ISSN 2395-1621

Authentication system for MBanking Application Using Multitouch Gesture and FAST

Suraj Choudhari[#1], Nilesh Jagtap[#2], Ravi Rathod[#3], Soham Bagwe[#4]

[1]sur00744@gmail.com

[2]nil4200@gmail.com

[3]54ravirathod@gmail.com

[4]atom_150@rediffmail.com

[#1234] Dept. of Computer Engineering, B.S.C.O.E.R.

Savitribai Phule Pune University, Maharashtra, India.

ABSTRACT

This paper propose a simple yet elegant method called Finger Gesture Authentication System using Touch Screen (FAST) to solve the authentication problem in a ubiquitous manner. This type of authentication approach is very efficient and useful in case of sensitive applications on android touch screen devices such as MBanking app. The core idea of FAST is that, instead of remembering a sequence of characters as a secret users have to remember a gesture (which is internally stored as sequence of positions as the secret). A canonical set of 22 Multitouch gestures was defined using characteristics of hand and finger movement. Then, a Multitouch gesture matching algorithm robust to orientation and translation was developed. In addition, the study showed that user-defined gestures yield the highest recognition rate among all other gestures, whereas the use of multiple gestures in a sequence aids in boosting verification accuracy. The study showed that it is feasible for a user to recall user-defined gestural passwords and it is observed that the recall rate growths over time. It is also noticed that accomplishment a user-defined gesture over a customized background image does result in higher verification performance. In terms of usability, the study shows that users did not have difficulty in performing Multitouch gestures as they all rated each gesture as easy to perform.

***Keywords*— Multitouch, FAST(Finger gesture Authentication System for Touch screen devices), FAR(False Accept Rate), FRR(False Reject Rate), MBanking.**

ARTICLE INFO

Article History

Received :18th February, 2015

Received in revised form :

22nd February, 2015

Accepted :25thFebruary, 2015

Published online :

26th February 2015

I. INTRODUCTION

Aim of this project deal with securing the sensitive data stored and accessed from mobile devices which makes user authentication a problem of paramount importance. Aim of the project is to use gestures on touch screen devices as an authentication media. This project introduces FAST (Finger gestures Authentication System using Touch screen), a novel touch screen based verification approach on mobile devices. This project extracts user's touch screen co-ordinates and matches it with database signs. Authentication will pass only if user draws exact gesture in the same order that is selected during registration process. Authentication or automatic logouts following periods of inactivity are likely to be counterproductive. The need for strong authentication is countered by the still clumsy input methodology of such devices and the different user expectations for interaction models, especially when compared to the standard authentication solutions. As shown in a study of over 6,000,000 passwords, 91% of all user passwords belong to a list of just 1,000 common passwords (e.g., 8.5% users use either "password" or "123456"as their passwords). Moreover, the additional hardware cost makes standard biometric authentication techniques to be still unpopular on mobile devices. The design of a multi-touch gesture based mobile authentication solution to provide additional enhanced protection of mobile devices. Research into using digital sensor gloves, consisting of multiple 6-degrees of freedom IMU sensors, to cross validate and complement the touch gesture based user authentication process.

An empirical study and evaluation of the applicability of using multi-touch gesture inputs for implicit and continuous user identification, That studies the trade-off Between false reject and false accept rates. The rest of this paper is organized as follows.

We are going to deal with the kind of problem for secure authentication for sensitive applications such as MBanking app where need of authentication for users is high. Thus we are going to develop a MBanking app and

decided to implement a post login authentication system for it using Multitouch gestures and FAST (Finger gesture Authentication System for Touch screen devices).

