ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

Vol. 3, Issue 11, November 2015

# Touchscreen Mobile Authentication Using Multi-Touch Sequential Gestures

Balaji Chaugule*, Prof. Asha Pawar

Dept. of Computer Engineering, ZES's Dnyanganga college of Engg. & Research, Pune, India

**ABSTRACT:** Recently all handheld devices are touch screen and the popularity of touchscreen devices increases more and more due to the easy fast Internet access and large storage capacity. People may store their all personal information such as banking detail, password, confidential documents, trade secrets etc. on the handheld devices. In any case such handheld device is lost or stolen then security of such handheld device are more important because it contains users personals, banking information, secrets of user and that can be misuse by unauthorized person in any terrorist activity or other purposes that harm to user financially and socially. Securing the personal data stored and accessed from android touchscreen mobile makes user authentication a problem of paramount importance. The rigidity between security and usability renders however the task of user authentication on mobile devices a challenging task. This paper introduces Multi-Touch Authentication and unauthorized user tracking technique to protect mobile banking data stored on touch screen mobile devices (Finger gestures with priority Authentication System using Touch screen Devices), a behavioural touch screen based authentication approach on mobile devices. Besides extracting touch data from touch screen equipped smart phones. This system complements and validates this data using a touch screen mobile device. A addressable feature in the system is its continuity, users transparent post login authentication and tracing of location of mobile devices.

**KEYWORDS**: Touchscreen Devices, Mobile Authentication, Gesture Authentication, Multi-Touch Gesture Authentication.

## I. Introduction

Technological advances in computing, I/O capabilities and also network connectivity are shifting the focus towards the mobile devices. Market study expects that in 2015 there will be 1.5 billion smart phones and 640 million tablets in use world-wide [1], [2]. Moreover, companies, colleges, and government organizations are increasingly handing out mobile computing systems and applications that permit their employees to work remotely while constantly staying connected to the groups or societies structure. The name of handheld devices makes them a frequent storage medium for sensitive and confidential information as well as trade secrets and credentials. As handheld mobile devices are easily lost or stolen, the security of these devices becomes an important issue. As a first defence step, user authentication is quite essential to protecting handheld devices. However; mobile devices make a trade-off between the security and usability of most existing authentication solutions: one-shot authentication solutions are not protective from theft and loss [3], while periodic authentication or automatic logouts following periods of inactivity are likely to be counterproductive. The strong authentication is required by the still clumsy input methodology of such devices and the different user expectations for interaction models, particularly when compared to the normal authentication solutions. As displayed 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 passwords) [4].

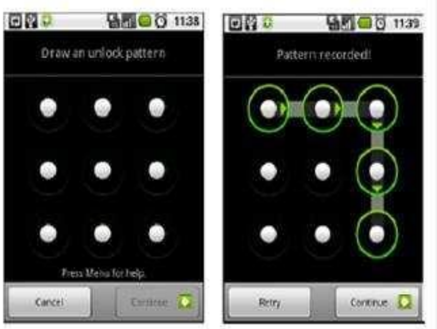
These devices often contain privacy sensitive Information such as personal photos, email, credit card numbers, passwords, corporate data, and even business secrets. Losing a smart phone with such private information could be a terrible for the user. In recent times touchscreen handheld devices contains number of sensors like touch, voice, image recognition. These sensors provide the use of biometric authentication technique. A current android device uses a single gesture recognition technique for the authentication but it has large probability to crack and also victim of shoulder surfing [5].It is also seen that performing a user-defined gesture over a customized background image and asking question after each gesture does result in higher authentication performance. In relations of usability, the reading shows that users did not have trouble in accomplishment multi-touch gestures as they all rated each gesture as easy to use [6].

DOI: 10.15680/IJIRCCE.2015. 0311175

The proposed system is post authentication service which is in three-shot authentication and one shot tracking solutions for protecting touch screen android handheld devices from theft and loss. Proposed system builds as the android application for touch screen android OS devices for stronger security to the banking data stored over the handheld devices from illegal users. This system will address the authoritative demand for a more secure and user friendly mobile authentication solution that supports both passive and continuous authentication for mobile users based on users touch gestures. This system will take advantage of the fact that during their interaction with mobile devices, users disclose their unique touch features, such as finger pressure and path, the speed and acceleration of movement. An essential advantage of our approach is its transparency to the user, the touch data is captured by mobile sensors without disturbing normal user-device interactions. During the post login stage, the traditional explicit authentication process is triggered only when system detects that the current user is likely different from the smart phone owner, that means it detects loss or theft of the device.

