ISSN Number: 2454-2024(Online)
International Journal of Technical Research & Science

ARCHITECTURE OF BIOMETRIC SYSTEMS FINGERPRINTS FOR HOME SECURITY SYSTEM

Vikash Kumar[1], Lokesh Kumar[2], Bhupender Sharma[3], Naman Chauhan [4], Ritik Kumar Singh [5], Bhanu Pratap Singh [6]
E-Mail Id: vikashpaper1991@gmail.com, lokeshkashyap1707@gmail.com, pandit271997@gmail.com, namanc206@gmail.com, ritiksingh0101@gmail.com, pratap.bhawani111@gmail.com
[1,3,4,5,6] COER University, Roorkee, Uttarakhand, India
[2]Kalinga University, Raipur, Chhattisgarh, India

Abstract- Home Security System has become the prime concern in the recent years or time. If we talk about the technology so now a days technology comes out every second, ample home-based security systems have been expanding and implementing with many of the latest features. So, that we can keep our home safe [15]. This paper represents the design and model or prototype implementation of a home security system that makes the home security more convenient, flexible, and less expensive.
Keywords: Biometric techniques, fingerprint verification, smart home, home security, home network.

1. INTRODUCTION

Biometrics is that process which are automate the process of the recognizing or identify an authorized person which is based on their psychological or behavioral characteristics. It is a technology which is used to analyze, identify, and measure an individual's access using biometrics devices. There are number of different characteristics on which biometric devices processed the identification and analyzation process.

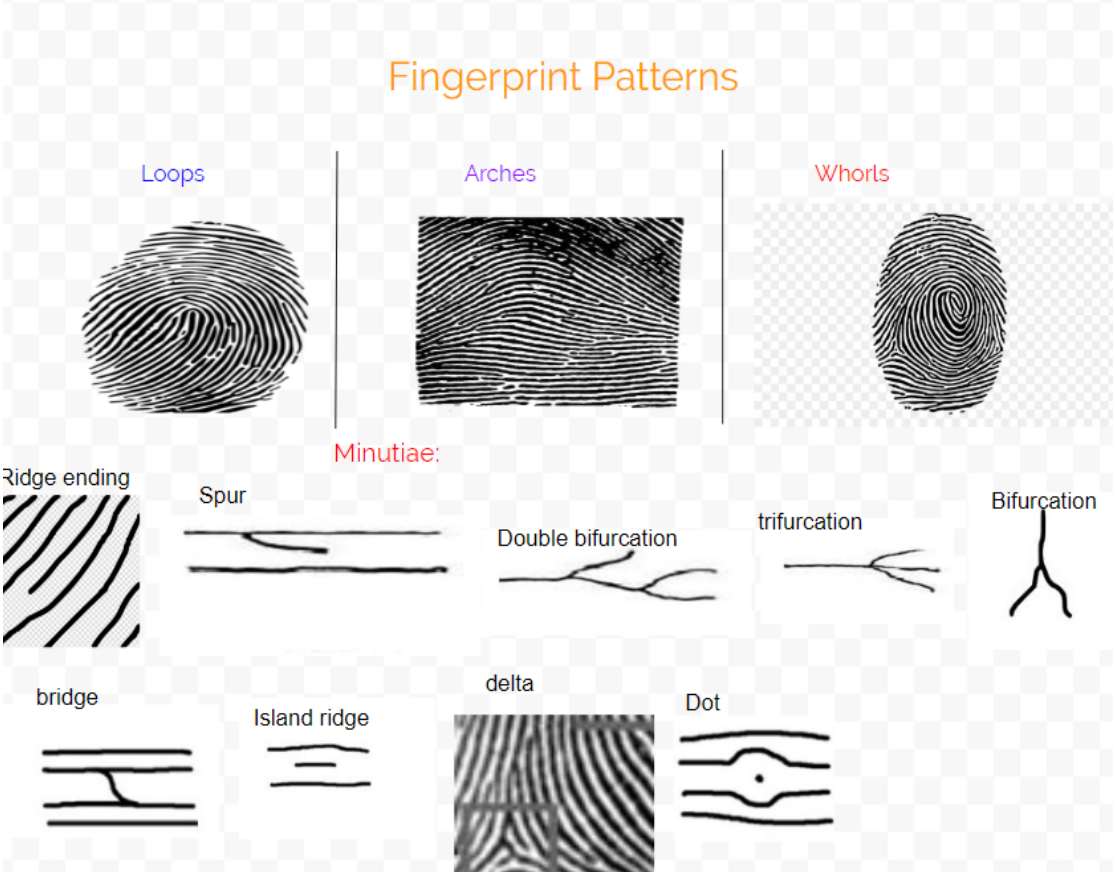

Fig. 1.1 Fingerprint Patterns

2. RESEARCH

Technology: Biometric is the latest technology that is used as an application to conduct the statistical analysis on biological data.Its components: Reader, Software and Database.
Architecture Industry: Architecture industry is responsible for planning and designing new building in an area. They take major consideration so that no built building collapse in any way or it any situation.

