Mobile Waving Girls Safety IOT: Android based Unlocking Mobile Waving pattern with waving pattern for Emergency support system

Shiyana J S
PG Scholar
Department of IT
St.Peter's University
Chennai, India

Prof.Malathi
Assistant Professor
Department of IT
St.Peter's University
Chennai, India

Abstract:

Smart phone users have their own unique behavioral characteristics when performing touch operations. Users tend to choose simple and weak pass codes for the sake of convenience and memorability, investigates the reliability and applicability on the usage of users touch-interaction behavior for active authentication on smart phones. Characteristics are reflected on personal with different strength, angle preferences and rhythm of touch interaction behavior. Android Application is developed in which users Hand Waving Pattern is recorded Stored as Users Pattern. We are using SVM Algorithm for User Identification. Modification of the project which is our implementation, is same waving pattern is used. We deploy three applications based on the android device mobility pattern. 1st one is normal phone unlocking, 2nd is Girls / children safety application, 3rd is Emergency support to the user. Girls safety / emergency Pattern is matched both GPS Camera are initiated to fetch Location and Photos. Voice is Recorded and uploaded to the Server. Both GPS Audio Link are sent as SMS Alert to both Police Guardian.

Index Terms—Convenience and memorability, Touch-interaction, Emergency Support, SMS Alert, GPS and Audio Link.

I. INTRODUCTION

Android is a Open source and Linux-based Operating System for mobile devices such as smart phones and tablet computers. Developed by the Open Handset Alliance, led by Goggle, and other companies. Android offers a unified approach to application development for mobile devices which means developers need only develop for Android, and their applications should be able to run on different

devices powered by Android. The first beta version of the Android Software Development Kit (SDK) was released by Goggle in 2007 where as the first commercial version, Android 1.0, was released in September 2008. On June 27, 2012, at the Goggle I/O conference, Goggle announced the next Android version, 4.1 Jelly Bean. Jelly Bean is an incremental update, with the primary aim of improving the user interface, both in terms of functionality and performance. The source code for Android is available under free and open source software licenses. Goggle publishes most of the code under the Apache License version 2.0 and the rest, Linux kernel changes, under the GNU General Public

Smart phones have become omnipresent platforms of personalcomputing for users to access the Internet and on line services at anytime and anywhere. As more and more privacy information (e.g., text messages, emails, and contact list) and security information (e.g., passwords, CVS code of credit cards, and transaction information) are stored in smart phones, the risk of information leakage is becoming a major concern for the entire information society, especially with the consideration that the smart phones are much easier to get lost or stolen in comparison with conventional computing platforms, according to a recent survey on US state of Cyber-crime.

The most common approach to address this problem is the use of authentication mechanisms, e.g., PIN-based and pattern- based pass codes, which have been integrated into smart phone systems like Android and Io's. Unfortunately, most smart phone users tend to choose simple and weak pass codes for the sake of convenience and memorability, and some recent studies have shown how simple an attacker can derive the PIN pass codes from the oily residues left on the screen or the pattern pass codes from the shoulder surfing attack. An attacker could even infer the pass codes from the accelerometer and gyroscope readings. Therefore, it is highly desirable to enhance smart phone authentication with a passive and transparent authentication mechanism without active user involvement, to further detect whether the logged in user is the true owner of a smart phone. An ongoing research project, the Active Authentication and Monitoring program initialized by DAR PA (Defense Advanced Research Project Agency), aims to develop computational behavioral traits for validating the identity of the users in a meaningful and continual manner (without requiring the deployment of additional hardware sensors), through how users interact with the computing systems. Of various potential solutions to this problem, a particularly promising technique is the use of touch-interaction behavior.

Compared with other biometric features on smart phones such as face and fingerprint, touch-interaction behavior does not require specialized sensors to collect data, and the detection process can be integrated seamlessly into users routine com- putting activities. Thus it can provide a non-intrusive and implicit solution for active authentication after entry-point based authentication by PIN-based or pattern-based pass codes, or could even substitute entry-point based authentication when reaching an acceptable level of performance. Although there is a growing body of literature about touch-interaction behavior for entry-point based authentication, there is little work on the use of this behavior for active smart phone authentication. The major reasons may be the lack of in-depth analysis for various types of touch operations in terms of stability, discriminant, and usability for active authentication, and examination for its applicability across different application tasks and different application scenarios. Others might be the difficulty of extracting effective features or building reliable models from touch-interaction behavior.

In this paper, we attempt to explore the reliability and applicability of user's touch-interaction behavior for active smart phone authentication across various application tasks and application scenarios. The rationale behind our work is that individual users have their own unique behavioral characteristics when performing touch-interaction operations, which are based on different rhythm, strength, and angle preferences of finger movement. We qualitatively analyzed touch-interaction behavior in user's daily usage, and focus our attention on common touch-sliding operations. We extracted both static and dynamic features to fine-grained characterize users touch behavior, and made a systematic exploration on the stability and discriminant of these features across different touch types. We applied four types of two-class classifier to perform the active authentication task. Then we conducted extensive experiments on the data from around 134900 touch operations of 71 participants, and examined the active authentication performance for various types of touch operations, at varying operation lengths, across different application tasks, and under different application scenarios.