## II. MOTIVATION

Numbers of peoples are using a touchscreen android Smartphone because of having a large storage capacity and easy of Internet access from any location. Touchscreen android Smartphone are easy for access and available at cheapest rate in market, it provides same functionality (e.g.-pdf file reading, document file editor etc.) as compare to the computer so the popularity of the touchscreen mobile devices increases. Hence, peoples used touchscreen Smartphone devices to save some personal details as well as to access their bank accounts details from such devices, so providing security to such devices, the user used authentication Mechanisms applied on them still common text passwords or PIN. The recognized problems related to users selecting weak textual passwords [4]. In recent user uses a pattern authentication mechanism for security it provide security using a single gesture it check we use the password as a pattern. The Password pattern is like draw-secret shape on the screen. The form contains of an random number of strokes between dots shown in the finger.1 [7].It have large possibility to crack that single pattern by shoulder surfer or Intruders. Our system provides security against such attackers and keep our data secure from Intruders and shoulders suffers.


Draw an unlock pattern

Press Menu for help

Pattern recorded!

Fig. 1. Single Pattern Gesture.

In our proposed system we mainly focus on online Banking application security against unauthorized users. This system ensures and provides users safe and private banking.

This system uses sequential multiple gesture recognition and Tracking unauthorized user scheme for the authentication. It gives the stronger authentication for the touchscreen handheld devices also if our touchscreen handheld device may be lost or stolen and unauthorized user try to access our banking account for financial damage then our system will be activated and it send the message and mail of device location and image of that unauthorized user captured by front camera of that device to the registered user. This system provides security from the intruders or attackers. So to provide a strong security against such intruders or hacker our system protect our Banking data like username and password, multiple gestures patterns with a particular sequence and fingerprint recognition to overcome the drawbacks of password authentication. It introduces a new authentication technology to unlock devices which are very difficult to crack by unauthorized person

## III. PROPOSED MODEL

Here the input is provided to the mobile device through the touch screen which is gesture patterns. Basically the system is divided in the four parts our project mainly consists of 4 parts:

1. User Registration and Gesture selection

a User has to choose minimum two gestures from given list for authentication.

b User has to choose the gestures and order of the gesture needs to be defined.

2. User Authentication
In this stage user have to login with registered Gestures.

3. Gesture authentication module

a Collecting Gesture Data from user

b Examine gestures data to detect the correct shape.

c Shape can be flick, pinch, spread, drag and rotate.

4. Unauthorised user detection Module
This phase helps the registered user when his or her mobile is lost or stolen. When android Mobile is lost or stolen and unauthorized user going to access the banking application installed

