PROVIDE SECURITY TO USERS THROUGH BIOMETRIC AUTHENTICATION

[1]Kanchan Sharma, [2]Mamta Kumari, [3]Neha Giri,
[4]Rohit Kumar, [5]Mr. Ashok Rai

[1,2,3,4]CSE/IT, [5]Assistant Professor, CSE/IT

Buddha Institute of Technology, GIDA, Gorakhpur, India

ABSTRACT:

This application is a social media application but it increase the security which is important for the users.In this application security provide to the users with their Aadhar number, fingerprint and face. With the using of Aadhar number and two biometrics the human can create only one account which is a way to control the creating unnecessary data.

Biometrics are automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic.This project is developing with the help of python programming language. This application increases the security level and control the fake account which are unnecessary. This application also tries to control the fraud. Biometric is very interesting and exciting field that has been growing exponentially in recent year.

This Project increases the security level of social media by introducing biometric authentication. Increasing both privacy and identity security. Possibly in the near future, you will not have to remember PINs and passwords.

Keywords: *Ardiuno Uno, Machine, Operating System, Python , Scanner with connecting wires.*

1. Introduction

“Biometric technologies” are automated method of verifying or recognizing the identify of a living person based on a physiological or behavioural characteristic.

There are two key words in this definition: “automated” and “person”. The word “automated” differentiates biometrics from the larger field of human identification science. Biometric authentication techniques are done completely by machine, generally a digital computer.[1]

Forensic laboratory techniques, such as latent fingerprint, DNA, hair and fiber analysis, are not considered part of this field. Although automated identification techniques can be used on animals, fruits and vegetables manufactured goods and the deceased, the subjects of biometric authentication are living humans. For this reason, the field should perhaps be more accurately called “anthropometric authentication”.[3]

The second key word is “person”. Statistical techniques, particularly using fingerprint patterns, have been used to differentiate or connect groups of people or to probabilistically link persons to groups, but biometrics is interested only in recognizing people as individuals. All of the measures used contain both physiological and behavioural components, both of which can vary widely or be quite similar across a population of individuals [8]. The behavioural component of all biometric measures introduces a “human factors” or “psychological” aspect to biometric authentication as well.

So “biometric”, in this context, is the use of computers to recognize people, despite all of the across-individual similarities and within-individual variations. Biometric systems inherently require no identity data, thus allowing anonymous recognition.

The Purpose of this project is to build the secure social media app for the human. With the

help of this app we can give security to people, in this app, only one person can create his own account so that no one can use it wrongly.

Biometric authentication has grown in popularity as a way to provide personal identification.[4] Person’s identification is crucially significant in many application and the hike in credit card fraud and identify theft in recent years indicate that this is an issue of major concern in wider society.

