

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

Two Step Authentication Using Selfie

Akshay Surve, Radhika Degloorkar, Pinku Margale, Shubham Jadhav

B. E Students, Department of Computer Engineering, Maaer's MIT College of Engineering, Pune, Maharashtra, India

ABSTRACT: Face recognition is important for a major role in biometrics research which helps to identify the users based on various parameters. In this fast developing technological world face recognition is increasingly used to distinguish the users in mobile. In existing system we can access any system/application using username and password. After entering correct username and password we get access to the system, but this traditional account/password-based authentication is not privacy- preserving. Programmers can steal the credentials of user by simply introducing spyware in the system. So mainly security issue occurs. This security issue we can solve using two step authentications. By looking at new selfie trend we have proposed new system which is called two step authentication using selfie. It uses selfie password as second layer of authentication.

KEYWORDS: Android; Selfie Image; Face Recognition; Face Detection; Authentication

I. INTRODUCTION

In secure system, to access the system one has to authenticate the system. Authentication is the process of verifying user's identity. The common authentication method uses text password to access the system. Some systems provide two factor authentication using OTP (one time password) or graphical passwords. Aim of authentication should be checking who you are, and not what you remember. In our proposed system, we are using selfie password for verifying user. Selfie password is form of biometric password which uses facial characteristics of particular person as a password. It is second layer of authentication in our system. The paper is divided into V sections. In section II literature survey of face recognition in network-based system is presented. Section III describes the Existing system which we are using currently. In the section IV we have elaborated proposed system. Section V concludes and gives future scope for this system.

II. LITERATURE SURVEY

In this paper [1] it presents a mobile application for real time facial expression recognition running on a smart phone with a camera. That system uses a set of Support Vector Machines (SVMs) for classifying 6 basic emotions and natural expression along with checking mouth status. While the system keeps updating natural features, it creates new dynamic features with displacement between latest natural feature and current feature if the face is recognized as non-natural expressions, and the system returns the recognized expression by the SVM classifiers for facial expression recognition with the dynamic features. this paper [2] describes, face recognitions plays a major role in biometrics research which helps to identify the users based on various parameters. The goal of the paper is to provide mobile users to safeguard their device when some intruder tries to access the device. This paper [3] states that new internet-based face recognition system to be used in portable devices. The proposed system uses mobile device only for image capturing and user-interface. All complex image processing tasks are performed by a remote high-powered network server to achieve robust and real time face recognition. In the paper [4] sensor-assisted facial authentication method to overcome these limitations. Results show 95-97% detection rate and 2-3% false alarm rate over 450 trials in real-settings, indicating high security obtained by the scheme ten times faster than existing 3D facial authentication. This paper [5] talks about there work with the plan what's more, execution of face acknowledgment applications utilizing our portable cloudlet-cloud design named MOCHA and its underlying execution comes about.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

III. EXISTING SYSTEM APPROACH

In existing system, we can access any system/application using username and password. Once we enter the correct username and password, we get access to the system, but this traditional account/password-based authentication is not privacy-preserving. It might be simple for programmers to introduce some spyware to take in the login secret key from the web-browser. So mainly security issue occurs. Some systems use OTP (one time password) as a second layer of authentication. [6] in this they have implemented colour shade scheme for second layer of authentication. Usability of this scheme is low.

IV. PROPOSED SYSTEM APPROACH

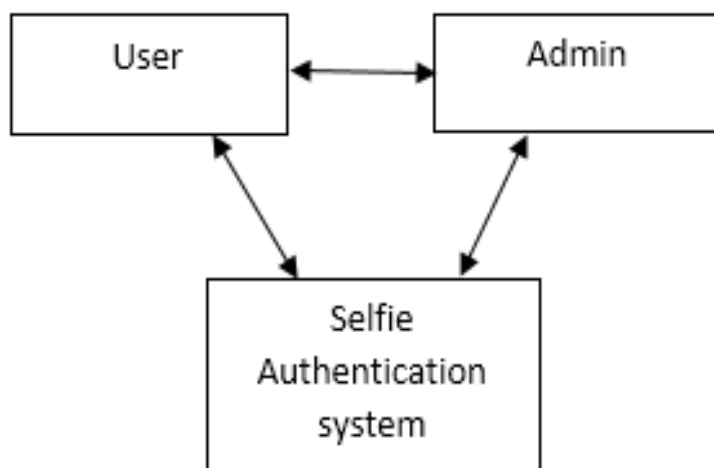


Fig.1 Block Diagram of Proposed System

In a Two Step Selfie Authentication, system contains mainly user and admin modules. In this system we can maintain security. If any user wants to access system/application, user must take a selfie with a particular angle. If user takes selfie properly with that particular angle then user can access the system. If not then user cannot proceed further.

User:

First user has to do the registration on web portal by filling the details and taking selfie from different angles. After registration user logs in with correct username and password. After successful authentication of first layer, user requests admin for access to the system/application for further process. Admin views the request and notifies user to take a selfie with particular angle. If user takes a selfie with that angle and that matches with the stored image then user can access the system/application for further process.