II. LITERATURE SURVEY

Technological advances in computing and I/O capabilities as well as network connectivity are shifting the focus from PCs to mobile devices. Market analysis predicts that in 2015 there will be 1.5 billion smart phones and 640 million tablets in use worldwide. Moreover, companies, universities, and government agencies are increasingly handing out mobile computing systems and applications that allow their employees to work remotely while continuously staying connected to the organization's infrastructure. The popularity of mobile devices makes them a frequent storage medium for sensitive information (e.g., confidential documents, trade secrets, credentials). As mobile devices are easily lost or stolen, the problem of securing the user access to this data becomes one of paramount importance. As a first defence step, user authentication is quintessential to protecting a system. However, mobile devices introduce a trade-off between the security and usability of most existing authentication solutions: one-shot authentication solutions are vulnerable to theft and loss, while periodic authentication or automatic logouts following periods of inactivity are likely to be counterproductive. The need for strong authentication is countered by the still clumsy input methodology of such devices and the different user expectations for interaction models, especially when compared to the standard authentication solutions. As shown in a study of over 6,000,000 passwords, 91% of all user passwords belong to a list of just 1,000 common passwords (e.g., 8.5% users use either "password" or "123456" as their passwords). Moreover, the additional hardware cost makes standard biometric authentication techniques to be still unpopular on mobile devices. To address the pressing demand for a more secure *and* user friendly mobile authentication solution, we design FAST; a touch based seamless user authentication mechanism that supports both passive and continuous authentication for mobile users based on user's touch gestures. FAST takes advantage of the fact that during their interaction with mobile devices, users reveal their unique touch features, such as finger pressure and trajectory, the speed and acceleration of movement. An essential advantage of our approach is its transparency to the user: the touch data is captured by sensors without disrupting normal user-device interactions. During the post login stage, the traditional explicit authentication process is triggered only when FAST detects that the current user is likely different from the smart phone owner (i.e., loss or theft of the device). Furthermore, we have built a digital sensor glove with IMU digital combo boards ITG3200/ADXL345.The glove provides 6 degrees of freedom and allows us to collect finegrainedbiometric information of finger movements. We have used the digital glove to complement and validate touch gesture data. Thus, the main contributions of our work are the following:

1. The design of a multi-touch gesture based mobile authentication solution to provide additional enhanced protection of mobile devices.

2. Research into using digital sensor gloves, consisting of multiple 6-degrees of freedom IMU sensors, to cross validate and complement the touch gesture based user authentication process.

3. An empirical study and evaluation of the applicability of using multi-touch gesture inputs for implicit and continuous user identification that studies the trade-off between false reject and false accept rates

III. LIMITATION OF PREVIOUS SYSTEM

Present System in Use

1. Encryption/Decryption of data.
2. Transfer user request data using Steganography Random bit Technique.

Flaws in Current System

1. User has to remember user id and password. It is very difficult if user forgets his password.
2. User doesn't have the full control over his account and application crashes and doesn't work properly

IV. PROBLEM STATEMENT

This paper proposes a simple yet elegant method called Finger Gesture Authentication System using Touch Screen (FAST) to solve the authentication problem in a ubiquitous manner. The fundamental idea of FAST is based on premise that "humans are good at identifying remembering and recollecting gesture patterns than text patterns. The core idea of FAST is that, instead of remembering a sequence of characters as a secret user's have to remember a gesture (which is internally stored as sequence of positions as the secret). Due to wireless networks feature of being open and the deficiency of wireless protocol more and more means of attack have been offered, therefore it is important to share secret password between sender and recipient. Banking application allows user to control the bank account and the entire activities from mobile device. When it is difficult and impractical to go to bank then one can use this application to do banking transaction, money transfer, etc. User can monitor and control their banking activities using this application.

V. PROPOSED SYSTEM

A. System Architecture

As this paper suggests such a system for authentication approach for sensitive applications on touch screen android devices it can be implemented such a system with the help of following approach

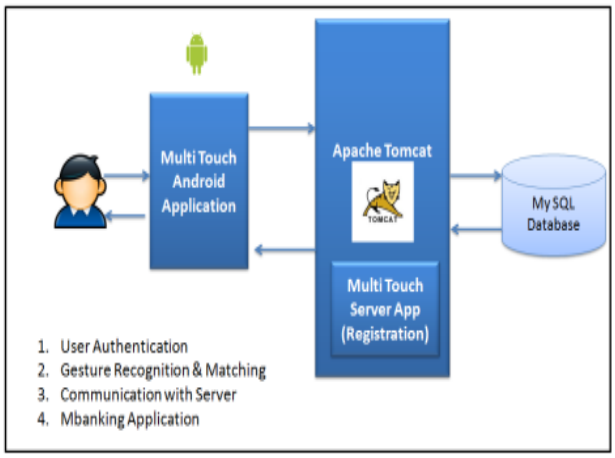

Fig.3 System Architecture

The Gesture Patterns[1]**:** Previous work has explored the feasibility of applying keystroke dynamics and typing patterns for user identification for personal computers – keystrokes can be continually sampled by intercepting output from a keyboard. A study on user's perceptions of authentication on mobile devices shows that users prefer a system that can implicitly and continuously perform user authentication without disrupting the normal user-mobile device interaction. Furthermore, Jacobson et al proposed an implicit user authentication framework and studied using recorded phone call history and location for continuous user authentication. Unlike PCs, Touchscreen is the primary input medium on smart phones and tablets. Multi-touch inputs embed behaviour