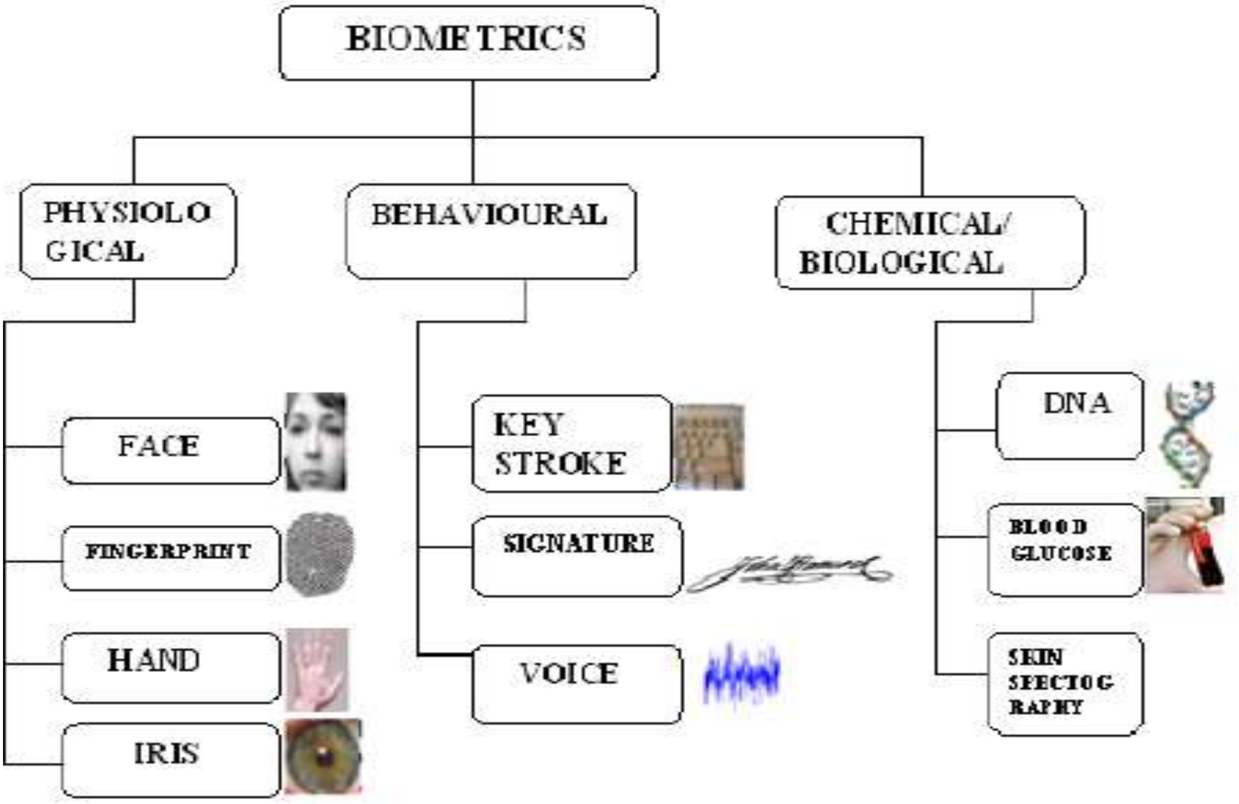

Fig 1: Biometrics

2. Types of biometric identification

2.1 Fingerprint

Fingerprint identification techniques all into two major categories-Automated Fingerprint Identification System (AFIS) and fingerprint recognition systems. AFIS is typically restricted to law-enforcement use.

Fingerprint recognition derives a unique template from the attributes of the fingerprint without storing the image itself or even allowing for its reconstruction [5]. Fingerprint recognition for identification acquires the initial image through live scan of te finger by direct contact with a reader device tha can also check fo validating attributes such as temperature and pulse. Since the finger actually touches the scanning device, the surface can become oily and cloudy after repeated use and reduce the sensitivity and reliability of optical scanners. Fingerprint recognition is generally considered reliable enough for commercial use, and some vendors are already actively marketing readers as part of Local Area Network login schemes.

Fig 2: Fingerprint

2.2 Face

Face recognition technology is still its early stage, and most tests and application have been run against relatively small database [4]. A facial recognition system is a technology capable of matching a human face from a digital image or a video frame against a database of faces, typically employed to authenticate users through ID verification services, works by pinpointing and measuring facial features from a given image.

Facial recognition systems attempt to identify a human face, which is three-dimensional and changes in appearance with lighting and facial expression, based on its two-dimensional image.[2] To accomplish system perform four steps. First face detection is used to segment the face from the image background. In the second step the segmented face image is aligned to account for face pose, image size and photographic properties, such as illumination and greyscale. In the third steps the facial feature extraction. And in the last step matched against a database of faces.

Fig 3: Facial recognition

2.3 Retinal Scan

A retinal scan is a uses unique patterns on a person's retina blood vessels.[6] The human retina is a tissue made up of neural cells that is located in the posterior portion of the eye. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique, making retinal scan an emerging authentication method. Although retinal patterns may be altered in cases of diabetes, glaucoma or retinal degenerative disorders, the retina typically remains unchanged from birth until death. Due to its unique and unchanging nature, the reina appears to be the most precise and reliable biometric.

A retinal scan is performed by casting an unperceived beam of low-energy infrared light into person's eye as they look through the scanner's eyepiece.[7] This beam of light traces a standarlized path on the retina. The pattern of variation is digitized and stored in a database.

Fig 4: Retinal Scan

2.4 Voice

Voice or speaker recognition is the ability of a machine or program to receive and interpret dictation or to understand and carry out spoken commands.[3] Voice recognition has gained prominence and use with the rise of AI and intelligent assistants. Voice recognition systems enable consumers to interest with technology simply buy speaking to , it enabling hands-free requests, reminders and other simple tasks.

Speech recognition is an interdisciplinary subfield of computer science and computational linguistics that develops methodologies and technologies that enablethe recognition and translation of spoken language into text by computers. It is also known as automatic speech recognition (ASR) , computer speech recognition or speech to text (STT) [4]. Speech recognition applications include voice user interfaces such as voice dialing, call routing, domotic appliance control, search key words, simple data entry preparation of structured documents, determining speaker characteristics, speech-to-text processing and aircraft.