Admin:

Admin logs into the system. Admin can view the request by the user. Then admin can send the notification to that user to take a selfie with particular angle for getting a system/application access for further procedure. Admin can also view all the information of user.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

Selfie Authentication System

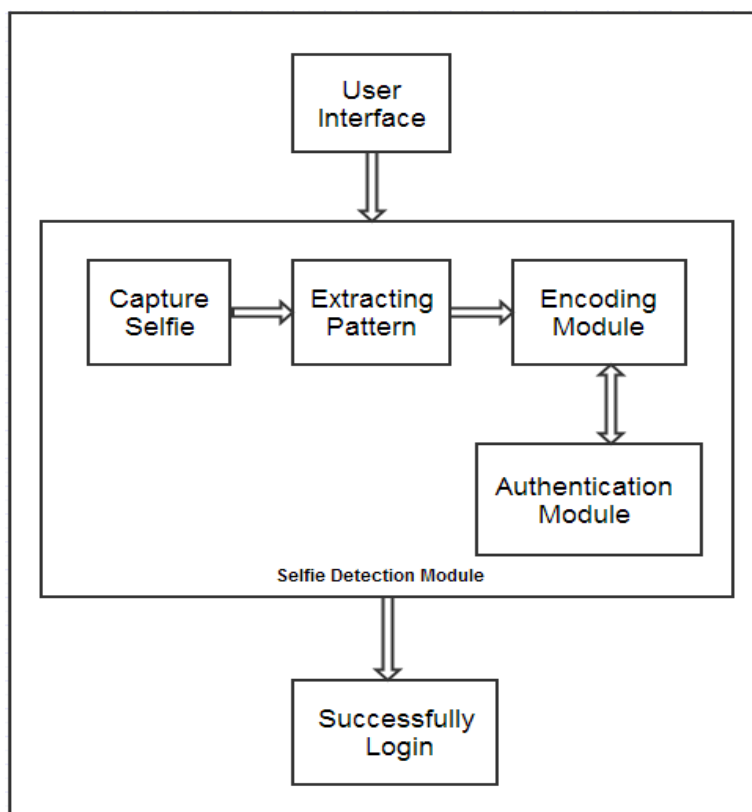


Fig.2 Block Diagram of Selfie Authentication System

In this, selfie authentication system contains a training image dataset. In this system, user's captured selfie image is compared with training dataset.

❖ **User Interface:**

It is an interface where the system will ask to enter the details of user like, Login Id and Password.

❖ **Selfie Detection Module:**

1. Capture selfie:

If your login Id and password is correct then system will ask user to take a selfie.

2. Extracting Pattern:

It will extract the useful patterns from the selfie taken by user by using feature extraction algorithm like geometry based, template based, Appearance based approaches.

3. Encoding Module:

Data extracted from selfie will be encoded using data encryption algorithm like RSA etc.

❖ **Authentication Module:**

In this module actual verification of user will be done. In this module data obtained from user is compared with the data stored in database.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 2, February 2018

❖ Successful Login:

After successful authentication of user, actual user interface of system will appear.

V. CONCLUSION AND FUTURE SCOPE

We can provide more security to access the system/application. It is very easy to use. It is more secure than traditional authentication. It restricts various attacks like shoulder surfing, eavesdropping. There is scope for improvement in the feature extraction algorithm. In the future we can improve the accuracy of system.

REFERENCES

- [1] Myunghoon Suk and Balakrishnan Prabhakaran Department of Computer Engineering The University of Texas at Dallas, Richardson, "Real-time Mobile Facial Expression Recognition System – A Case Study" 2014 IEEE Conference on Computer Vision and Pattern Recognition Workshops 23-28 June 2014
- [2] Deepak S , Sai Goutham N2 Programmer Analyst, Cognizant Technology Solutions, India1 Market Analyst, GoFrugal Technologies, "Face Recognition using Cloud Based Security in Mobile Devices" India2 International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 6, June 2015
- [3] Keita Imaizumi and Vasily G. Moshnyaga Graduate School of Engineering, Faculty of Engineering Fukuoka University Fukuoka, "Network-Based System for Face Recognition on Mobile Wireless Devices", 2014 Fifth International Conference on Intelligent Systems, Modelling and Simulation, 147
- [4] Shaxun Chen, Amit Pande, Prasant Mohapatra ,Department of Computer Science, University of California Davis, CA, 95616 USA, "Sensor-Assisted Facial Recognition: An Enhanced Biometric Authentication System for Smartphones" ,2013 IEEE Third International Conference on Consumer Electronics $\gamma\gamma$ Berlin (ICCE-Berlin), 9-11 Sept. 2013
- [5] Tolga Soyata , Rajani Muraleedharan , Colin Funai , Minseok Kwon , Wendi Heinzelman ,Dept. of Electrical and Computer Engineering Dept. of Computer Science University of Rochester Rochester Institute of Technology Rochester, NY 14627 "Cloud-Vision: Real-time Face Recognition Using a Mobile-Cloudlet-Cloud Acceleration Architecture" ,12th annual international conference on mobile systems, applications, and services pages 109-122, Bretton woods, new Hampshire, USA – June 16-19,2014 ,ACM 2014, ISBN: 978-1-4503-2793-0.
- [6] Manish M. Potey, Dr. C. A. Dhote, Deepak H. Sharma, Associate Professor, Department of Computer Engineering, K J Somaiya College of Engineering Mumbai, India, "Secure Authentication for data protection in cloud computing using color schemes", 2016 international conference on computational systems and information system for sustainable solutions,978-1-5090-1022-6/16/\$31.00 2016IEEE 427.