II. PROBLEM DEFINITION

In the existing system there is no monitoring system for girls it should create many problems for them. And the no safety mechanism to protect the girl's from the misbehavioractivities. And in the existing system also there is no alert mechanism for the girl's safety it should be done by manually only.

A. Objective

Aim of the project is android based unlocking mobile waving pattern with waving pattern for emergency support system for girl's safety.

III.RELATED WORKS

A.SHOULDER SURFING DEFENCE FORRECALL-BASED GRAPHICAL PASSWORDS

Graphical passwords are often considered prone to shoulder- surfing attacks, where attackers can steal a user's password by peeking over his or her shoulder in the authentication process. In this paper, we explore shoulder surfing defense for recall-based graphical password systems such as Draw-A- Secret and Background Draw-A-Secret, where users doodle their passwords (i.e. secrets) on a drawing grid. We propose three innovative shoulder surfing defense techniques, and conduct two separate controlled laboratory experiments to evaluate both security and usability perspectives of the proposed techniques. One technique was expected to work to some extent theoretically, but it turned out to provide little protection. One technique provided the best overall shoulder surfing defense, but also caused some usability challenges. The other technique achieved reasonable shoulder surfing defense and good usability simultaneously, a good balance which the two other techniques did not achieve. Our results appear to be also relevant to other graphical password systems such as Pass-Go.

B. TOUCH ANALYTICS: ON THE APPLICABILITY OF TOUCHSCREEN INPUT AS A BEHAVIORAL BIOMETRIC FOR CONTINUOUS AUTHENTICATION

We investigate whether a classifier can continuously authenticate users based on the Way they interact with the touch- screen of a smart phone. We propose a set of 30 behavioral touch features that can be extracted from raw touchscreen logs and demonstrate that different users populate distinct subspaces of this feature space. In a systematic experiment designed to test how this behavioral pattern exhibits consistency over time, we collected touch data from users interacting with a smart phone using basic navigation maneuvers, i.e., up-down and left-right scrolling. We propose a classification framework that learns the touch behavior of a user during an enrolment phase and is able to acceptor reject the current user by monitoring interaction with the touch screen. The classifier achieves a median equal error rate of 0 percent for intra- session authentication, 2percent-3 percent for inter-session authentication and below 4percent when the authentication test was carried out one week after the enrolment phase. While our experimental findings

disqualify this method as a standalone authentication mechanism for long-term authentication, it could be implemented as a means to extend screen-lock time or as a part of a multi-modal biometric authentication system.

C. THE SCIENCE OF GUESSING: ANALYZING AN ANONY- MOUS CORPUS OF 70 MILLION PASSWORDS

We report on the largest corpus of user-chosen passwords ever studied, consisting of antonym zed password histograms representing almost 70 million Yahoo! users, mitigating privacy concerns while enabling analysis of dozens of sub populations based on demographic factors and site usage characteristics. This large data set motivates a thorough statistical treatment of estimating guessing difficulty by sampling from a secret distribution. In place of previously used metrics such as Shannon entropy and guessing entropy, which cannot be estimated with any realistically sized sample, we develop partial guessing metrics including a new variant of guess work parameterized by an attackers desired success rate. Our new metric is comparatively easy to approximate and directly relevant for security engineering. By comparing password distributions with a uniform distribution which would pro- vide equivalent security against different forms of guessing attack, we estimate that passwords provide fewer than 10 bits of security against an on line, trawling attack, and only about 20bits of security against an optimal offline dictionary attack. We find surprisingly little variation in guessing difficulty; every identifiable group of users generated a comparably weak pass- word distribution. Security motivations such as the registration of a payment card have no greater impact than demographic factors such as age and nationality. Even proactive efforts to nudge users towards better password choices with graphical feedback make little difference. More surprisingly, even seemingly distant language communities choose the same weak passwords and an attacker never gains more than a factor of 2 efficiency gain by switching from the globally optimal dictionary to a population-specific lists.

D. MULTI-TOUCH AUTHENTICATION ON TABLETOPS

The introduction of tabletop interfaces has given rise to the need for the development of secure and usable authentication techniques that are appropriate for the co-located collaborative settings for which they have been designed. Most commonly, user authentication is based on something you know, but this is a particular problem for tabletop interfaces, as they are particularly vulnerable to shoulder surfing given their remit to foster co-located collaboration. In other

words, tabletop users would typically authenticate in full view of a number of observers. In this paper, we introduce and evaluate a number of novel tabletop authentication schemes that exploit the features of multi-touch interaction in order to inhibit shoulder surfing. In our pilot work with users, and in our formal user-evaluation, one authentication scheme -Pressure-Grid - stood out, significantly enhancing shoulder surfing resistance when participants used it to enter both PINs and graphical passwords.

E. TOUCH ME ONCE AND I KNOW ITS YOU! IMPLICIT AUTHENTICATION BASED ON TOUCH SCREEN PAT- TERNS

Password patterns, as used on current Android phones, and other shape-based authentication schemes are highly usable and memorable. In terms of security, they are rather weak since the shapes are easy to steal and reproduce. In this work, we introduce an implicit authentication approach that enhances password patterns with an additional security layer, transparent to the user. In short, users are not only authenticated by the shape they input but also by the way they per-form the input. We conducted two consecutive studies, a lab and a long-term study, using Android applications to collect and log data from user input on a touch screen of standard commercial smart phones. Analyses using dynamic time warping (DTW) provided first proof that it is actually possible to distinguish different users and use this information to increase security of the input while keeping the convenience for the user high.