Fig 5: Voice

2.5 Signature

Signature recognition is an example of behavioural biometrics that identifies a person based on their handwriting. It can be operated in two ways:

Static: In this mode, users write their signature on paper, and after the writing is complete, it is digitized through an optical scanner or a camera to turn the signature image into bits[8]. The biometric system the recognizes the signature analyzing its shape. This group is also known as “off-line”.

Dynamic: In this mode, users write their signature in a digitizing tablet, which acquires the signature in real time. Some systems also operates on smart-phones or tablets with a capacitive screen, where users can sign using a finger or an appropriate pen. Dynamic recognition is also known as “on-line”[7].

The most popular pattern recognition techniques applied for signature recognition are dynamic time warping, hidden Markov models and vector quantization.

Fig 6: Signature

3. Features

3.1 Requires data validation and integrity check

This project ensures that the data being provided by the user is handles in a secured manner, that is, it is validated everything that is passed through it. For eg, if the user enters a number in username blank, string type data in Aadhar card number and any wrong format of email address blank then it throws an error message to insert numbers [1]. It also validate the Aadhar card number.

3.2 Security

In this project, high level of security is provided by biometric authentication, which means, the fingerprint provided by the user act as their password. For making it more secure, all the user accounts is linked to their Aadhar card to verify their details.

3.3 Simplicity

This project makes the social media application secure. Today generation everyone well known about the social media and its use therefore they can easily use it.

3.4 Control creating unnecessary Data

If users have any account and he/she want to create new another account it is controlled by this project therefore, the user can't create another account.

4. Methodology

4.1 Methodological Approach

This project is made as a waterfall approach, which is a very simple and efficient approach. It included following steps:

4.2 Requirement Analysis

In this project first analysis is done that what this system requires and what are the extra requirements of the users to make it more efficient. Data is also collected from different sources.

4.3 Design

After requirements and data are collected, designing of the project started which include flow chart, SRS etc for understanding how to do this project.

4.4 Implementation

After designing, the implementation phase came where coding of the project is done. In this project the coding is done in python language which included MySql for backend purpose.

4.5 Verification

At last, the errors and faults are removed and project is finalized.

5. Related work

Biometric (bios = "life", metron = "measure") is the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In this app the identify verification is performed in some ways:

5.1 **Thumb Scanning:** It is done by thumb scanner, in is app Ardiuno uno is also used. Arduino is an open hardware platform[1]. There are Arduino IDE, an Integrated Development Environment required for programming Arduino devices.

6. Conclusion

6.1 This project gives an easy and efficient way of banking and increase the security level by biometric authentication and aadhar linked. It increases the ability to do online banking in a secured manner.

6.2 The modules results in a faultless banking as the errors are removed in every module when the details provided by the users by error messages.

The different modules are :

Registration : For new users

Login : For registered users. It further include submodules like, Friend request send and receive also accept and reject, Chatting, Profile setting.

6.3 This project "Biometric Authentication" is made to increase the features of any social media application by integrating biometric authentication system in it[3]. This project also gives a way to verify details of the users by linking their details to their Aadhar card details.

6.4 This project includes the features like, error detection, security, easier, and flexible [2]. This project has modules: Registration, Login and sub modules: Friend request send and receive, Chatting, Profile Setting.

6.5 This System is made on python language, using aurduino uno, fingerprint scanner, and other electronic systems. It uses many softwares like: Python IDLE, Aurduino uno IDLE and MySql for backend.

REFERENCES

[1]. Aurduino : A technical refence book by J.M. Hughes Released May 2016, Published by O'Reilly Media,Inc.

[2]. MySQL Reference Manual by Michael Widenius,David Axmark,Kaj Arno Released June 2002 Published by O' Reilly Media,Inc.

[3]. MySqL for python by A Lukaszewski – Cited by 15

[4]. Paper: Biometric Authentication : A review- Bhattacharyya Cited by 316

[5]. Python for Programmers book by Paul J. Deital, Harvey Deital Released March 2019, Published by Addison-Wesley Professional

[6]. by M Liu · 2004 · Cited by 12 — Cite this paper as: Liu M., Jiang X., Kot A.C. (2004) Fingerprint ... In: Zhang D., Jain A.K. (eds) Biometric Authentication.

[7]. A survey on iris biometrics research: 2008-2010, Boywer cited by 165.

[8]. by W Wójcik · 2016 · Cited by 18 — Face recognition.