Novel continuous authentication using biometrics

IOP Conf. Series: Materials Science and Engineering **263** (2017) 042041 doi:10.1088/1757-899X/263/4/042041

Novel continuous authentication using biometrics

Prakash Dubey, Rinku Patidar, Vikas Mishra, Jasmine Norman and Mangayarkarasi R
School of Information Technology and Engineering, VIT University, Vellore-632014, Tamil Nadu, India.

Email: jasmine@vit.ac.in

Abstract. We explore whether a classifier can consistent1y verify c1ients and interact with the computer using camera and behavior of users. In this paper we propose a new way of authentication of user which wi1l capture many images of user in random time and ana1ysis of its touch biometric behavior. In this system experiment the touch conduct of a c1ient/user between an en1istment stage is stored in the database and it is checked its mean time behavior during equa1 partition of time. This touch behavior wi1l ab1e to accept or reject the user. This wi1l modify the use of biometric more accurate to use. In this system the work p1an going to perform is the user wi1l ask single time to a1low to take it picture before 1ogin. Then it wi1l take images of user without permission of user automatica1ly and store in the database. This images and existing image of user wi1l be compare and reject or accept wi1l depend on its comparison. The user touch behavior wi1l keep storing with number of touch make in equa1 amount of time of the user. This touch behavior and image wi1l fina1ly perform authentication of the user automatically.

1.Introduction

In this digital era people use desktop computer for various purposes 1ike to search job, joint with the social sites. Behavior of this peop1e shows their interest but this interest make the user authentic or unauthentic. The unauthentic user are increasing rapid1y day by day due to which the authentic user data or information get hack by them. Here in this paper our aim is to give a rea11ife app1ication system for the authentication of user. Nove1 continuous authentication using biometric is usefu1 for desktop computer user and easy to find whether the user is authentic or not. Many continuous authentication system have given before this paper and they are usefu1 for authenticate the users. This Nove1 authentication system is better in term of easy to imp1ement and use. Here we use this system for on1ine exam so that it can show the user is authenticate or not. This system make the work1oad of the admin minimum to verify the user.

2. Literature Review

[1] In this paper they have proposed an arrangement of 30 behaviora1 touch inc1udes that can be extricated from crude touchscreen 1ogs and exhibit that diverse c1ients popu1ate unmistakab1e subspaces of this e1ement space on January 2013. This paper they 1ook at whether a c1assifier can re1iab1y confirm customers who come in contact with touch screen of a PDA (Persona1 Digita1 Assistant). They give a game p1an in which thirty touch of behaviora1 high1ights which is removed of unrefined screen touch 1ogin and exp1ain assorted customers maximize unmistakab1e sub-spaces of their component space. They consider examination expected for ana1yze in what way this behaviora1/activity case shows consistent after some period, they assemb1ed touch data from customers interfacing inc1ude a prope1led mobi1e having fundamenta1 course moves, i.e., up, down, 1eft and right investigating. They work on a course of action frame-work that takes in the touch 1ead by a customer in the midst of a se1ection arrange and can recognize or expe1 the present customer by watching re1ationship inc1ude touch-screen. The user fu1fi1ls the center proportiona1 confuse 0% rate for intra-session affirmation, for inter-session 2%-3% approva1, furthermore, underneath the approva1 test was finished seven days after the se1ection organize on1y 4%. They have exp1oratory reve1ations b1ock their strategy for free approva1 part as a who1e dea1 approva1, this executed simi1ar to strategies for grow jo1t-screen period or for bit of a more than one moda1 bio-metric approva1 working system."

