JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Biometric Authentication in Web Application

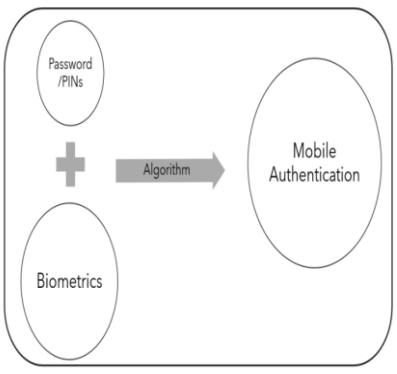
[1]Hyma J, [2]Devarakonda Sandeep
[1]Associate Professor, [2]M.Tech Scholar
[1]GITAM University, Visakhapatnam

Abstract : With the advanced of technology on mobile device, living the life through modern technology seems convenient and beneficial. Various of sensor and application installed on mobile device support and continuously change the way of people's life such as how to communicate with each other, to shop and to make transaction on financial and banking. One of the most things needed to be considered is how people protect on their own rights, data and private information among the insecure environment aside the mobile technology. Thus, security becomes seriously and complexity issues. Many techniques were developed and tested in order to ensure the reliability for user on using mobile device and its technology over decade. Biometrics which represents something existing in every human being is used to identify individual as it is unique. In this paper, the review of mobile user authentication and problems, the benefit of using physical biometric such as face, fingerprint, retina and iris also behavioral biometric for example voice, keystroke and touch dynamics are defined. The practical attacks on biometric recognition approaches available presently are stated along with the future work of biometric authentication. As a result, to improve accuracy and to enhance resistance against many types of attack on mobile device.

IndexTerms **- Biometrics,User Authentication,Fingerprint.**

I. INTRODUCTION:

Security on mobile phone is important as mobile device and its application change the way of human's life. With the supporting for life and activities anywhere anytime, authentication on mobile device should be concerned as it provides reliability and trust for each user on their private data and access rights into sensitive information such as password, financial transaction and banking accounts. User authentication is typical way to verify and validate the right of user on their mobile phone using Password and Personal Identification Number (PIN). Anyway, as many services available need the secured password to gain access rights, each user has more load to remember all of their own keys. Therefore, most of active users decide to apply the easy to remember password which leads them into an insecure situation and mobile phone crimes [3]. The use of authenticated tokens and biometrics become considerate as other alternatives way to protect their right. Authentication using token has many drawbacks as it can be easily to lose and stolen, moreover, inconvenient as it requires extra equipment.



Electronic passport is one of the hottest research fields nowadays due to reported different attacks against various countries. Several attacks such as brute force attack, guessing machine readable zone's information are performed on Basic Access Control Protocol (BAC) due to its low entropy[1]. Due to the size of smart devices, they can be easily lost and may expose details of users' private lives. In addition, this might enable pervasive observation or imitation of one's movements and activities, such as sending messages to contacts, accessing private

communication, shopping with a credit card, and relaying information about where one has been[4]. Biometric systems such as fingerprint, iris, DNA became popular methods in user authentication. Compared to these biometric systems, keystroke biometric authentication systems have not gained so much attention because of lower accuracy compared to other biometric systems. user verification technique using 1-substate Hidden Markov Model through keystroke dynamic. To verify the effectiveness of the proposed system, extensive experiments have been conducted and 80% accuracy was achieved by the proposed system [3].

II. RESEARCH METHODOLOGY

The methodology section outline the plan and method that how the study is conducted. This includes Universe of the study, sample of the study of using Biometric Authentication, study's variables and analytical framework. The details are as follows;

2.1 Methods

A. Iris recognition from distant images based on multiple feature descriptors and classifiers

K-Nearest Neighbor (KNN), Support Vector Machine (SVM) and Kernel based Extreme Learning Machine (KELM) algorithms are adopted for the recognition stage. Experiments are conducted on publicly available data set CASIA-v4 to evaluate the effects of the above features and classifiers. The experimental results suggest that, the contextual eye image features are better than the segmented iris features for human identification and also recommend that feature level fusion is better than the single feature descriptor. The recognition performance of KELM is 98.60% for fusion case of CNN iris and CNN contextual eye image features which is the maximum result in this distance images [2].