F. SMUDGE ATTACKS ON SMART PHONE TOUCH SCREENS

Touch screens are an increasingly common feature on personal computing devices, especially smart phones, where size and user interface advantages accrue from consolidating multiple hardware components (keyboard, number pad, etc.) into a single software definable user interface. Oily residues, or smudges, on the touch screen surface, are one side effect of touches from which frequently used patterns such as a graphical password might be inferred. In this paper we examine the feasibility of such smudge attacks on touch screens for smart phones, and focus our analysis on the Android password pattern. We first investigate the conditions (e.g., lighting and camera orientation) under which smudges are easily extracted. In the vast majority of settings, partial or complete patterns are easily retrieved. We also emulate usage situations that interfere with pattern identification, and show that pattern smudges continue to be recognizable. Finally, we provide a preliminary analysis of applying the information learned in a smudge attack to guessing an Android password pattern.

G. TAP LOGGER: INFERRING USER INPUTS ON SMART PHONE TOUCHSCREENS USING ON-BOARD MOTION SENSORS

Today's smart phones are shipped with various embedded motion sensors, such as the accelerometer, gyroscope, and orientation sensors. These motion sensors are useful in sup- porting the mobile UI innovation and motion-based commands.However, they also bring potential risks of leaking user's private information as they allow third party applications to monitor the motion changes of smart phones. In this paper, we study the feasibility of inferring a user's trap inputs to a smart phone with its integrated motion sensors.

IV. EXISTING SYSTEM

Unfortunately, most smart phone users tend to choose simple and weak pass codes for the sake of convenience and memorability.

1) Dis Advantages:

There is no security
There is no pattern recognition for emergency system
No recording system

V. PROPOSED SYSTEM

Investigates the reliability and applicability on the usage of users touch-interaction behavior for active authentication on smart phones. Smart phone users have their own unique misbehaviorcharacteristics when performing touch operations. These personal characteristics are reflected on different rhythm, strength, and angle preferences of touch interaction behavior. Android Application is developed in which users Hand Waving Pattern is recorded Stored as Users Pattern. We are using SVM Algorithm for User Identification.

VI. MODIFICATION PROCESS

In the process of modification, is same waving pattern is used. We deploy three applications based on the android device mobility pattern. 1st one is normal phone unlocking, 2nd is Girls / children safety application, 3rd is Emergency support to the user. Girls safety / emergency Pattern is matched both GPS Camera are initiated to fetch Location and Photos. Voice is Recorded and uploaded to the Server. Both GPS Audio Link are sent as SMS Alert to both Police Guardian. .

1) Advantages:

High reliability
Pattern recognition for emergency system for girls safety

VII. REQUIREMENT ANALYSIS

Requirement analysis determines the requirements of a new system. This project analyses on product and resource requirement, which is required for this successful system. The product requirement includes input and output requirements it gives the wants in term of input to produce the required output. The resource requirements give in brief about the software and hardware that are needed to achieve the required functionality.

A. Hardware Requirement

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design. It shows what the systems do and not how it should be implemented.

Hard disk : 120 GB
Monitor : 15 color with vgi card support
Ram : Minimum 256 MB
Processor : Pentium iv and above (or) equivalent
Processor speed : Minimum 500 MHZ

B. Software Requirement

The software requirements are the specification of the system. It should include both a definition and a specification of requirements. It is a set of what the system should do rather than how it should do it. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating cost, planning team activities, performing tasks and tracking the teams and tracking the teams progress throughout the development activity.

Platform : Windows Xp/7/8
Front End : Java-JDK1.7,Android-sdk and Eclipse, Apache tomcat
Back End : MYSQL