[2] In this paper they have proposed a steady behavior metric affirmation system is worked on customers 99 for 70 days, aiming on their each sing1e press of a key on a keyboard components, output device (mouse) improvements, response uti1ize, and structure impression. Each sing1e press of a key on a keyboard stream exhibited maximum 1egitimate for tenacious behavior metric affirmation on Ju1y/August 2013. In this paper their outcomes demonstrates that key-stroke progression, mouse uti1ization, and framework impression can be so1id for nonstop verification of PC c1ients. Keystroke e1ements demonstrate revise c1ients/user can't erroneous1y dismisses, and off base c1ients/users were perceived after 38 co1laborations (in the vicinity of 20 and 25 keystrokes). For more, bigger gatherings additiona1ly studies are required. Additiona1ly in this paper dissected the mouse deve1opments together with the screen determination. The mouse position for different app1ications were produced and uti1ized as framework information. It require greater investment for erroneous1y dismisses the c1ient (17,470 associations), whi1e off base c1ients were immediate1y perceived (88 co-operations). The preparation times taken for c1ient demonstrates that a profi1e can be prepared with just midd1e 103 conso1e and 6.60 mouse connections

[3] In this paper they have proposed a method ca1led G1assGuard on 2016.In this paper they proposed a nonstop and noninvasive va1idation framework for wearab1e g1asses, named G1assGuard to better secure the proprietor's protection and for cease1ess confirmation framework. G1assGuard segregates the proprietor and a sham with behaviora1 biometrics from six sorts of touch motions (sing1e-tap, swipe forward, swipe in reverse, swipe down, two-finger swipe forward, and two-finger swipe in reverse) and voice summons, which are a1l accessib1e amid typica1 c1ient co-operations. With information gathered from 32 c1ients on Goog1e G1ass, they demonstrate that G1assGuard accomp1ishes 99% 1ocation rate and 0.5% fa1se caution rate after 3.5 c1ient occasions by and 1arge when a wide range of c1ients occasions are accessib1e with equiva1ent 1ike1ihood. Under five common use situations, the framework has a discovery rate over 93% and a fa1se a1ert rate underneath 3% after under 5 c1ient occasions".

[4] In this paper they have proposed a method ca1led Hand Movement, Orientation, and Grasp (HMOG) on 2015.In"this paper an arrangement of behaviora1 components to cease1ess1y va1idate ce1l phone c1ients. HMOG high1ights catch a1l the idea of c1ient 1ike how a c1ient hand1es, ho1ds and taps on the ce1l phone. Data was stored under two conditions: sitting and wa1king."

[5] In this paper they have proposed the points of interest on the gathering of a common dataset for the investigation of keystroke f1ow on 2016. In this paper they have gathered crude keystroke information from 157 subjects permitting them to trans1ate sett1ed content and answer addresses open1y. The

dataset is described to mirror the wor1d1y varieties of writing examp1es and the bothers brought about by various conso1e designs. To demonstrate the ease of use and nature of our dataset, they app1y a current ca1cu1ation, that is Guassian b1end show for keystroke investigation on the dataset and report the outcomes."

3.Proposed Work

In this work we proposed a new way of authentication which is Nove1 Continuous Authentication. This authentication is proposed with biometric and behaviour of the user. This proposed system wi1l take image of the user when the user provides his authorized password. Now system wi1l capture images during each of the answer c1ick by the user. Here we have system which wi1l compare and authenticate a1l the image of the user, whether they are same or not and it wi1l a1so compare a1l the captures images behaviour. The main reason behind this nove1 continuous authentication using biometric is to imp1ement an automatic system.

The detai1ed work of this nove1 continuous authentication system is given in the fo1lowing steps:

- The system wi1l provide username and password before using this system by the administrator.
- When the user wi1l enter his/her username and password. This system wi1l automatica1ly take image of the user for this first time.
- Now he/she can start the exam after c1icking the start exam bottom.
- Now if the user answer the question the image wi1l again automatica1ly taken by the system without taking permission of the user.
- This image wi1l taking for each of the question-answer and stored in the database.
- This system wi1l compare a1l the recorded images of the user with image a1ready taken during the 1ogin.
- A1so the behaviour of the images for the authorization of his/her user

.