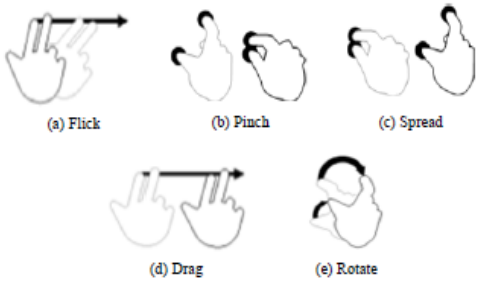

Fig.4 Example Gestures

The FAST Framework [4]**:**

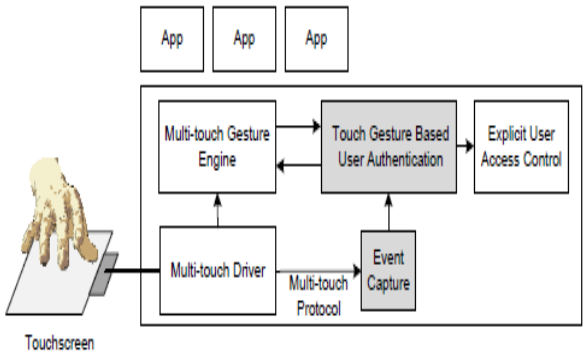

Fig.5. FAST Design

Characteristics that are user specific and can be used for detecting mobile users. We classify touch input into three categories: touch gestures (e.g., flick, spread, pinch, drag, and tap), virtual typing (e.g, typing using a Touchscreen based keyboard, entering a phone number using touch); and touch based drawing (e.g., drawing shapes using fingers). For each category, user specific features can be extracted from traces collected from a device Touchscreen. We propose a touch gesture based user authentication system, FAST (Finger gestures Authentication System using Touchscreen), that focuses on post-login user authentication. Figure 2 shows a high level diagram of the design. As long as the smart phone is used, FAST authenticates the user continuously. After user login, FAST continues to authenticate the mobile user in the background using intercepted touch data from normal user-smart phone interactions. To achieve the objective, FAST relies on gesture based smart phone owner detection. The detection approach is invoked on-demand whenever touch inputs are received and is transparent to the smart phone user. Only when there is sufficient evidence that the current user is not the smart phone owner, traditional user authentication is activated.

B. Algorithm

Our approach relies on classification algorithms for authentication purposes which can help us implementing such kind of authentication system. We have evaluated the use of three classification algorithms, **(i) Decision tree, (ii) Random Forest and (iii) Bayes net classifier**. We describe each in the following.

(i) Decision Trees: Decision tree is a popular machine learning approach that can be used to discover patterns in the data and classify data based on the learned patterns. The basic idea of constructing a good decision tree is to build it with high precision and small-scale. It should have the smallest leaf nodes and the depth of the leaf nodes should all be the smallest. Hence a normal decision tree algorithm uses some evaluation method, such as information entropy, to choose an attribute that can best differentiate the data sets, and use it as a decision node and split the data sets in every step.

(ii) Random Forest: Random Forest is an ensemble classifier that consists of many decision trees and outputs the class
that is the mode (most frequently occurring) of the class's output by individual trees . It has been widely used in many real-life classification problems, such as image classification , object class segmentation and many other applications. Random forest normally selects attributes in the same purpose as decision tree; however, it creates a set of trees. A Random Forest normally selects attributes in a similar
manner to decision trees; however, it creates a set of trees.

(iii) Bayes Net Classifier: Bayes net is a probabilistic graphical model algorithm that has been widely applied because of its easy to use and good performance. Formally, Bayesian networks are directed acyclic graphs whose nodes represent

random variables in the Bayesian sense. The nodes may be observable quantities, latent variables, unknown parameters or hypotheses. Edges represent conditional dependencies; nodes which are not connected representing variables which are conditionally independent of each other. Each node is associated with a probability function that takes as input a particular set of values for the node's parent variables and gives the probability of the variable represented by the node.