B. Authentication of Smartphone Users Using Behavioral Biometrics.

One of the greatest concerns is the possibility of breach in security and privacy if the device is seized by an outside party. It is possible that threats can come from friends as well as strangers. Due to the size of smart devices, they can be easily lost and may expose details of users' private lives. In addition, this might enable pervasive observation or imitation of one's movements and activities, such as sending messages to contacts, accessing private communication, shopping with a credit card, and relaying information about where one has been[4].

2.2 Algorithms used in Biometric Authentication

The method of authentication each's biometric can be divided into two categories consider the way to identify user.

1. Static authentication represents the process of identification and authentication user via the physical features which encounter security weaknesses. Whenever the data used to authentication user is hacked or created a copy, then the attacker can gain access rights over user (Vergara, 2019).

2. Dynamic authentication is the method of learn and analyze individual pattern of user behavior to authenticate user. It is normally applied to workwith behavior biometric as well. This type of authentication can provide continue monitoring and can be adjustable when user's behavior changed. For this reason, thedynamic biometric method is trustworthy way to the authentication user and providesgreater security than the static method (Smejkal & Kodl, 2018).

2.3 Methodology

The purpose of this project describing various authentication for mobile devices such as password based authentication, biometric authentication such as finger print and face recognition. Password based authentication is not secure as it can be hacked by anyone so most of the applications such as banking, healthcare and many more applications are using finger or face based authentication.

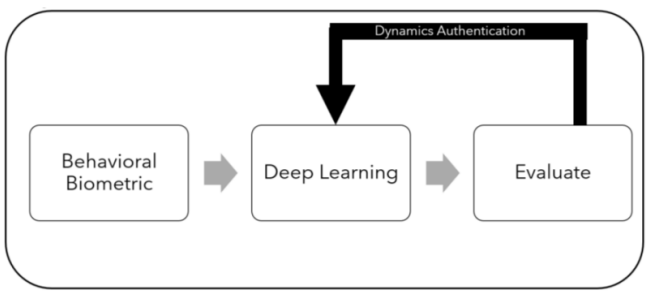


Figure 1

In propose requirement authentication if given for mobile device security such as Android but on student request we are adding this biometric authentication on python based web application. In propose project user can signup with the application by using finger print images and while login user has to upload similar images then application will authenticate fingerprint by using Harris Corner.

We are using following fingerprint image for signup and this images are available inside 'BiometricImages' folder

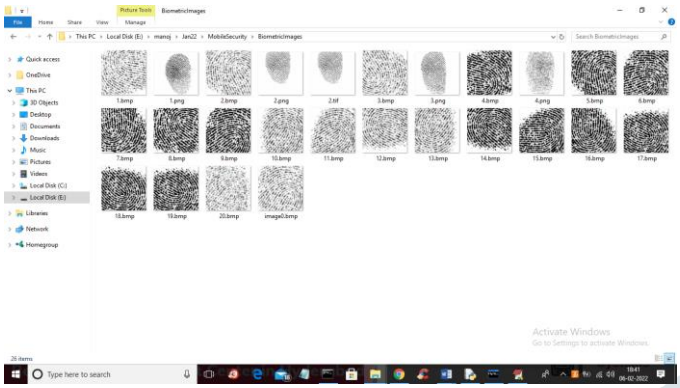


Figure 2: Sample Biometric fingerprints

Functional Requirements:

1.Data Collection

2.Data Preprocessing

3.Training And Testing

4.Modiling

5.Predicting

To run project install python 3.7 and MYSQL database and then open MYSQL console and then copy content from 'database.txt' file and then paste in MYSQL console to create database.

2.4 Steps for executing project

1. Register Here: using this module user can signup with the application by uploading finger print image and other details such as username, contact no, address etc.
2. User Login: using this module user has to enter username and then upload fingerprint image as password and then application will compare database image given at registration with the login image and if both images found then user will be authenticated successfully else authentication get failed
3. Authentication module: while authentication application will used following algorithms such as Keypoints measurements, GAR BFMatcher will find nearest similar matching between source and target fingerprint images, drawmatches which matches both fingerprint and returned matching score and if score less than 10 then authentication is successful.