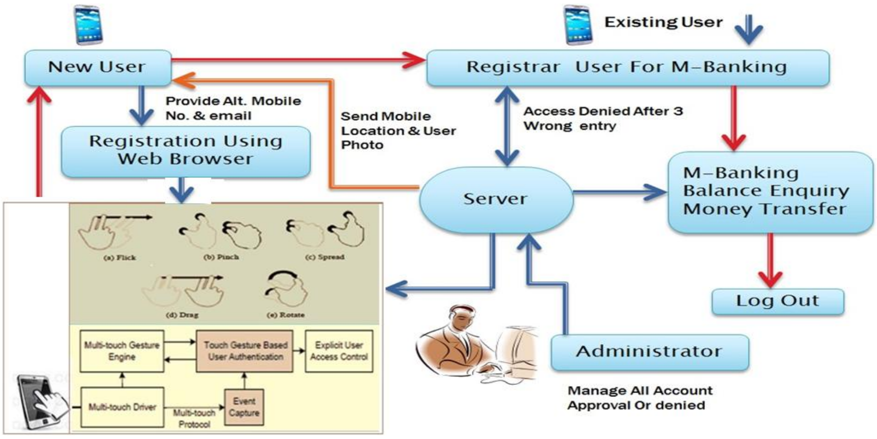

Existing User
New User
Registrar User For M–Banking
Provide Alt. Mobile No. & email
Send Mobile Location & User Photo
Access Denied After 3 Wrong entry
Registration Using Web Browser
Server
M–Banking Balance Enquiry Money Transfer
(a) Flick
(b) Pinch
(c) Spread
(d) Drag
(e) Rotate
Multi-touch Gesture Engine
Touch Gesture Based User Authentication
Explicit User Access Control
Multi-touch Driver
Multi-touch Protocol
Event Capture
Log Out
Administrator
Manage All Account Approval Or denied

Fig. 2. Touchscreen Mobile Authentication System.

Over on this mobile phone then he or she asks the draw the gestures with in sequence which is registered by the authorized user. If he or she fails to draw same gestures in registered order the mobile front camera automatically capture his or her image using front camera and current location of mobile phone. This information sends to the registered email address and alternative contact number of users.

d User has to draw same number of gestures and in the same order that are selected during registration process.
The three stages in detail are shown in figure above.

### A. Stage-I: Enrolment Phase

This Phase Used to register the user by taking different user details and Mobile International Mobile Equipment Identity (IMEI) number. Initially user has to register with some personal details like User Name, Finger Print, E-mail

Id, and alternate mobile number. The user should also select number of different gestures (i.e. 2 to 5 gestures) with the priority sequence.

### B. Stage-II: Training Phase

In the training phase registrations data from the users are collected, extracted, pre-process and normalized for the future verification process. The selected gestures are classified by using Classification algorithm with the consideration of features timestamp, finger pressure, X-Y co-ordinates and finger size. These features are normalized or pre-processed for better result. The registered gestures are classified by Using classification methods. The length of the gestures is calculated by considering the X-Y co-ordinates of the starting and ending point of the gestures. In this system there is more than one gesture are used for the authentication so there is time limit is consider between the two gestures that also calculated Finger size and pressure is also considered as features in the gestures recognition. These normalized features are stored in the database for verification.

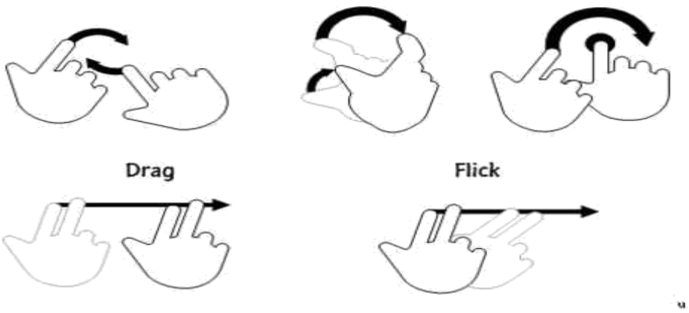


Fig. 3. Multitouch gestures.

### C. Stage-III: Verification Phase

In verification Phase user entered gestures, priority of the gestures and fingerprint matches with the registered gestures, priority order and fingerprints. If the match is found then user will authenticate for the access of that mobile device otherwise

he or she will be denied from the access of device. In case of unauthorized users if he or she will denied more than five times then current location of the device send to the resisted alternative number and e-mail address .

### D. Stage-IV: Unauthorized user Tracking Phase

This phase helps the registered user when his or her mobile is lost or stolen.
When android Mobile is lost or stolen and unauthorized user going to access the banking application installed over on this mobile phone then he or she ask the draw the gestures with in sequence which are registered by the authorized user. If he or she fails to draw same gestures in registered order the mobile front camera automatically capture his or her image using front camera and current location of mobile phone. This information send to the registered email address and alternative contact number of users.

## IV. RESULT AND DISCUSSION

In proposed system we are providing stronger security and tracking mechanism using multiple gestures with priority. This system traces touchscreen mobile devices, if unauthorized user tries to use the system. This system provides better security against unauthorized user also find our devices if lost.