2.1 Problem Statement OR Related Research OR Related Work

- Strategy for resolving lack of encryption in IOT device using biometric fingerprint technique.[18][19]
- Biometrics are not the private
- Biometrics are the Hackable
- Biometrics Hack May Have Greater Consequences
- Strategy for reducing the lack of encryption in IOT automated home using the biometric techniques [19][18].

So, in this proposal we will discuss in brief about the problem, identifying it and how to resolve it with simple technique with the aims and its objectives that have been planned.

2.2 Aim and Objectives

- The aim is to be capture, identify, and analyze an item of the biometric data from the personnel. It could be the image of their face, their fingerprint, a record of their voice, or hand, palm vein.
- Then captured data is compared to be the sets of biometric data of all the authorized persons kept in the database.

3. LITERATURE REVIEW

Presently a day's cell phones, or PDAs are turning out to be most famous all over the planet since it joins a large portion of the quality cell phones with the other determination like Worldwide Situating Framework (GPS), it is essentially for that gives clients situating, route and timing (PNT) administrations and the web perusing, remote loyalty, and the outsider applications. For example, in association to iris recognition, the significant advancements started in the late 1980s with the first algorithm patent that is issued in 1994 for automated iris recognition. Nowadays, most of the airports and border controls are using fingerprints, facial characteristics, or iris scanning on record for reference point when a suspicious or suspected person tries to breach security. Among cell phones, Android cell phones are turning out to be so famous now a days. As of now, Android OS catch or rules around 81% of the world cell phone commercial center. So, our avoidance of wrongdoing by utilizing android cell phone is one of the objectives or points of this examination. We should have some familiarity with the tech wrongdoing which is developing or speeding up the mobile's innovation world.

4. RESEARCH METHODOLOGY

- Fingerprint Verification
  - So it is the variety of the approaches to fingerprint verification. It can be detected if some of them when a live finger is presented.
- Hand geometry
  - It is the part of physical characteristics of the human being hand and fingers[14].
- Voice verification
  - It is basically the voice or sound of the human beings and from this we can also lock or unlock our devices.
- Retinal scanning
  - It is the internal eyes part of the human body and it is the where the unique patterns of the retina are scanned by the low intensity light source via the optical coupler.
- Iris scanning
- Signature verification
- Facial recognition

4.1 Research Design and Methodology

So basically, in this chapter we discusses the research the design and patterns, target to the population, which are describes to the research instruments, and the sample and the sampling of the procedures, to the data collection for the procedures and concludes by description of data analysis procedure which are described.

4.2 Requirements Resources

Biometric Evaluation Framework: Python[16] (libraries which is used in this like numpy, pandas, matplotlib, plotly, OpenCV).
OpenCV[17]: for image processing and scanning their face and then identify Pandas and matplotlib and plotly for dataset and presenting the dataset as graphically

