Mobile Hand Waving Behavior Analysis for Establishing Emergency Support and Protection

Anitha G
B. Tech Student
Department of Information Technology
KCG College of Technology, Tamilnadu, India

Sowbhakya M
B. Tech Student
Department of Information Technology
KCG College of Technology, Tamilnadu, India

Rajkumar Rajavel
Associate Professor
Department of Information Technology
KCG College of Technology, Tamilnadu, India

Abstract

In today's world most smartphone users relies on easy and weak password for the sake of convenience and memorability. However still there are various problems. The problem identified in this paper is that attackers can derive the password from the oily resides left on the screen or through shoulder surfing. So there is a need to figure out how to eliminate this issues. This paper proposes an effective solution for eliminating the problems. The main aim is to develop hand waving pattern by using application thereby aiding the smartphone users. It is an android application in which user's hand waving pattern is stored and recorded as user pattern which can be used for emergency purpose. The concept of support vector machine is used for user identification. This paper deploys three application based on the android device mobility pattern. First is normal phone unlocking, Second is safety application and third is emergency support to the user. If the safety or emergency pattern is matched, both GPS and camera are initiated to fetch location and photos. Voice is recorded and uploaded to the server. Both GPS and audio link are sent as SMS alert to both police and guardian.

Keywords: Hand waving, mobile locking and unlocking, user's safety, support vector machine, emergency support system

I. INTRODUCTION

Smartphones have become omnipresent platform of personal computing for users to access the internet and online services at anytime and anywhere. As more and more privacy information (e.g., passwords, CVS code of credit cards, and transaction information) are stored in smartphones, the risk of leakage information is becoming a major concern for the entire information society, so it is a necessity to keep the mobile phone secured. This can be done by automating the process to extent which unlocks the mobile phone by hand waving pattern. Earlier smartphone users approach the authentication mechanisms, such as PIN- based and pattern-based passwords, which can be easily derived from the oily resides or through shoulder surfing. It is an android application in which user hand waving pattern is stored and recorded as user's pattern and that can be used to unlock the mobile phone and for emergency purpose. First we are going to register two hand waving patterns. One for mobile unlocking system and another one are used for emergency purpose. In case of emergency, when the mobile phone is unlocked along with volume button an alert message is sent to the police or guardian which has been already registered by the user in the database. Later, GPS and camera are initiated to fetch location and photos. Voice is recorded and uploaded to the server. Finally GPS and audio link are sent as SMS to both police and guardian. Thus this paper concentrates on developing a system with a use of hand waving pattern that aids mobile users to keep their mobile phone secure and to alert the police or guardian. With the immense growth in the field of technology and widespread use of smartphone, it is possible to keep the mobile phone secured and to trace out the user if they struck in emergency. This application eliminates the issues of security. It not only has security features but it also includes features like pattern recognition, audio recording and alert system.

II. RELATED WORK

The authors of "Performance analysis of Touch-Interaction Behaviour for Active Smartphone Authentication" published is in International Journal of advance Research in computer Science and Management studies, investigates the reliability and applicability on the usage of user's touch screen interaction behaviour for active authentication on smartphones. The pin and pattern passcodes has been used for the sake of convenience and memorability. The attacker can easily trace the passwords using the oily residues left on the screen. To overcome this hand waving passcodes has been introduced. That the individual users have their own unique behavioural characteristics when performing touch-interaction operation, which are based on different rhythm, strength, and angle preferences of finger movement [3].

The author of the article titled "Touch me once and I know it's you implicit authentication based on touch screen patterns" describes the usage of password pattern on android. It enables user authentication by drawing a shape on the screen. The shape consists of an arbitrary number of strokes between nine dots. The pattern can be remembered as image. The user's memory improves the memorability every time when the user draws the pattern manually.The major drawback is security. Drawn passwords are easy to spy on and the other attack includes the smudge attack [2].

The author of the article titled "Smudge attack on smartphone touch screen" examines the feasibility of smudge attacks on touch screens for smartphones, and focus on analysis of the android password pattern. It investigates the conditions under which smudges are easily extracted. In the vast majority of settings, partial or complete pattern are easily retrieved and also emulates usage situations that interfere with pattern identification, and show that pattern smudges continue to be recognizable. It provides a preliminary analysis of applying the android password pattern. Its major disadvantage is smudges remains on the screen [1].

The author of the article titled "Shoulder surfing defence for recall based graphical passwords" describe that graphical passwords are often considered prone to shoulder surfing attacks, where attacker can easily steal the user password by peeking over his or her shoulder in the authentication process. The paper explores shoulder surfing defence for recall based graphical password system such as Draw a secret and background Draw a secret where users doodle their passwords on a drawing grid. The major disadvantage is passwords can be stolen by a bystander who observes over the users shoulder [5].

The author of the article titled "Batch incremental learning for mining data streams" describes about the classification of data. The continuous growth of data makes previously constructed data out dated. To avoid the data to be out dated the incremental classification model used. The major drawback is it leads to storage problem. Its contribution to our paper is to store the common use of passwords and deletes the unwanted history of passwords [4].