**The Comparative discussion of our system is shown in the following table.**

We are circulating our system in five users for collection the result of our system to comparative system. Our system results collected from different five users which are using our system and giving the feedback of system depending upon the parameters, this result is calculated over the considering the parameter time of accessing system, accuracy rate of system, security compared to other system, space required to install this system over the local system.

User Provide marks of parameters out of 10.

Table1.-Result Over the consider parameter

| Parameters | User 1 | User 2 | User 3 | User 4 | User 5 | Avg |
|---|---|---|---|---|---|---|
| Time | 7 | 8 | 8 | 7 | 8 | 75% |
| Space | 10 | 10 | 9 | 10 | 9 | 96% |
| Security | 9 | 9 | 8 | 9 | 9 | 88% |
| Accuracy Rate | 10 | 10 | 10 | 9 | 10 | 98% |

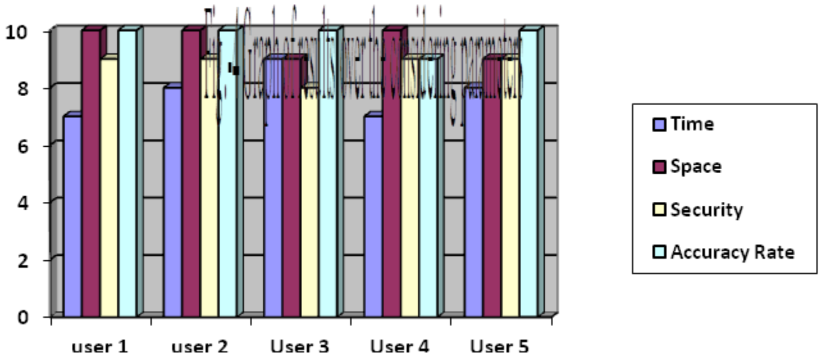
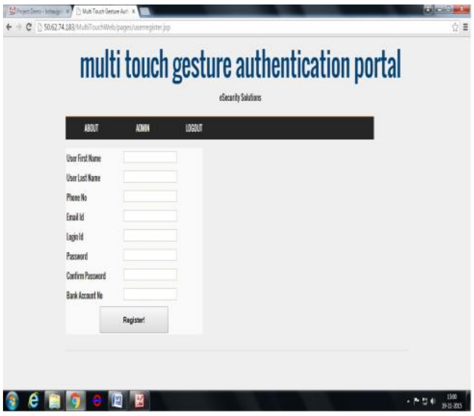


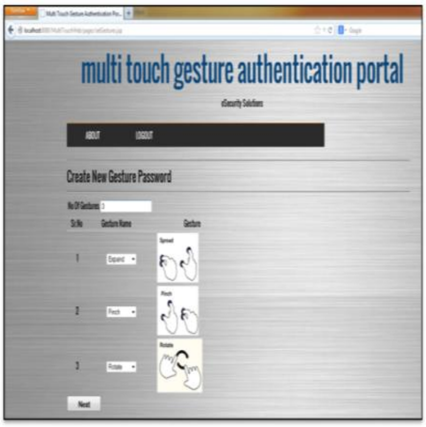
Fig.-4 Graph of results over the considering parameters

**1. User Registration Window:**


Multi Touch Gesture Auth
50.62.74.183/MultiTouchWeb/pages/userregister.jsp
multi touch gesture authentication portal
eSecurity Solutions
ABOUT
ADMIN
LOGOUT
Register!

User First Name
User Last Name
Phone No
Email Id
Login Id
Password
Confirm Password
Bank Account No

**2. Gesture and Order Selection Window :**

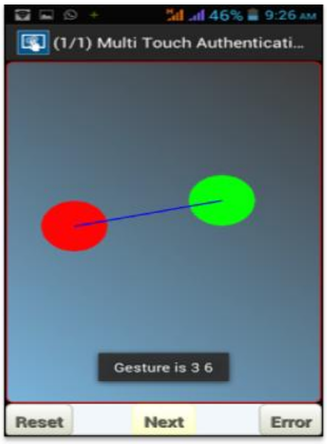

Multi Touch Gesture Authentication Po...
multi touch gesture authentication portal
eSecurity Solutions
ABOUT
LOGOUT
Spread
Pinch
Rotate
Next