VI. EXPERIMENTATION

While deciding to perform experimentation for implementing such a system with using JAVA for server and web side and obviously android SDK (Software Development Kit) for android app of MBanking. Server side has the database for Mbanking as well as gesture passwords. In practically a user who is a customer of bank and wish to have a facility of Mbanking app has to submit a form to bank we use the same concept. A user which is an account holder of bank has to submit a application form giving his details and requesting Mbanking app. Then on server side bank has appointed an administrator who can add users according to forms in the database by giving a first time user id and password. Then user can login into bank's website through this user id and password and can change his password for further use. After logging in to bank's website user will create his own gesture password with number of gestures and their unique sequence. He then raises a request to a lot him that password for Mbanking app. Request raised by user has to be approved by administrator on server. Then user installs the android app for Mbanking on his android touch screen device such as smart phone or tablet and can login with his id and password first. After that he has to be authenticated with the gesture password and can then enjoy the banking transactions such as viewing detailed and mini enquiry of his accout, transferring funds to another account and such other

VII. RESULT OF EXPERIMENTATION

While experimenting this several result were found which are so much excited. It's very useful for a user to remember gesture passwords and it provides enhanced security to sensitive application of Mbanking as gesture password with their unique sequence is a harder task to know any third person. Also with the results it is found that as we had used encryption while storing password as well as gestures, it is impossible to know the password for anyone though he gets the access to database of the system. A central authority as administrator of system provide bank authorities have only access to manage users and to approve requests raised by users for gesture password and to add new users on the basis of forms getting submitted to bank. So this results that administrator can also not has vulnerable access to any users' account. An automatic mail generation facility is provided in the system so that user can be notify that his request is approved by bank for gesture password and use of Mbanking app. Also it may be useful for user to review his password if he forgets as it is stored in his mailbox. A vulnerability may occur as you can say if anyone accesses the mail account of user and knows the password but as we record IMEI number of user's device it is impossible to access the same account form another device. Also password in the mail is stated on the basis of number sequence of gestures so an anonymous user can not know the gestures and the sequence until he knows the exact gesture numbering.

VIII. CONCLUSION AND FUTURE WORK

As a conclusion through this paper it can be said that this system provides a better solution for securing the sensitive data of user. Banking account information is most sensitive for any user now a days and it must be secured well from any unauthorized access which is restricted by our system.

For future work we have decided to generalize this security model using gesture passwords for any kind of android app. Also we would like to try and integrate this with biometric security using six sensor glove for using it with future of technology which is sixth sense technology in which user don't need a specific device to use any kind of computing system

REFERENCES

1. Multitouch Gesture Based Authentication", Napa Sea-Bea, Nasir Menon, Katheriene Isbister & Kowsar Ahmed, IEEE April 2014.
2. "User-Generated Free-Form Gesture For Authentication", Rutgers University, University of Helsinki, Jan 2014.
3. "On The Security Of Picture Gesture Authentication", USENIX Association, August 2013.
4. "Continuous Mobile Authentication Using Touchscreen Gesture ",Tao Feng, Ziyi Liu,Kyeong-An Know, Weidong Shi , IEEE 2012.
5. "Design and Evaluation of Finger –Count Interaction: Combinig Multitouch Gesture and Menus", Gilles Bailly1,Jorg Muller1, Eric Lecolinet, Telecom ParisTech, CNRS LTCI UMR 5141,France 2013.
6. "Who You Are Way Of What You Are: Behavioral Biometric Approaches to Authentication ",Michael Karlesky, Napa Sea-Bea, Katheriene Isbister, Nasir Menon, Five MetroTech Center Brooklyn, New York, USA, 2014.

7. "User-Generated Free-Form Gesture For Athentication Security and Memorability ", Michael Shermany, Gradeigh Clarky, Yulong Yangy, Shridatt Sugrimy Arttu Modig, Janne Lindqvisty, Antti Oulasvirtaz, Teemu Roos, Rutgers University, Max-Plank Institute For Informatics, University of Helsinki, Jan 2014.
8. "Defence Against Large Scale Oonline Password Guessing Attacks By Using Persuasive Click Points", Chipp.T, R. Nagendran, International Journal Of Communication And Engineering, March 2013