VIII. METHODOLOGY

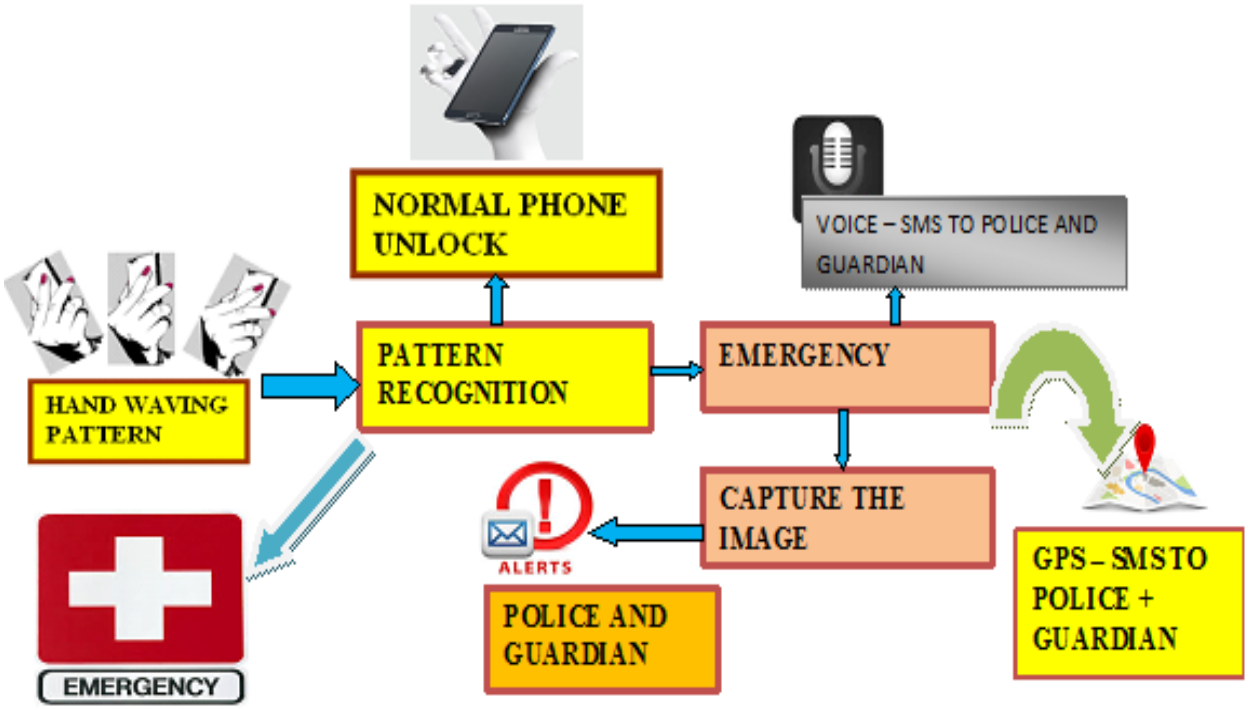
Smart phones are no longer the devices theater only used to call or text others. They become prevalent with much more powerful functions. Acting as pocket PCs, smart phones can be used to deal with complicated tasks such as sending/receiving e-mails, shopping, mobile payment, etc. Screen locker is a fundamental utility for smart phones to prevent the devicefrom unauthorized use. For example, the Apple iPhones and Android phones can lock themselves

automatically after being idle for a short time. It can protect the privacy of users as well as prevent unintentional operations.
Classical screen lockers have been proposed long time back.

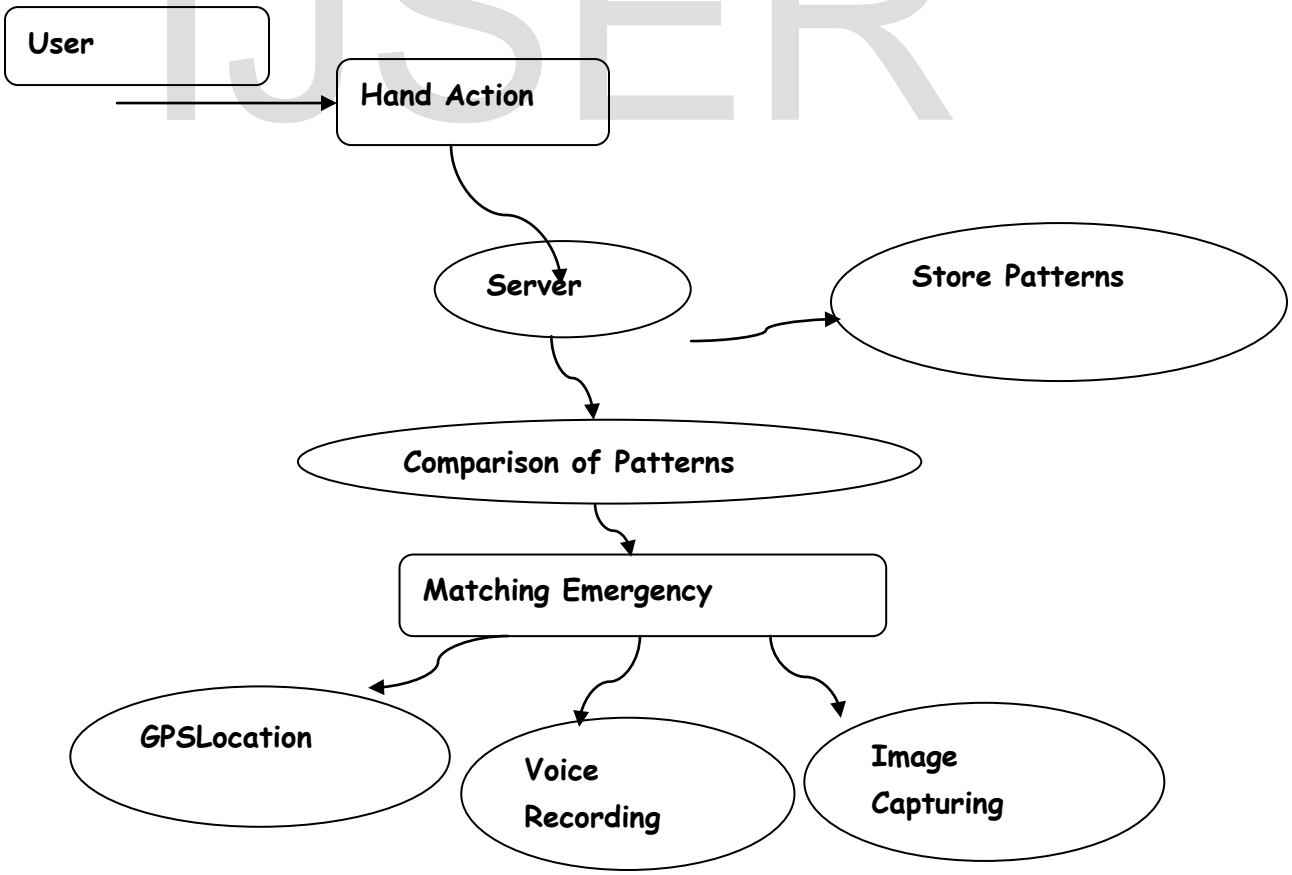
(1)The most widely used one is Slide-to-Unlock. The user can unlock his/her phone through sliding his finger across a defined trajectory. This method is too simple to protect user's privacy.