Create New Gesture Password

No Of Gestures 3

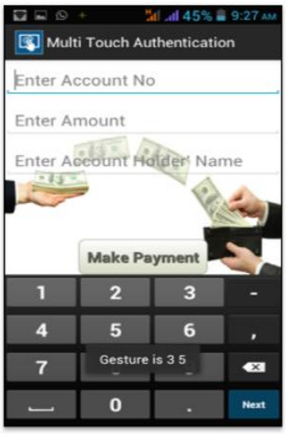
| Sr.No | Gesture Name | Gesture |
|---|---|---|
| 1 | Expand | |
| 2 | Pinch | |
| 3 | Rotate | |

3. **Gesture Drawing Window:**



Gesture is 3 6

4. **Mbanking Menu:**



Gesture is 3 5

## V. Conclusion and Future Work

This paper proposes multi-touch gestures for secure user Mobile banking authentication and tracking unauthorized users if device is lost or stolen. The multi-touch gestures have the potential for evolving new user authentication techniques. This improves both the security and usability of such devices .Multi-Touch gesture has high Feasibility of the proposed approach in terms of performance and usability. This system will provide stronger security against the unauthorized user if the mobile lose or stolen this system will work as tracker of the unauthorized user.

In Future this system may be used in ATM machines or touchscreen laptops for more and better security of data and financial transaction.

## References

1. Worldwide smartphone markets: 2011 to 2015 analysis, data, insight and forecasts http://www.researchandmarkets.com/ 7a1189/worldwide smart-phone.
2. Dennis Guse and Master Thesis, “Gesture based User Authentication on Mobile Devices using Accelerometer and Gyroscope”,2011.
3. Xi Zhao,Tao Feng and Weidong Shi,”*Continuous Mobile Authentication Using A Novel Graphic Touch Gesture Feature*”,BATS IEEE Sixth Conference Publications 2013
4. T.Feng,Z.Liu,K.A.Kwon,W.Shi,B.Carbunar,Y.Jiang and N.Nguyen, “*Continuous mobile authentication using touchscreen gestures*” ,In Homeland Security(HST),IEEE Conference on Technologies for,2012.
5. Muhammad Shahzad,Alex X. Liu and Arjmand Samuel, “*Secure Unlocking of Mobile Touch Screen Devices by Simple Gestures”,* You can see it but you can not do it,MobiCom13 ACM,2013.
6. Napa Sae Bae,Nasir Memon,Fellow,Katherine Isbister and Kowsar Ahmed, “*Multi-touch Gesture Based Authentication*”, IEEE Transactions on Information Forensics and Security, 2014.
7. Arpit Agrawal and Ashish Patidar,”*Smart Authentication for Smart Phones*”, International Journal of Computer Science and Information Technologies, Vol.5(4),2014.
8. D.Maio, D.Maltoni,J.L.Wayman and A.K. Jain, “*Fingerprint Verification”* Competition,IEEE Transactions on Pattern Analysis and Machine Intel-ligence, March- 2012.
9. N.H.Zakaria, D.Griffiths, S.Brostoff and J.Yan , “Shoulder surfing defence for recall-based graphical passwords” ,in Proceedings of the Seventh Symposium on Usable Privacy and Security,NY,USA-ACM,2011.
10. T.Feng, 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,2012.
11. Napa Sae Bae,Nasir Memon, Fellow,Katherine Isbister and Kowsar Ahmed,“Multi-touch Gesture Based Authentication”, IEEE Transactions on Information Forensics and Security,2014
12. I.Jermyn, A.Mayer, F.Monrose,M.Reiter and A. Rubin, “*The design and analysis of graphical passwords”,* in Proceedings of the 8th USENIX Security Symposium. Washington DC, 1999
13. ] .S.Chiasson,P. van Oorschot and R. Biddle, “*Graphical password authentication using cued click points*” ,Computer Security ESORICS 2007
14. ] N.Sae-Bae, K.Ahmed, K.Isbister and N.Memon, “*Biometric-rich gestures: a novel approach to authentication on multi-touch devices*”, in ACM annual conference on Human Factors in Computing Systems.ACM,2012.