III. RESULTS AND DISCUSSION

3.1 Test Cases

S.NO	INPUT	If available	If not available
1	User registration	Registered with valid details	There is no process

2	User Login	Login with username & password	There is no process
3	Finger password	Authentication of the result displayed	There is no process

3.2 Results

The main problem of users are facing problem on the biometric authentication. There are various methods have been used to implement biometric authentication in Web Application one the main option is to monitor the web application by using fingerprint images while signing into website that might help from authentication issue.

The implementation has shown how the biometric authentication can be worked in Web Application by using sample biometric images that are stored in folder with the help of different algorithms.

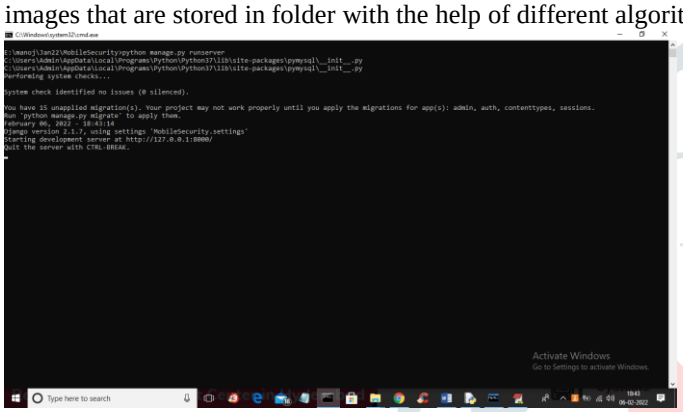


Fig 1 : 'runServer.bat' file to start DJANGO server .

Fig 2 : first register in the website.

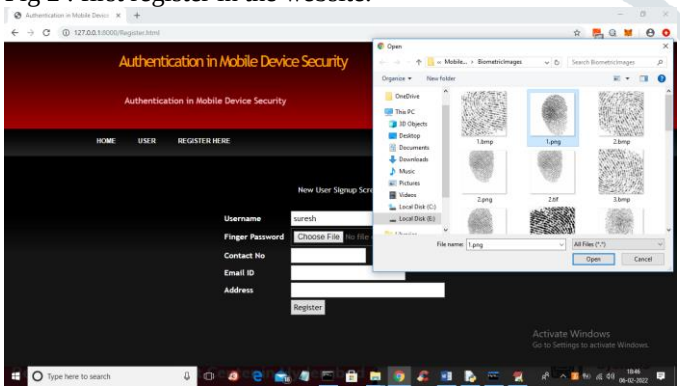


Fig 3: user will enter signup details and then upload fingerprint image as password and then click on "Register".

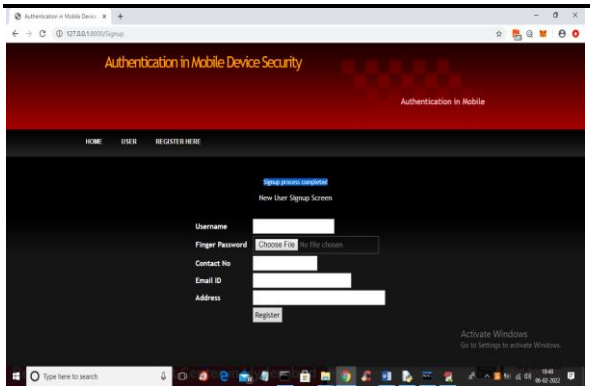


Fig 4: In above screen in blue colour text we can see signup process completed and now click on 'User' link to get authenticate.