(2)PIN, the most common method used by traditional digital device, is always adopted on smart phones for unlocking smart phones. 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 iPhones default setting. Such a short and simple PIN can often be easily guessed.

(3) The user cans pre-define a graphical password, like connecting at least four circles shown in the screen. Being similar to the PIN, simple graphic passwords are easy to be peeked and guessed, while the complex pattern may confuse the user and make inconvenience. To enhance the security aswell 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 natural features. The biometric measures are grouped into two main categories: physiological biometrics and behavior biometrics. Physiological biometrics leverages 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, it is hard to distinguish the voice from the ambient interference in extremely noisy environments, like subway or restaurant, has to establish the connection to communicate with the Users. The Server will update the each Users activity in its database. The Server will authenticate each user before they access the Application. So that the server will prevent the unauthorized user from accessing the application.



IX. DATA FLOW



UML DIAGRAMS

UML is simply anther graphical representation of a common semantic model. UML provides a comprehensive notation for the full lifecycle of object-oriented development.

ADVANTAGES

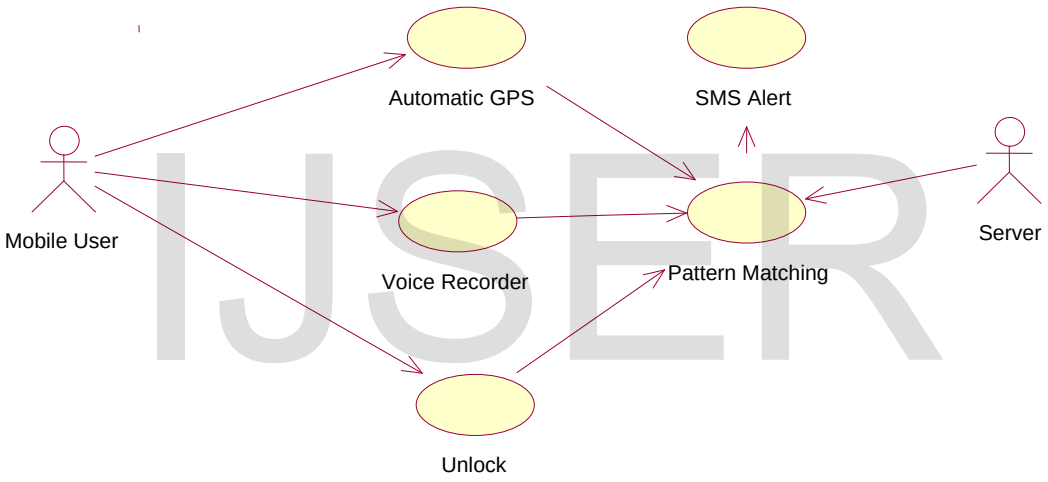
- To represent complete systems (instead of only the software portion) using object oriented concepts
- To establish an explicit coupling between concepts and executable code
- To take into account the scaling factors that are inherent to complex and critical systems
- To creating a modeling language usable by both humans and machines

UML defines several models for representing systems

- The class model captures the static structure
- The state model expresses the dynamic behavior of objects
- The use case model describes the requirements of the user
- The interaction model represents the scenarios and messages flows
- The implementation model shows the work units
- The deployment model provides details that pertain to process allocation