4.3 Research Plan

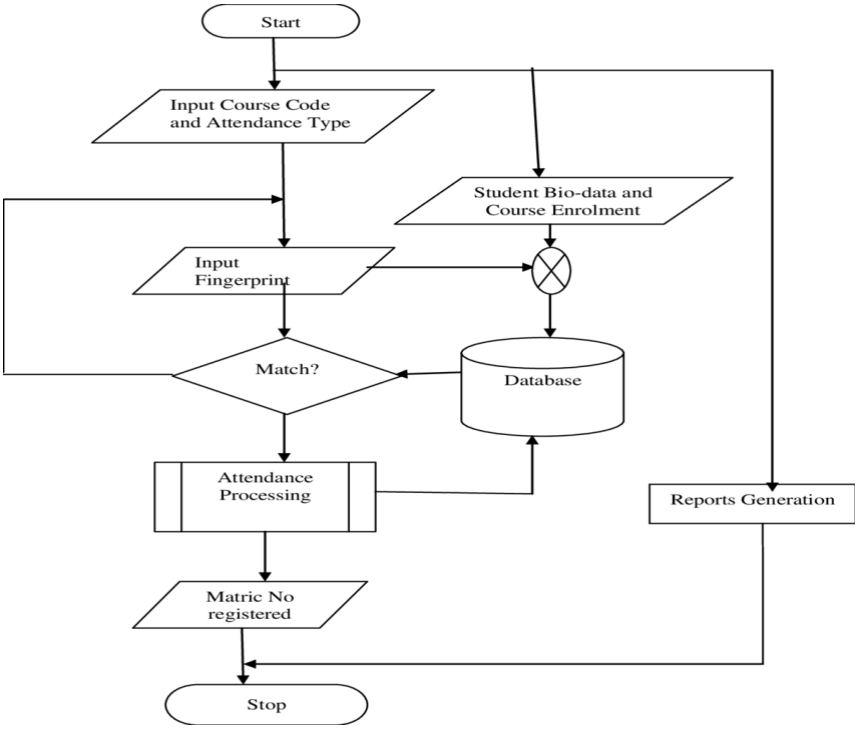

Fig. 4.1 Flowchart of Research Plan Biometric

Identifies the individual as a genuine malicious user.

- Authentication
- Authorization
- Verification
- Authentication

So, basically authentication is all about the validating your credentials like the Username and the password to verify your identify [11].

For example, if you are going to cinema hall to watch the movie so there will be a process before entering in the cinema hall. Showing the ticket. So firstly, they will verify your account related data or information like username and password or scan the QR code through their scanner machine then if machine will get the response your data is correct or valid. So they will you give you permission to go watch the movie or entry in the cinema hall or if your details will not valid on their database so they don't give you the permission go to watch the movie [12].

4.4 Authorization

Authorization it is the process to determine whether the specific applications, files and data are used by only authenticated users. It verifies your access to use the resources such as applications, information, databases, files, etc[13].

Example: So, in authorization [13] process firstly this process will come after the authentication process so basically it is the process which user can access specific things like they get the air conditioner wind or to sit on the chair or to the wear the 3D glass, etc.

4.5 Verification

"Verification is a process to verify the valuation, ownership, existence and possession of a particular Liability or Assets."

"The verification of the assets implies an enquiry into the value, ownership and the little; the existence and possession the presence of the any exchange in the assets".

4.6 Two factors Authentication

Before we move to Two Factor Authentication concept, first we have to understand what Identification and Authentication is [11].

So, let's take the first example of practical life, in which Amit reaches the hotel for check-in. and Amit had already booked in to the hotel. After reaching reception Amit says I am Amit Kumar and have booked a room for three days. The process of declaring Amit's name, i.e. the process of claiming his identify, is called Identification. Saying what you are is Identification. Now the receptionist says, okay sir, please show me your

ID proof. The receptionist now verifies Amit's ID proof and checks whether the mentioned name is correct or not. This process of verification carried out by the receptionist is called authentication [11].
This means authentication is verification of identify [12]. Now for better understanding it more clearly we take the second example of the digital world.Suppose I want to log in to my Gmail. So what do I, I open Gmail and write my email ID i.e. Gmail ID in place of username. And I say to Gmail, Bro, I am Amit Kumar and this is my Gmail email id. This process of claiming this identify uniquely is called Identification, which means telling who you are. Now what Gmail says it's okay, if you are Amit Kumar, then prove it, means provide the password of this ID.Now I type the password and press enter, after this, Gmail verifies the user ID and password in the backend. That is, Gmail verifies the identify that we have mentioned. So basically this is the concept of authentication, it is called simple authentication, that is, only once the authentication process is carried out. But in two factor authentication, authentication process would have happened twice with the different factors. Factors – So there are the three types of factors which are,

- Something you know – Something you know, which you can keep in memory, things you can remember like your password and PIN.
- Something you have – Something you have, which you physically possess like the smart card, digital signature in pen drive, ATM card.
- Something you are – Something you are means your biometric parameters like the fingerprint, your voice, retina and face.

So basically from in these two factor authentication, out of these 3 factors, 2 factories are used for authentication. For example,If you have activated 2 Factor Authentication on a website, then you will have to enter the username and password at the time of login, but along with that you will have to enter an OTP which will be sent on your mobile to complete. So now basically for 2 factor authentication we have to take two different factors. Using 2 factor authentication greatly reduces the probability of your account being hacked.
Because of even if someone gets your account username and password, then they will not be able to login to your account. Because it will also require OTP to login your account to access, which is only is going to come on your mobile.

