Touchscreen Mobile Device Owner Identification Using Continuous Successive Gestures

[1]Balaji A. Chaugule,[2]Prakash D. Kshirsagar,[3]Shraddha P. Mankar,[4]Gopal R. Chandangole

[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor, [4]Assistant Professor
Department of Computer Engineering,
Zeal College of Engineering & Research, Pune, India

Abstract: Behavioral biometric on cell phones has turned out to be well known in previous some years and the capability of finger touch gestures as a new biometric style has been investigated of late. Securing the individual user information on touch screen smart mobile devices and makes the correct user validation is a critical issue. The unbending nature amongst security and ease of use renders, however the errand of client confirmation on cell phones a testing undertaking. This paper enlightens Multi-Touch Authentication method to ensuring information put away on touch screen cell phones (unique mark and Finger motions with need Authentication System utilizing Touchscreen Devices), a behavioral touch screen constructs validation approach in light of touchscreen cell phones. other than extricating touch information from touch screen prepared advanced mobile phones. This framework provides and approves this information utilization on touch screen smart mobile devices. A prominent motivation of this paper is to provide consistent, client straightforward post login authentication and verification Techniques.

IndexTerms - Hand-held touchscreen Mobile device, Mobile authentication, gesture recognition, Biometric.

I. INTRODUCTION

Technological proposals in computing world moving the attentiveness towards the touchscreen mobile phone devices by considering the I/O effectiveness and conjointly network property. According to Market study in 2015 there'll be 1.5 billion good phones and 640 million tablets in use worldwide [1],[2]. Moreover, companies, colleges, and government organizations square measure increasingly more handing out mobile computing systems and applications that authorize their staff to figure remotely whereas invariably staying connected to the group's or society's structure. The name of hand-held devices makes them the safe verification is required by the still massive information system of such gadgets and the diverse client suppositions for connection models, outstandingly when related to the ordinary validation arrangements. As showed in an investigation of more than 6,000,000 passwords, 91% of all client passwords have a place with a rundown of only 1,000 normal passwords [4] (e.g., Number of clients utilize either "secret key" or "123456" as passwords). These contraptions consistently contain private tricky Information, for instance, singular photos, email, bank card numbers, passwords, corporate data, and even business special bits of knowledge. Losing a PDA with such private information could be a shocking for the customer.

The proposed framework is three-shot confirmation answers for shielding touch screen handheld gadgets from robbery and misuse. We are implementing a Touchscreen Mobile Authentication System (TMAS) for better secure authentication. This framework works as the android application for touch screen android OS gadgets for more grounded security to the information put away finished the handheld gadgets from unlawful clients. This framework will address the definitive interest for a more secure and easy to use versatile verification arrangement that backings both aloof and ceaseless confirmation for portable clients in view of client's touch motions and unique finger impression acknowledgment. This framework will exploit the way that amid their connection with cell phones, clients reveal their one of a kind touch highlights, for example, finger weight and way, the speed and quickening of development. A basic favorable position of our approach is its straightforwardness to the client: the touch information is caught by versatile sensors without irritating typical client gadget collaborations. Amid the post login organize, the customary unequivocal confirmation process is activated just when framework recognizes that the present client is likely not quite the same as the advanced cell proprietor, that implies it identifies misfortune or burglary of the gadget.

II. MOTIVATION

Quantities of people groups are utilizing a touchscreen cell phone as a result of it have an extensive stockpiling limit and simplicity of Internet access from remote area. Touchscreen cell phone cell phones are simple for get to and accessible at least expensive rate in showcase, it gives almost same usefulness (e.g.- pdf record perusing, archive document proofreader and so forth.) as contrast with the PC, thus the ubiquity of the touchscreen cell phones increments. People groups utilize touchscreen cell phone gadgets to store individual points of interest like photo, contact subtle elements, monetary points of interest and so on and to get to their financial balances points of interest from such cell phones so giving security to such gadgets is the most critical thing The client utilized confirmation components connected on them still normal content passwords. The perceived issues identified with clients choosing feeble literary passwords [7]. In latest, user uses gesture pattern for authentication as a mechanism for security. They use gesture to provide security, Smart devices using a single gesture for authentication and it allows to authentic user to use the password as a pattern. The Password pattern is like draw-secret gesture (shape) on the screen. The form contains a random number of strokes between 9 dots shown in the finger.1 [8].It have large possibility to break single pattern by shoulder surfing attacks.