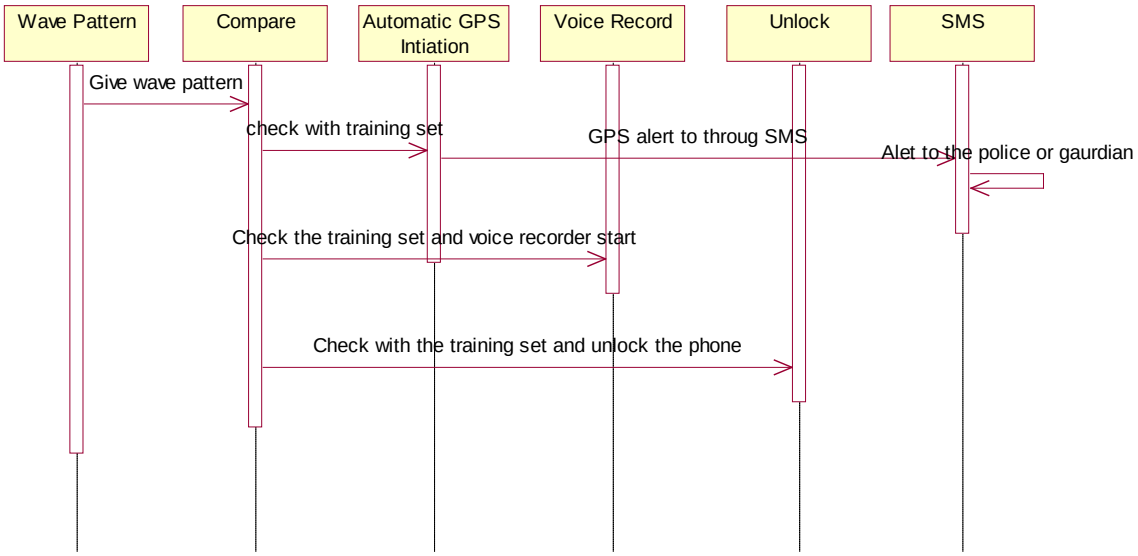
USECASE DIAGRAM

Use case diagrams overview the usage requirement for system. They are useful for presentations to management and/or project stakeholders, but for actual development you will find that use cases provide significantly more value because they describe “the meant” of the actual requirements. A use case describes a sequence of action that provides something of measurable value to an action and is drawn as a horizontal ellipse.



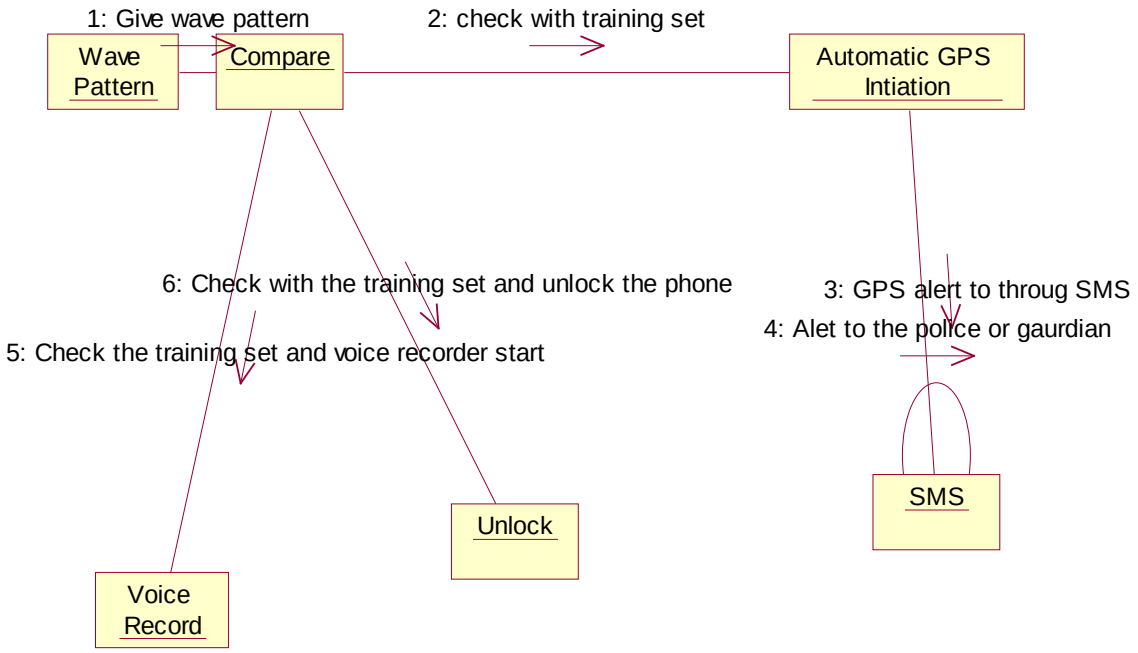
SEQUENCE DIAGRAM

Sequence diagram model the flow of logic within your system in a visual manner, enabling you both to document and validate your logic, and commonly used for both analysis and design purpose. Sequence diagram are the most popular UML artifact for dynamic modeling, which focuses on identifying the behavior within your system.



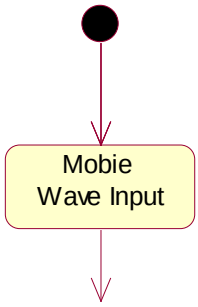
COLLABORATION DIAGRAM

Another type of interaction diagram is the collaboration diagram. A collaboration diagram represents a collaboration, which is a set of objects related in a particular context, and interaction, which is a set of messages exchange among the objects within the collaboration to achieve a desired outcome.