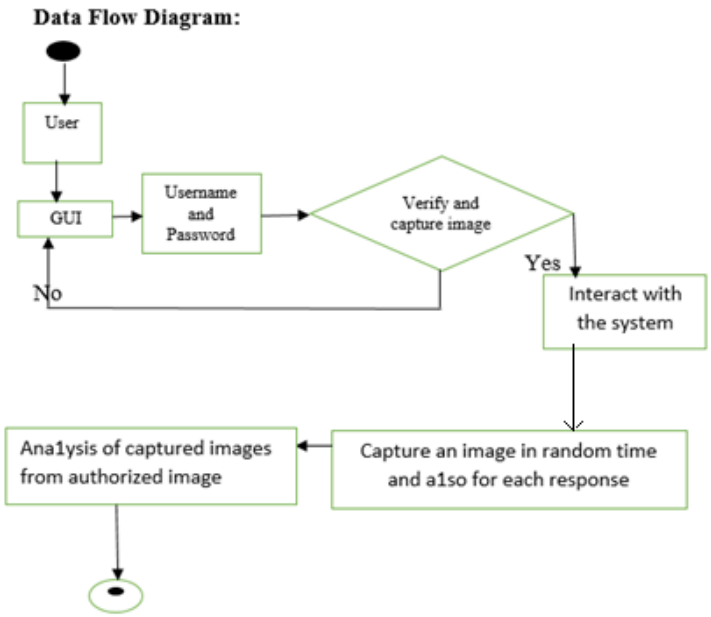
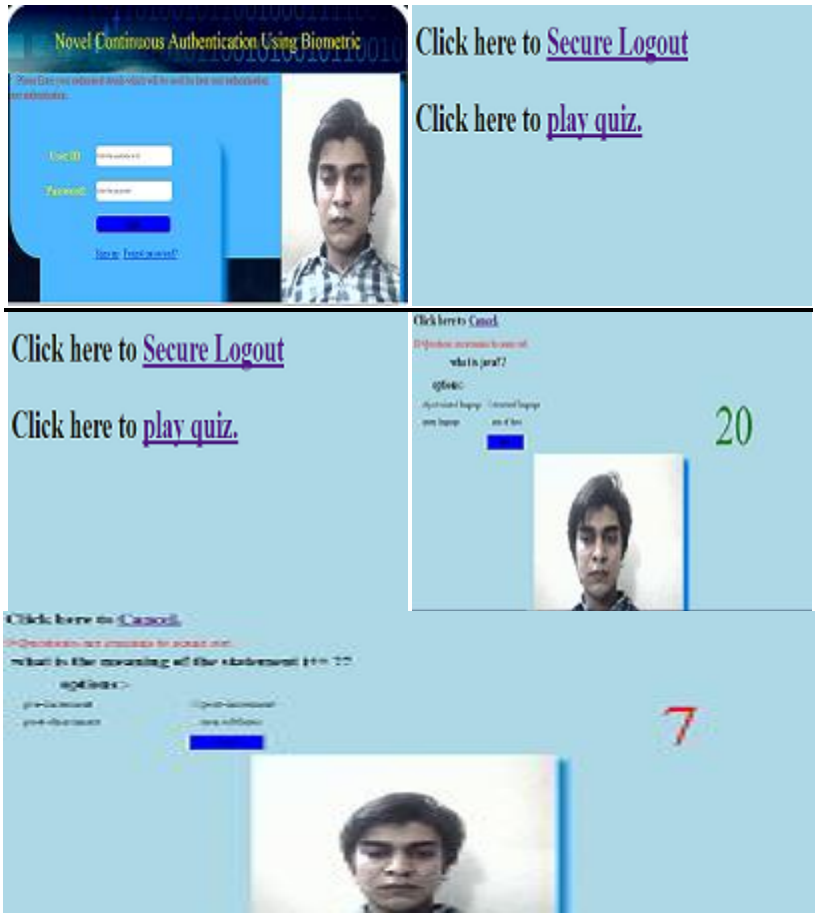