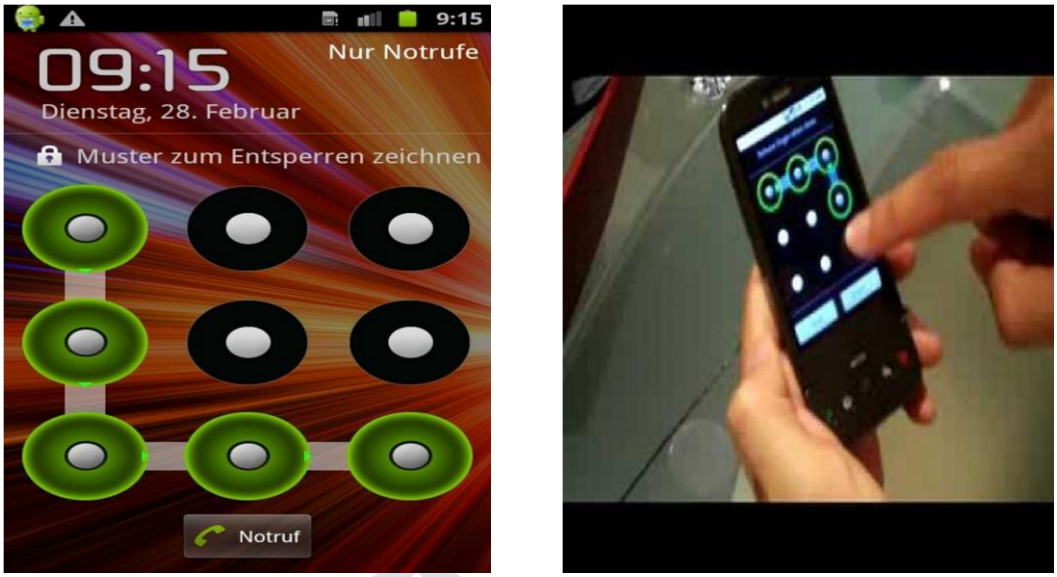

Fig.1. Single Pattern Gesture.

In this paper we will utilize blend of two biometric security component i.e. physiological biometrics typically utilizes estimations from the human body, for example, fingerprints and successive numerous gestures acknowledgment plot for the confirmation. It gives the more grounded validation to the touchscreen handheld gadgets from the interlopers or assailants. So to give a solid security against such interlopers or programmer to ensure our own information, different motions designs with a specific succession and unique finger impression acknowledgment to beat the downsides of secret key validation, acquainted with open a gadget which are exceptionally hard to split by unapproved individual. If unauthorized user attempt with wrong gestures it photograph will be captured by mobile device front camera and sent it to registered email address.

III. ARCHITECTURE OF TMAS:

Here the information is given to the cell phone through the touch screen which is signal examples. Essentially the framework is separated in the three sections Our project mainly consists of 3 parts:

1. User Registration and Gesture determination

a. Owner has to select gestures to be used for authentication on Touchscreen Smartphone.

b. Owner has to select the gestures and order of each the gesture needs to be defined.