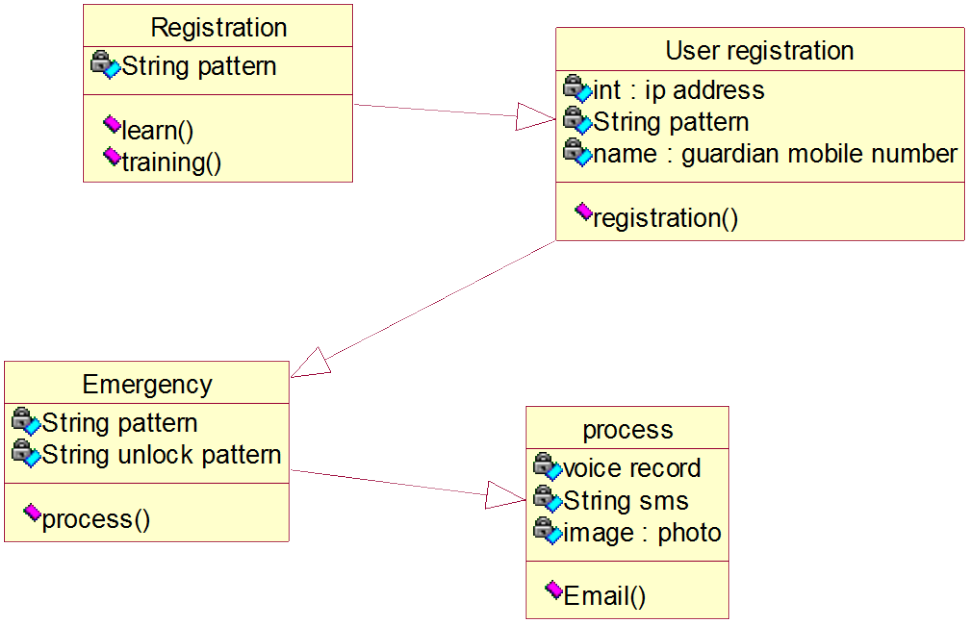


ACTIVITY DIAGRAM

Activity diagram are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. The activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. Activity diagram consist of Initial node, activity final node and activities in between.



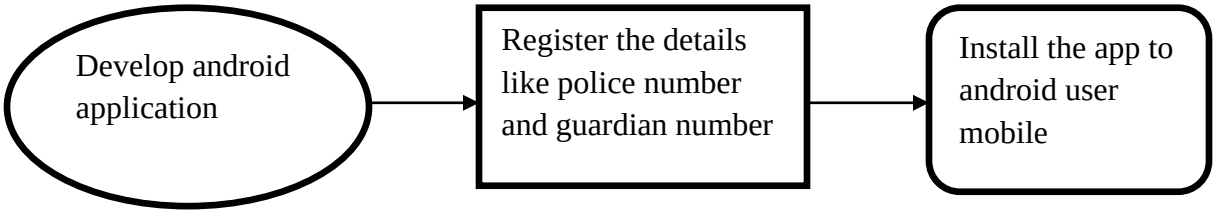
CLASS DIAGRAM



X.IMPLEMENTATION DETAILS

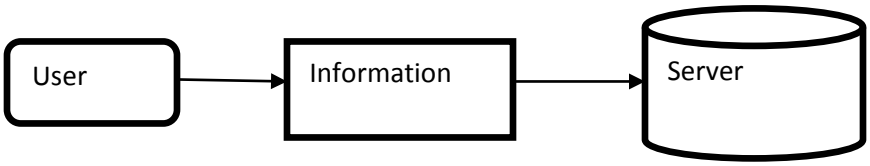
A.ANDROID USER

Develop an android application. Develop an android application. Mobile Client is an Android application which created and installed in the Users Android Mobile Phone. So that we can perform the activities. The Application First Page Consist of the User registration Process. Well create the User Login Page by Button and Text Field Class in the Android. While creating the Android Application, we have to design the page by dragging the tools like Button, Text field, and Radio Button. Once we designed the page we have to write the codes for each. Once we create the full mobile application, it will generated as Android Platform Kit (APK) file. This APK file will be installed in the Users Mobile Phone an Application.