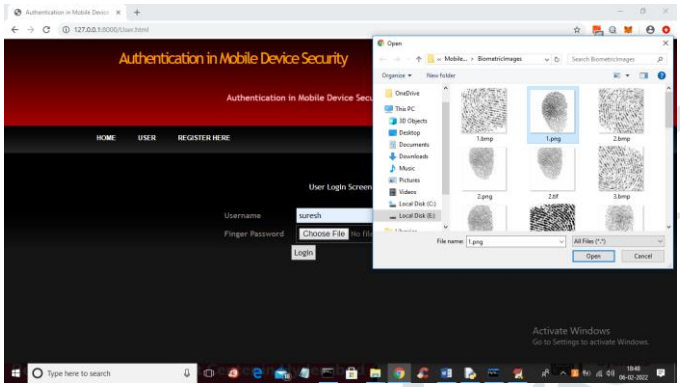


Fig 5 : In above screen for login I entered username as 'suresh' and then uploading correct image given at signup time and then click on "open' and 'Login' button.

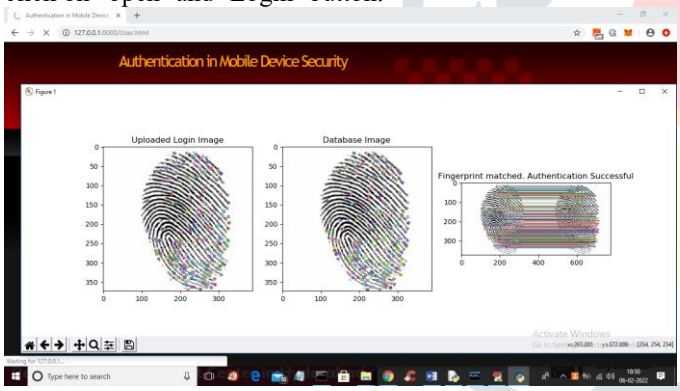


Fig 6: In above screen application displaying first image as the login uploaded image and second image is the database image and in first and second image we can see minute points in different colour indicating which points are matched and in 3rd image we are connecting both images points with lines which get matched and in 3rd image title we got result as "Fingerprint matched.

IV. CONCLUSION

In this paper, we presented the use of biometric authentication on mobile device based on existing research literature as it is generally used in people's everyday life. Mobile technology offers many convenient and benefit to life. However, with the change way of life, one of the most important things should be considered is the security. The problem of mobile user authentication has been concerned for over decade. Many researches applied methods to ensure the reliability and trust since password based and token based were found many points of failures. Biometric authentication makes the most of unique existing character in every human being as factor to verify. However, there are still many hard works on the accuracy rate of each method plus the tolerance to practical attacks available today.

V. ACKNOWLEDGMENT

I am deeply grateful to **Hyma.J, AssociateProfessor**,GITAM deemed to be university, Visakhapatnam, for his constant support and guidance throughout the project.

.

REFERENCES

[1] Abdal-Ghafour, N. M., Abdel-Hamid, A. A., Nasr, M. E., & Khamis, S. A. (2016, 28-30 Nov. 2016). Authentication enhancement techniques for BAC in 2G E-passport. https://www.semanticscholar.org/paper/Authentication-enhancement-techniques-for-BAC-in-2G-Abdal-Ghafour-Abdel-Hamid/cee80d22cbadad649424bb60a548fad7fb437e68

[2] Ali, L. E., Luo, J., & Ma, J. (2016, 6-10 Nov. 2016). Iris recognition from distant images based on multiple feature descriptors and classifiers. Paper presented at the 2016 IEEE 13th International Conference on Signal Processing(ICSP https://www.hindawi.com/journals/complexity/2021/6641247/

[3] Ali, M. L., Thakur, K., Tappert, C. C., & Qiu, M. (2016, 25-27 June 2016). Keystroke Biometric User Verification Using Hidden Markov Model. Paper presented at the 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud). Alzubaidi, A., & Kalita, J. (2016). https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-020-0100-8

[4] Authentication of Smartphone Users Using Behavioral Biometrics. IEEE Communications Surveys & Tutorials, 18(3), 1998-2026 https://ieeexplore.ieee.org/document/7423666?reload=true

[5] Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., M, S., . . . ller. (2011). http://dl.acm.org/citation.cfm?doid=2037373.2037442

[6] The study on using biometric authentication https://www.sci.nu.ac.th/sciencejournal/index.php/journal/article/download/ID457/pdf

[7] Buza, K. (2016). Person Identification Based on Keystroke Dynamics: Demo and Open Challenge. http://ceur-ws.org/Vol-1612/paper21.pdf