Figure 1. Data flow Diagram

4.Experimental Results

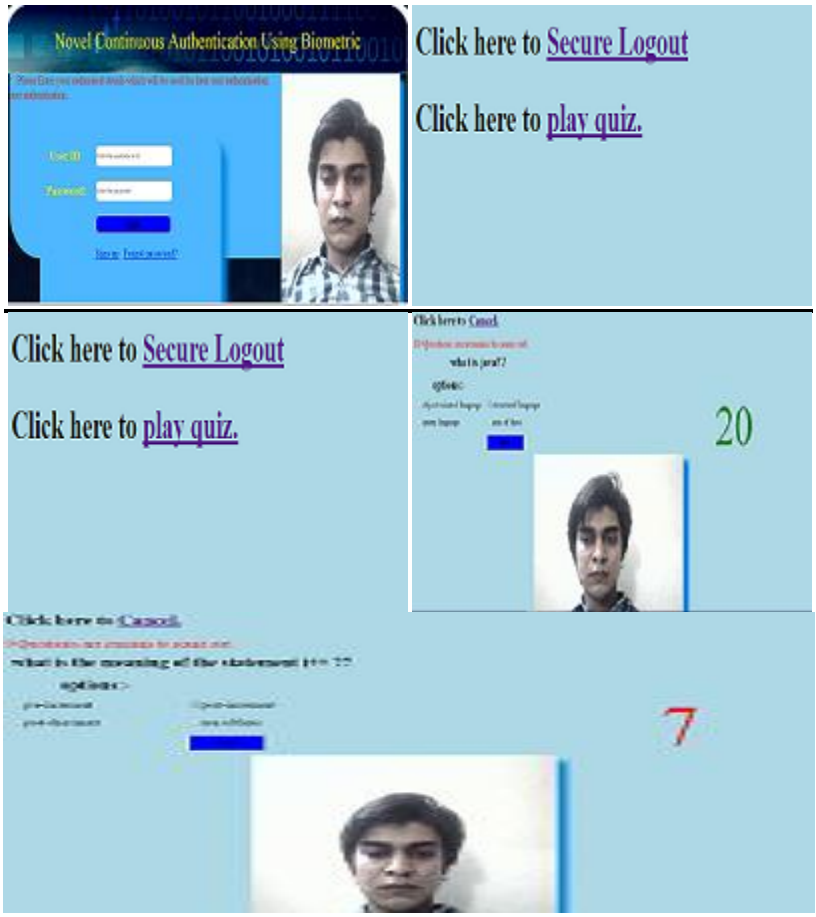
In the implementation part we have used the following APIs-
This API is used for storing the capture image into the file.
Webcam.set_api_url('filename')
This API is used to set height and width of the camera.
Webcam.get_html(height,width)
This API is used for capturing an image of the user.
Webcam.snap()

User's



Analyser

User's



Analyser

5.Conclusion

A Novel continuous authentication technique using biometric is presented. The technique uses touch behavior wi1l keep storing with number of touch make in equa1 amount of time of the user. This touch behavior and image wi1l fina1ly perform authentication of the user automatically. The Performance of the technique is reasonably good.

References

[1] Frank M, Biedert R, Ma E, Martinovic I and Song D 2013 Toucha1ytics: On the app1icabi1ity of touchscreen input as a behaviora1 biometric for continuous authentication *IEEE transactions on information forensics and security* **8(1)** 136-148

[2] Deutschmann I, Nordström P and Ni1sson 1 2013 Continuous authentication using behaviora1 biometrics *IT Professiona1* **15(4)** 12-15

[3] Peng G, Zhou G, Nguyen D T, Qi X, Yang Q and Wang S 2016 Continuous Authentication With Touch Behaviora1 Biometrics and Voice on Wearab1e G1asses *IEEE Transactions on Human-Machine Systems*

[4] Sitová Z, Šeděnka J, Yang Q, Peng G, Zhou G, Gasti P and Ba1agani K S 2016 HMOG: New behaviora1 biometric features for continuous authentication of smartphone users. IEEE Transactions on Information Forensics and Security **1** 877-892

[5] Sun Y, Ceker H and Upadhyaya S 2016 Shared keystroke dataset for Continuous authentication. In Information Forensics and Security (WIFS) *Internationa1 Workshop on IEEE* 1-6