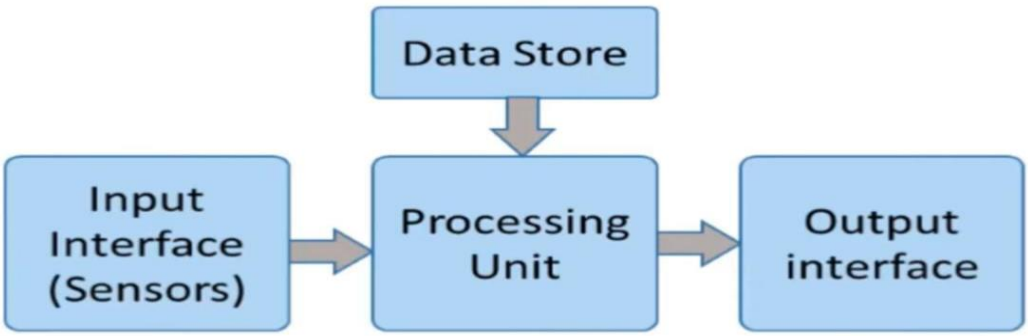

Fig. 4.1 Biometric System

- It is the most known and used biometrics solution to authenticate people on the biometric systems.
- Whenever we abstract the original finger print through the optical devices then we will get the as a result of monochrome image of a finger print which are the 8 bit grey scale.

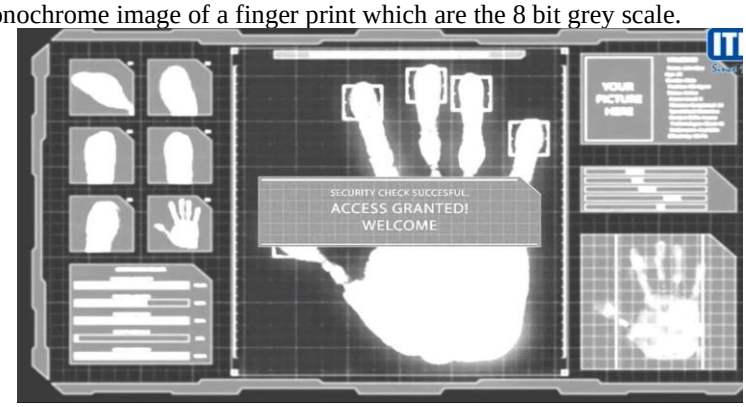

Fig. 4.2 Fingerprint Sensor

4.7 Algorithm of Fingerprint

Physiological characteristics contains vein technology, iris, palm print, face, and behavioral characteristics. There are some major examples of physiological characteristics like voice, odour, gait recognition.

There are number of applications or places such as banks, airports, Corporate IT, hospital security and all other restricted areas.We can use different types of authentications to identify authorized personnel.

- What do you have – smart card, key card, or token.
- What do you know – a PIN, password, or personal information.
- Who you are – a biometric characteristic for the authentication.

Biometric is the most or can say part of most powerful security authentication type which can't be broken, stolen, borrowed or forgotten and the forging biometric is the partially impossible. The personal identification using our palm and hand has gained the most research attentions this year's compared to other security identification methods. In palm vein, there are numbers of different properties and in vein the information is the very unique to person to person for each even between the twins. It is very difficult to be broken or damaged and if we are talking about the secured part, so it is highly secured as it is part of the authorized personnel body and it is residing inside the body. These characteristics make hand and palm vein is better biometric features compared to face and fingerprint.

