Using "Sequential Pattern Technique"

S.Radhika[1], B.Ramya[2], J.Supriya[3], P.Anuradha[4]
[1,2,3]B.Tech Student, [4]Assistant Professor , Dept. of IT,
Prathyusha Engineering College, Poonamallee, Tamil Nadu, India

Abstract: ***In the project Sequential pattern technique is used for Emergency Communication. The Android application is developed in which user's "Hand Waving Pattern" is recorded and the action is repeated for more times until the application registers the user's pattern. For identifying the user "SVM algorithm" is implemented. In the earlier Sequential pattern is used for locking/unlocking, currently it is used for Emergency Communication. If the user is in critical situation, they can notify to the authorities and guardian through their Hand Waving Pattern. Assume as the pattern is recognized, immediately GPS is triggered and location details are sent as URL Links, SMS to the guardian and authorities along with recorded Voice which is send as an SMS Link to the same.In addition to that snapshot is mailed.***

Keyword: Smart phone,Security,Privacy, Authentication, Accelerometer, Emergency Communication.

I. INTRODUCTION

Smart phones are the devices that are only used to call or text others. They become prevalent with much more powerful functions. Acting as pocket_PCs, smart phones can be used to deal with complicated_tasks such as sending/receiving e-mails, shopping, mobile-banking, etc. Screen locker is a fundamental service for smart phones to prevent the device from illegal use. It can the product privacy of users as well as avoid unintentional operations.

Classical screen lockers have been anticipated long time back. (1) Slide-to-Unlock,The user can unlock his/her phone through sliding his finger across a defined path. This method is simple to protect user's privacy. (2) PIN, always adopted on smart phones for unlocking. However, due to the relatively small screen and frequent unlocking request, it is inconvenient to set long and complex PIN on phones. For example, there are only four numbers allowed to be set as unlocking PIN in iPhone's default setting. (3) Graphical Password, like connecting at least four circles exposed in the phone screen. simple graphic passwords are easy to be peeked and guessed, while the complex pattern make user inconvenience. To enhance the security as well as the flexibility, many biometric authentication methods are introduced for screen lockers. The secrets of these methods cannot be easily spied and reproduced since they identify the user based on her accepted features. The biometric measures are grouped into two main categories : physiological biometrics and behavior biometrics. Physiological biometrics leverage the physiological features of human beings to identify the user, including recognitions of face , voice , fingerprint , ear , and so on. However, we find that (i) performances of these solutions are heavily influenced by external factors. For example, the face acquirement by the camera is severely affected by the illumination, resulting in the failure to identify user at night. Similarly (ii) Unlocking operation is a very frequent operation, of which energy consumption should be carefully considered. Camera is one of notorious energykillers in smart phones. (iii) lack of required hardware on current mainstream smartphones, like fingerprint scanner. The behavior biometrics is the other classification of biometric measure, which identify the user based on their behavior features, such as gesture.For example, user waves his smart phone, he always shakes in a similar way. This is because, without intentional changes, a specific person tends to follow his habits once the habits are developed.Based on above observations, we propose a handwaving biometric-based approach, called OpenSesame, to unlock the smart phone. Comparing with the existing methods,It increase the security of user information.

II. LITERATURE SURVEY

Surveys of the various papers, which are studied for this phase, are listed below. These papers were comprehensively analyzed and they are given below.

Dinei Flor enico and Cormac Herley [2007] states that A client component on users'machines recorded a variety of password strength, usage and frequency metrics. This allows us to measure or estimate such quantities as the average number of passwords and average number of accounts each user has, how many passwords she types per day, how often passwords are shared among sites, and how often they are forgotten.

IehabALRassan, HananAlShaher[2013] states that a new user authentication mechanism of mobile cloud computing using

fingerprint recognition system.

Roman V. Yampolskiy [2008] states that a survey and classification of the state-of-the-art in behavioral biometrics which is based on skills, style, preference, knowledge, motor-skills or strategy used by people.

Sukhdeep Singh, Dr. Sunil Kumar Singla[2013] states that recognizing people by their Ear is relatively new class of biometrics. Several reasons account for this trend: first,ear recognition does not suffer from some problems associated with other non contact biometrics.

III. MODULE DESCRIPTION

A. Android User

Mobile Client is an Android application which created and installed in the User's Android Mobile Phone. So that we can perform the activities.

B. Server Deployment

The Server will monitor the entire User's information in their database and verify them if required. Also the Server will store the entire User's information in the database.

C. Pattern Registration & Lock And Unlock Phone

In this user has to register his different pattern, so that we can able to train the system. Pattern will be validated by the server. Then code is send to the mobile to lock and another code is send to unlock the phone.

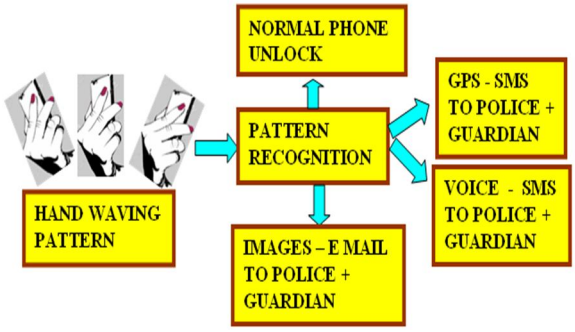
D. Pattern Emergency Matching

In this module we create a emergency matching system i.e. when the user is in the emergency condition he can show the pattern to rescue him from the difficulties.