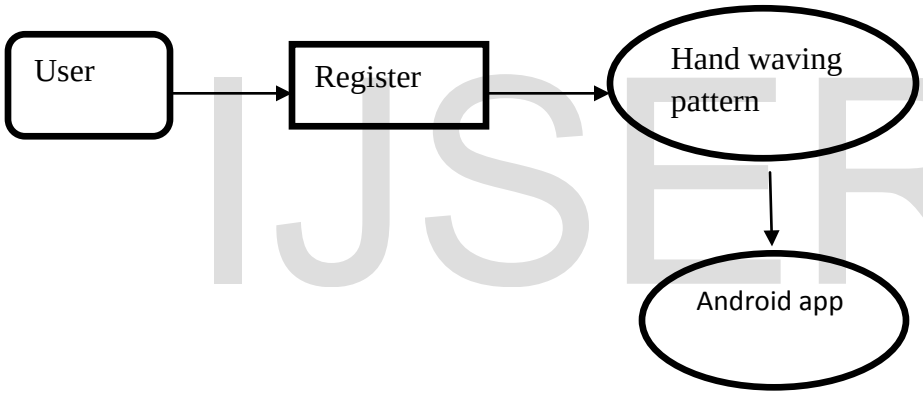
B. SERVER DEPLOYMENT

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



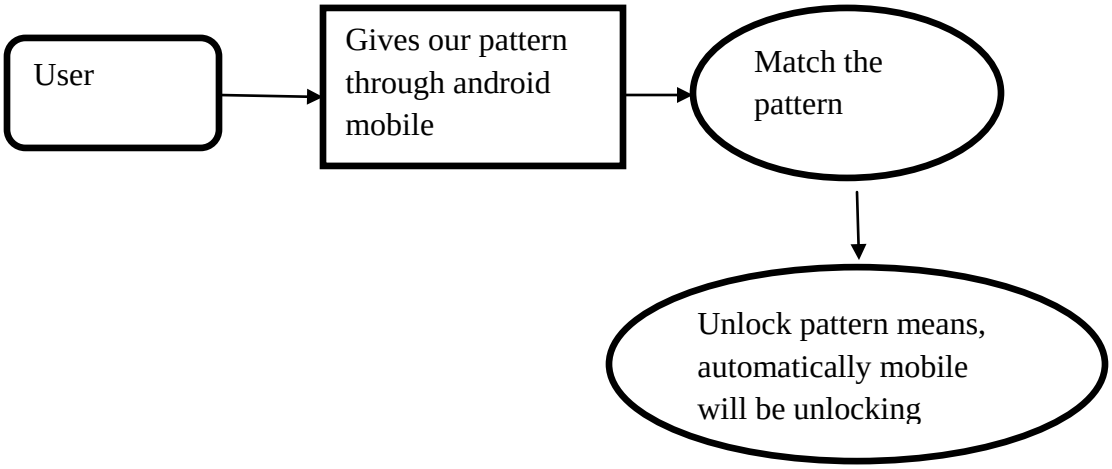
C. PATTERN REGISTRATION

In this user has to register his different pattern, so that we can able to train the system. If we train the system with different pattern so that user show any one of pattern that will be validated by the server.



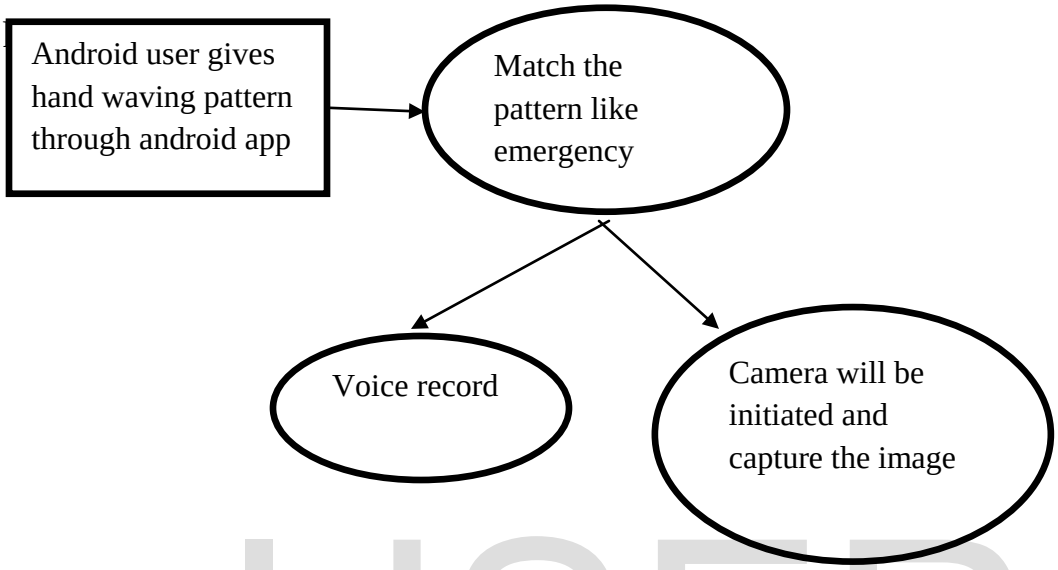
D. LOCK AND UNLOCK PHONE

In this function we create a concept of locking and unlock- ing the phone ie user can lock and unlock the other phone by using code send to the mobile to lock and another code is send to unlock the phone.



E. PATTERN EMERGENCY MATCHING

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



XI. CONCLUSION

We explored touch-interaction behavior based active authentication under various application scenarios. The results showed that touch-interaction behavior, under the scenarios which have long observation in the model-training phase or small time span between the model-training phase and detection phase would produce good and robust authentication performance. But these conditions may constrain the flexibility of this mechanism in some real-world application scenarios. One possible way is to employ effective online incremental learning strategy [36] to continuously learn the new-coming touch operations, and to increasingly enhance the validity and flexibility of the authentication model. Fig. 8. Data Flow REFERENCES [1] PwC, CSO Magazine , ”The CERT Division of the Software Engineering Institute at Carnegie Mellon University”, and The U.S. Secret Service. (May 2014). 2014 US State of Cybercrime Survey. [Online]. Available: http://www.pwc.com/us/en/increasing-it-effectiveness/ publications/2014-us-state-of-cybercrime.html , [2] J. Bonneau, ”science of guessing: Analyzing an anonymized corpus of 70 million passwords”, in Proc. IEEE Symp. Secur. Privacy, May 2012, pp. 538552, [3] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, ”Smudge attacks on smartphone touch screens”, in Proc. 4th USENIX Conf. Offensive Technol., Washington, DC, USA, 2010, pp. 17. , [4] 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. 112. , [5] Z. Xu, K. Bai, and S. Zhu, , ”TapLogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors”, in Proc. 5th ACM Conf. Secur. Privacy Wireless Mobile Netw., 2012, pp. 113124., [6] E. Owusu, J. Han, S. Das, A. Perrig, and J. Zhang, ”ACCessory: Password inference using accelerometers on smartphones”,in Proc. 12th Workshop Mobile Comput. Syst. Appl., 2012, pp. 914. , [7] Active Authentication, ”document DARPA-BAA-12-06”,Defense Advanced Research Projects Agency, Arlington, VA, USA, 2012. , [8] 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 Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 136148, Jan. 2013 ,