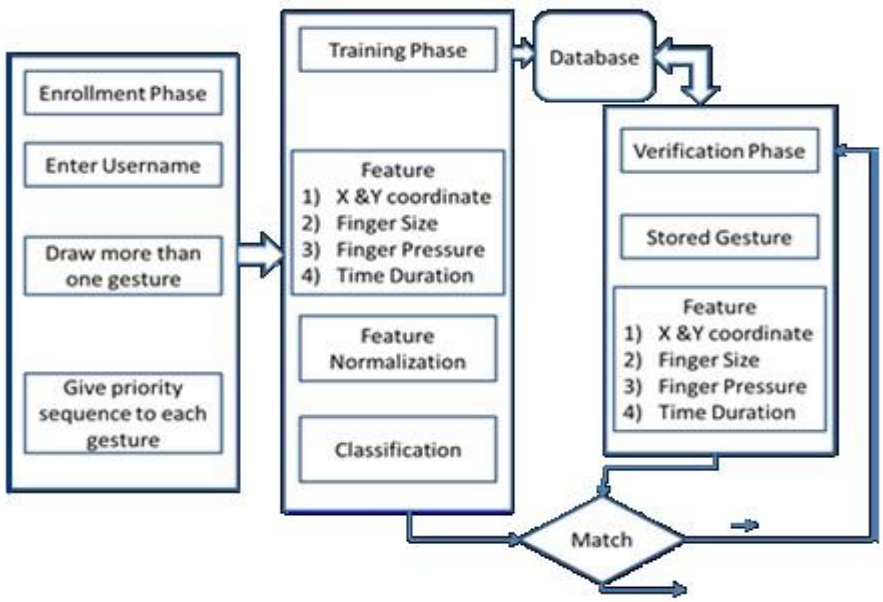

Fig.2 Touchscreen Mobile Successive Gestures Authentication System (TMAS).

2. User Authentication

3. Gesture authentication module

a. Selecting Gesture information from Owner

b. Analyzing gesture data selected from user to identify the shape

c. Gestures can be flick, pinch, spread, drag and rotate [4].

d. For authentication user need to enter equal number of gesture in matching order which are elected at the time of registration.

There are three phases of TMAS s Explanations regarding phases are displayed in above diagram.

3.1 Phase-I User Gesture Registration or Enrollment Phase

This Phase Used to enroll the client by taking distinctive client subtle elements and International Mobile Equipment Identity (IMEI) number. At first client needs to enlist with some individual points of interest like User Name, Finger Print, E-mail Id, and interchange versatile number. The client should likewise choose number of various signals (i.e. 2 to 5 signals) with the changeless need grouping.

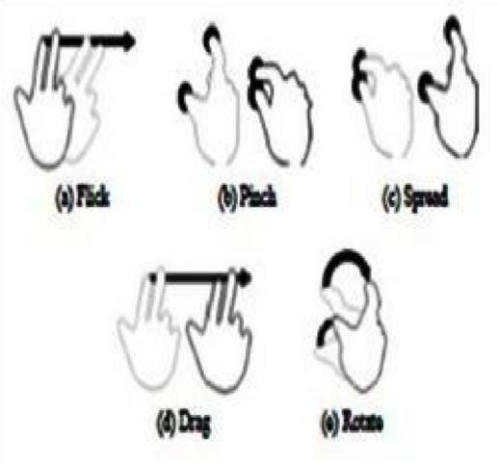

Fig.3. Multi-Touch Gestures.

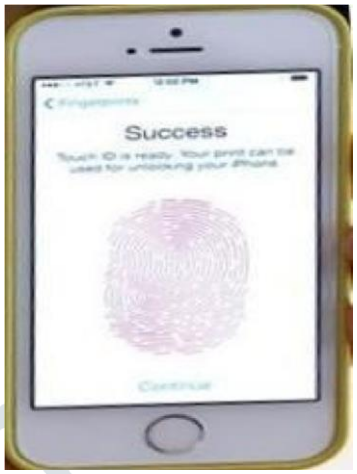

Fig.4. Fingerprint Scanning over Mobile Device

3.2 Phase-II Training Phase (Information Training Phase)

In the preparation stage enrollments information from the clients are gathered, separated, preprocess and standardized for the future confirmation process. The chosen signals are characterized by utilizing categorization calculation with the thought of highlights time limit, finger load, X-Y co-ordinates and finger estimate. These highlights are standardized or pre-prepared for a better outcome. The enrolled gestures are grouped by utilizing order strategies. The length of the gestures is curtained by considering the X-Y co-ordinates of the beginning and completion purpose of the motions. In this framework, there is more than one motion are utilized for the validation so there is time constrain is consider between the two motions that likewise figured Finger size and weight is additionally considered as highlights in the motions acknowledgment. These standardized highlights are put away in the stored location for check.

3.3 Phase-III User Confirmation Phase (Confirmation and Verification of Information Phase)

In confirmatory phase client input the gestures, need of the motions and unique mark matches with the enlisted motions fingerprints. On the off chance that the match is discovered then user will validate for the entrance of that handheld equipments else he or she will be prevented from the entrance from claiming gadget.

In unapproved clients situation on the off chance that if user will deny further than three times next current locality parameters of the gadget sent to another registered number and email address with front end camera capture image.

IV. RESULT & DISCUSSION

Existing framework comprise the more than one gestures with client characterized foundation and Questions about usability, joy, and energy level are asked subsequent to playing out each signal and at the beginning of each session aside from convenience [6].This gives a review of more than one gesture simple .