E. GPS Based Location Identification And Emergency Support

In this module we design a emergency support system by using gps,when the user is in the bad circumstance he can show on of the pattern so that automatic gps value triggered and send as SMS,so that person can be saved.

IV. ARCHITECTURE DIAGRAM



V. WAVING CHARACTERIZATION

A. Waving Sensing

The tremendous growth of MEMS technology, there are many powerful sensors equipped in our smart phone today, such as camera, microphone, proximity sensor, accelerometer, gyroscope, and magnetic sensor etc. In our system, the selected sensor should be able to depict the handwaving. In addition, it should be energy-efficient, stable, cheap, and compatible for wide deployment in most kinds of smart phones. Obviously, the first three sensors cannot capture the phone"s motion. The gyroscope sensor is attractive because it is designed for measuring or maintaining purpose, based on the principles of angular momentum. Unfortunately, this kind of sensor is not a standard equipment in most smart phones due to its high price. The magnetic sensor is usually used for compass.

B. Data Collection

Investigating the uniqueness of handwaving, we collect the waving action data from 200 distinct smart phone users. For each

specific user, he is asked to shake the smart phone for more than 10 seconds and repeat for three times. Note that there is no special restriction on user‟s waving actions.He can shake the smart phone arbitrarily in each trail.Indeed.The data is collected in two sampling modes: fast and normal modes. In the fast mode, the accelerometer samples every 10 to 20 milliseconds, corresponding to the acceleration value change rate. There are 100 users‟ traces collected using this mode. In the normal mode, the sampling interval is 200 milliseconds and 100 users‟ traces are sampled.Clearly, using normal sampling mode of accelerometer loses some data, but saves energy. We will compare these two modes in the evaluation section. All the raw waving action are recorded as a sequence of tuples represented as ðxt, yt, ztÞ, where x, y, z donate the acceleration along the x-axis, y-axis and z-axis respectively, and t donates the time.

C. Waving Measurement

We define the waving function to measure the global geometric properties of the waving shapes, which is formally given by: f=S(A)where A={(xt0,yt0,zt0),(xt1,yt1,zt1),…(xtn,ytn,ztn)}.A is a set of raw waving tuples collected during t0 and tn. The waving function considers A as input and outputs a feature vector f. A good waving function should have the following properties:Efficiency. Since shape function will be performed in the smart phone, it should be simple enough to be fast and efficiently function. Invariance. In most time, the smart phone is working in mobile environments. The waving function should be insensitive to the position or direction change of smart phones. Robustness. Although the waving data generated by one person is similar, there always exist many noises and the sampling time is variable. Hence, the waving function should be robust to noise, blur, cracks, and dust in the waving.

VI. ALGORITHM/METHODOLOGY

SMS, GPS, E- Mail

VII. RESULTS AND DISCUSSION

A. Open Sesame

In this section, we present our unlocking method for smart phone called OpenSesame.

B. Overview

OpenSesame consists of four components: sensing, filter, fetcher, classifier, and matcher.Sensing: This component is used to record the user's handwaving action.Filter: When no waving or very low level sensing data is detected. For better feature extraction, we use filter component to wipe out the silent periods.Fetcher: The filtered raw tuples is feeded into fetcher component in which four waving functions are applied to fetch the waving features.Classifier: To discriminate the authorized users and unauthorized users, the support vector machine is employed in our system for classification.Matcher: The extracted feature is used to determine whether it matches the predefined one.

VIII. CONCLUSION

In this paper, we propose a novel behavioral biometric-based authentication approach called OpenSesame for smart phone. We design three waving functions to fetch the unique pattern of user's handwaving actions. By applying the SVM algorithm, the smart phone can accurately verify the authorized user with the pattern of handwaving action.This handwaving pattern can also used for emergency communication.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," NIST Special Publication, vol. 800, p. 145, 2011.
[2] S. De Capitani di Vimercati, S. Foresti, and P. Samarati, "Managing and accessing data in the cloud: Privacy risks and approaches," in Proc. 7th Int. Conf. Risk Security Internet Syst., 2012, pp. 1–9.1272 IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 27, NO. 5, MAY 2015
[3] P. Williams, R. Sion, and B. Carbunar, "Building castles out of mud: Practical access pattern privacy and correctness on untrusted storage," in Proc. 15th ACM Conf. Comput. Commun. Security, 2008, pp. 139–148.
[4] P. Paillier, "Public key cryptosystems based on composite degree residuosity classes," in Proc. 17th Int. Conf. Theory Appl. Cryptographic Techn., 1999, pp. 223–238.
[5] B. K. Samanthula, Y. Elmehdwi, and W. Jiang, "k-nearest neighbor classification over semantically secure encrypted relational data," eprint arXiv:1403.5001, 2014.
[6] C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proc. 41st Annu. ACM Sympos. Theory Comput., 2009, pp. 169–178.
[7] C. Gentry and S. Halevi, "Implementing gentry's fully-homomorphic encryption scheme," in Proc. 30th Annu. Int. Conf. Theory Appl. Cryptographic Techn.: Adv. Cryptol., 2011, pp. 129–148.

[8] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, pp. 612–613, 1979.
[9] www.android developer.com
[10] www.analog.com/DSP-Software-Kit
[11] http://developer.android.com/sdk/
[12] www.w3school.com
[13] http://developer.samsung.com/android/technical-docs/Gestures-in-Android