The author of the article titled "Taplogger inferring user inputs on smartphone touch screens using on-board motion sensors" examines the feasibility of inferring users input to a smartphone along with integrated motion sensor. Trojan application is installed to monitor the movement and gesture changes of the smartphone. Its disadvantage is an attack based on motion sensor that can be accessed by the background service with no security information [6].

The proposed system consists with three main features to deploy three applications based on the android device mobility pattern. First is normal phone unlocking, second is safety application, and third is emergency support to the user. If the emergency patterns are matched, both GPS and camera are initiated to fetch location and photos. Voice is recorded and uploaded to the server. Both GPS and audio link are sent as SMS alert to both police and guardian.

III. ARCHITECTURE OF HAND WAVING PROTECTIVE MECHANISM

In this research work, a novel architecture of Hand Waving Protective Mechanism is proposed as shown in Figure 1. In this architecture, the user will first try to unlock the mobile phone during the emergency situations. Here, the unlocking will be carried out by the user using two steps: (1) Hand waving pattern is applied through rotation orientation, and (2) emergency pattern is applied through pressing of volume button. After applying these steps it will triggers the alert message, captures image, records voice and share GPS location. SVM algorithm is used in the volume button for user identification.

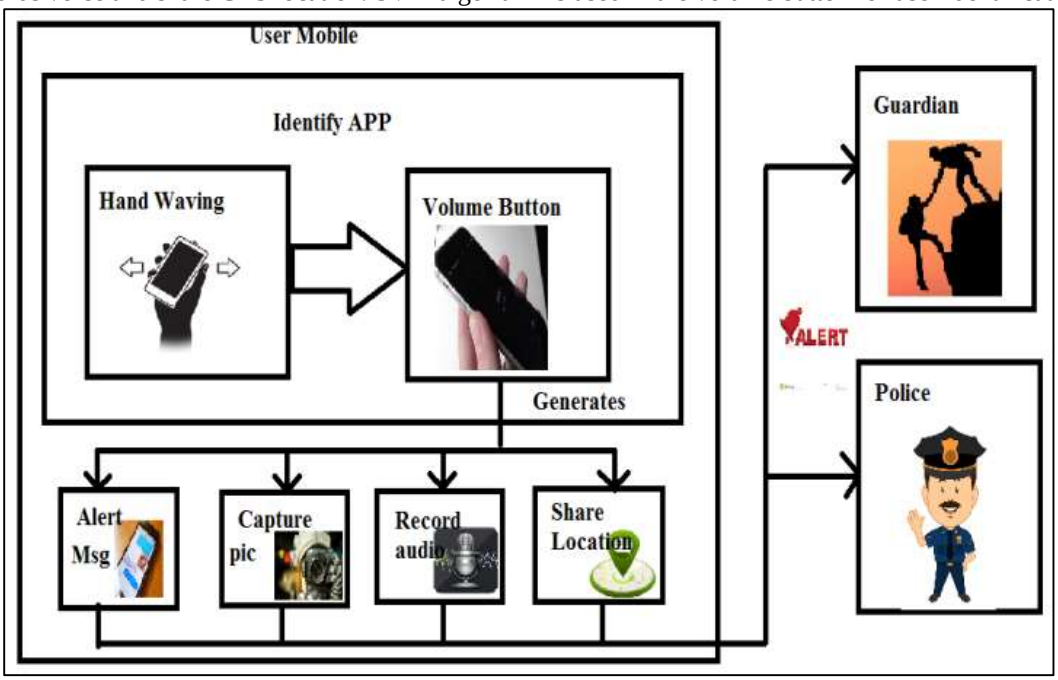

Fig. 1: Architecture of Hand Waving protective Mechanism

IV. EXPERIMENTAL SETTING

Android Eclipse is an integrated development environment used for developing this android application. SQLite database is used as backend and it stores the user's information. Android SDK is used as emulator to run the android application. In android Eclipse create an application and packages to design the screen by using the layout. Implement the java code for hand waving and volume button control for unlocking the mobile and initiating the emergency support in mobile application. Emergency support includes the triggering of alert message, image capture, audio capture, and location information service to the police and guardian. Here, the hand waving application control is initiated by the rotation orientation sensor available in the mobile device. To run the proposed hand waving and volume control application in smartphone, the apk file is installed in the mobile device and then turn on the auto rotate and GPS location options. Register the details (Password, Emergency password, guardian no, police no, Email ID, IP address). In case of any emergency, alert message will be sent to the police or guardian through IP address. The captured image and audio will be cached in Tomcat and old images and audio replaced by new images and audio.

The application performance is measure by testing with different level of users such as slow, medium, and fast. The obtained results for different unlocking mechanism are measured with respect to time as shown in Table 1.