TABLE 1. MEAN SCORES OF EASE OF USE FOR EACH GESTURE IN THREE SESSIONS

Gesture	Session 1	Session 2	Session 3
Drag	4:71 (0:84)	4:73 (0:50)	4:73 (0:50)
Pinch	4:40 (0:83)	4:49 (0:84)	4:56 (0:78)
CCW	3:98 (1:01)	4:02 (0:82)	4:15 (0:82)
Swipe	4:63 (0:62)	4:61 (0:70)	4:71 (0:51)
User-defined	4:27 (0:95)	4:30 (1:03)	4:37 (0:89)

In proposed framework we are giving more grounded security by mix of different gestures with sequence of each gesture. This framework follows touchscreen handheld Smartphone's, if unapproved client tries to get to the framework. The handheld device IMEI number and image captured by front end camera of gadget and send to registered email address and alternate mobile number. This framework gives better security against unapproved client likewise discover our gadgets if lost.

V. CONCLUSION

This paper proposes blend multi-touch motions and unique finger impression acknowledgment for secure user verification and tracking of unauthorized user on touchscreen gadgets. The multi-touch gestures with unique finger impression and sequence acknowledgment have the potential for developing new user validation strategies.
This enhances both the security and ease of use of such gadgets. Multi-Touch gestures validation utilizes arrangement calculation to recognize touch motions made by various clients. Possibility of the proposed approach as far as execution and ease of use. This framework will give more grounded security against the unapproved client also helps to identify unapproved user also. In portable touchscreen device loses condition this framework will function as tracker of the unapproved client

REFERENCES

1. 2011 to 2015 Worldwide smartphone markets analysis, data, insight & forecasts. http: //www.researchandmarkets.com /research /7a1189/ worldwide smartphone
2. D Guse , Master Thesis "Gesture-based User Authentication on Mobile Devices using Accelerometer and Gyroscope," 2011.
3. X. Zhao, T. Feng and W. Shi "Continuous Mobile Authentication Using A Novel Graphic Touch Gesture Feature," BATS IEEE 6TH 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), 2012 IEEE Conference on Technologies for, 2012, pp 451–456.
5. M. Shahzad, A. X. Liu, A. Samuel." Secure Unlocking of Mobile Touch Screen Devices by Simple Gestures – You can see it but you can not do it," MobiCom'13 ACM 2013.
6. N. Sae-Bae, Memon Nasir, Fellow, IEEE, Isbister Katherine, and K. Ahmed "Multi-touch Gesture Based Authentication," IEEE Transactions on Information Forensics and Security, 2014.
7. Agrawal, A. Patidar" Smart Authentication for Smart Phones" International Journal of Computer Science and Information Technologies, Vol. 5 (4), 2014, pp 4839-4843.
8. K. Huberty , M. Lipacis, A. Holt , E. GELBLUM, S. Devitt, Swinburne B., Meunier F. , HAN K. , F.
9. A.WANG, J.Chen, ONO, M., Nagasaka, M.,Yoshikawa, K., and Schneider, M. "Tablet demand and disruption:
10. Mobile users come of age,"
11. Maio, D., Maltoni, D.,Wayman, J.L., Jain, A.K." Fingerprint Verification Competition," IEEE Transactions on Pattern Analysis and Machine Intelligence, March, 2012, pp 402-412.
12. 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, ser. SOUPS '11 New York, NY, USA: ACM, 2011, pp. 6:1–6:12.
13. I. Jermyn, A. Mayer, F. Monrose, M. Reiter, A. Rubin et al., "The design and analysis of graphical passwords," in Proceedings of the 8th USENIX Security Symposium. Washington, DC, 1999, pp. 1–14. **[12]** S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," Computer Security–ESORICS 2007, pp. 359–374.
14. Sae-Bae N., Ahmed K. , Isbister K., & Memon, N., "Biometric-rich gestures: a novel approach to authentication on multi-touch devices," in Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems. ACM,2012, pp. 977–986.
15. E. Maiorana, P. Campisi," Cancelable Templates for Sequence-Based Biometrics with Application to On-line
16. Signature Recognition" IEEE Transactions On Systems, Man, And Cybernetics—Part A: Systems And Humans, Vol. 40, NO. 3,MAY 2010, pp. 525-538.