Table – 1
Results of different unlocking mechanism

Unlocking Mechanisms	*Time (Seconds)*	*Security (%)*
Pin Password	*3.6*	*52*
Alpha Numeric Password	*4.4*	*56*
Pattern Password	*2.9*	*40*
Proposed Hand Waving Pattern	*1.6*	*90*

From the performance graph as shown in Figure 2 states that the proposed hand waving pattern takes less time to alert the police or guardian then the existing patterns.

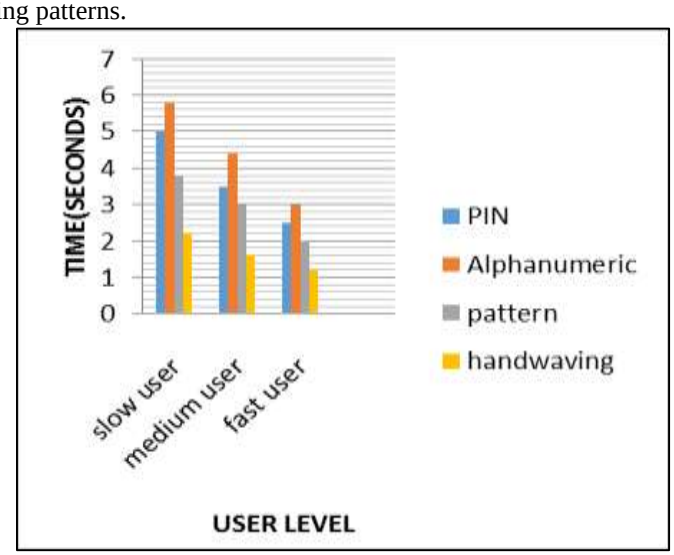

Fig. 2: TIME

From the performance graph as shown in Figure 3 states that the proposed hand waving pattern takes more security compared to other authentication mechanism

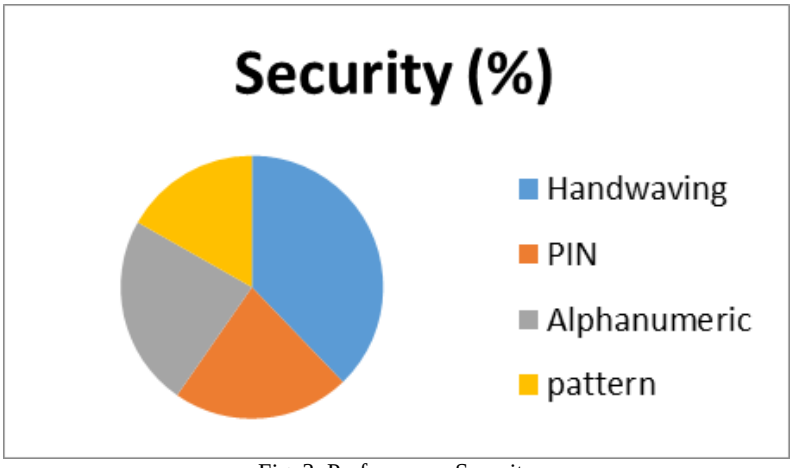

Fig. 3: Performance Security

Thus we conducted an analysis among different levels of user unlocking the mobile device in order to determine time and security. It is shown that the existing authentication mechanisms are less secured and it takes more time when compared to proposed hand waving pattern.

V. CONCLUSION AND FUTURE WORK

Thus it drives to the conclusion that helping the mobile users to unlock the system using hand waving pattern. First is to register two hand waving pattern, one is for mobile unlock and another one is for emergency pattern. This helps to secure the users emergency information. In case of any emergency, the alert message has been sent to police or guardian. In future this research work can be integrated to Internet of Things (IoT) based smart monitoring and safety system for lonely peoples.

REFERENCES

[1] Adam J.Avin, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M.Smith, "Smudge attacks on Smartphone Touch Screens" in Proc. 4th USENIX Conf. Offensive technology, USA , 2010.
[2] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, Heinrich Hussmann, "Touch Me Once And I Know it's you implicit Authentication based on Touch Screen Patterns", CHI 2012, May 5-10, 2012, Austin, Texas, USA.
[3] Chao Shen, Member, IEEE, Yong Zhang, Xiaohong Guan, Fellow, IEEE, and Roy A. Maxion, Fellow, IEEE, "Performance Analysis of Touch-Interaction Behaviour for Active Smartphone Authentication", IEEE transactions on information forensics and security, VOL. 11, No.3, March 2016
[4] Geoffrey Holmes, Richard Kirkby, Bernhard Pfahringer,"Batch-Incremental Learning For Mining Data Stream", University of Waikato, Hamilton, New Zealand, 2004.
[5] N.H.Zakaria, D.Griffiths, S.Brostoff, and J.Yan, "Shoulder Surfing Defence for Recall Based Graphical Passwords", in Proc. 7th Symp. Usable Privacy Secur., Pittsburgh, PA, USA, 2011, pp.1-12.
[6] ZhiXu, Kun Bai, Sencun Zhu,"Taplogger: Inferring user input on smartphone touch screens using on board motion sensors" Tucson, Arizona, USA, April 16-18, 2012.