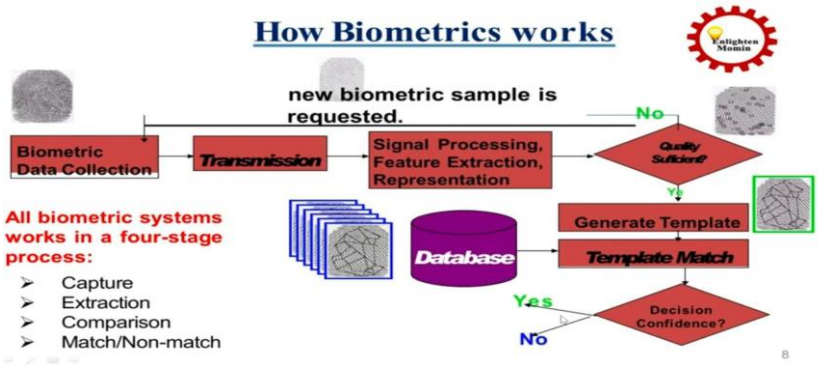

Fig. 4.3 Working Process Background

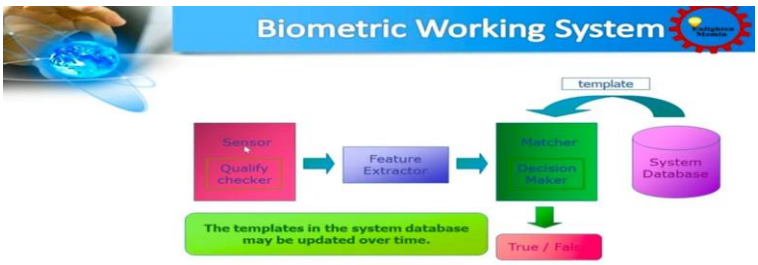

Fig. 4.4 Biometrics in Architecture Industry

RESULTS

The simplicity, adaptability, and cost-effectiveness of the prototype home security system were significantly improved by its successful design and implementation. The system's fingerprint verification and biometric procedures, which improve security and user authentication, are important aspects. Testing showed that the system offered real-time notifications and successfully prevented unwanted access, guaranteeing strong home security. Furthermore, the system's user-friendly control and seamless functioning were made possible by its interaction with smart home devices.

CONCLUSION

The created home security system shows to be a workable answer to the problems associated with contemporary house security. The system maintains user ease while guaranteeing a high level of security through the utilization of sophisticated biometric procedures and fingerprint verification. Positive test results and a smooth installation show that these kinds of systems are both feasible and efficient. To provide an even more complete security solution, future improvements might concentrate on adding more smart technologies and strengthening system integration.

REFERENCES

[1] Biometric Authentication Technology: From the Movies to Your Desktop or pc by Fernando L. Podio and Jeffrey S. Dunn.

[2] Common Biometric Exchange File Format (CBEFF) NISTIR January 3, 2001.Fingerprint Identification FBI Technology Assessment Technology Assessment Using Biometrics for Border Security Using Biometrics for Border Security, November 2002 (GAO-03-174).

[3] Arunarani, S., & Gobinath, R. (2018). Literature review on multimodal biometrics. International Journal of Engineering & Technology, 7(2.26), 31. doi: 10.14419/ijet.v7i2.26.12529.
[4] Chaudhari, R., Pawar, A., & Deore, R. (2013). The Historical Development Of Biometric Authentication Techniques: A Recent Overview. International Journal of Engineering Research & Technology (IJERT), 2(10), 1-8.
[5] Disrupting Construction: A Breakdown On Startup Driven Innovation. (2020). Retrieved 18 April 2020, from https://www.startusinsights.com/innovatorsguide/disrupting-construction-industry-breakdown-startup-driven-innovation.
[6] Sealy, P. (2018). Get smart: why biometric cards will reshape the payments industry. Biometric TechnologyToday,2018(8),5-8.doi: 10.1016/S09694765(18)30125-5
[7] Selvam, Venkatesan & Gurumurthy, Sasikumar. (2015). DESIGN AND IMPLEMENTATION OF BIOMETRICS IN NETWORKS. Journal of Scientific Research and Advances. 1. 10.14260/jtasr/2015/27.
[8] Radzi, Syafeeza Ahmad, et al. "IoT based facial recognition door access control home security system using raspberry pi." International Journal of Power Electronics and Drive Systems 11.1 (2020): 417.
[9] Bhattacharyya, Debnath, et al. "Biometric authentication: A review." International Journal of u-and e-Service, Science and Technology 2.3 (2009): 13-28.
[10] Wayman, James, et al. "An introduction to biometric authentication systems." Biometric systems: Technology, design and performance evaluation. London: Springer London, 2005. 1-20.Sudha, L. R., and Dr R. Bhavani. "Biometric authorization system using gait biometry." arXiv preprint arXiv:1108.6294 (2011).
[11] Ribaric, Slobodan, and Ivan Fratric. "A biometric identification system based on eigenpalm and eigenfinger features." IEEE transactions on pattern analysis and machine intelligence 27.11 (2005): 1698-1709.
[12] Sahani, Mrutyunjaya, et al. "Web-based online embedded door access control and home security system based on face recognition." 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]. IEEE, 2015.
[13] Singh, B. P. & Joshi, A. (2024). Ethical Considerations in AI Development. In R. Kumar, A. Joshi, H. Sharan, S. Peng, & C. Dudhagara (Eds.), The Ethical Frontier of AI and Data Analysis (pp. 156-179). IGI Global. https://doi.org/10.4018/979-8-3693-2964-1.ch010
[14] Joshi, A., & Tiwari, H. (2023). No. 10. An Overview of Python Libraries for Data Science: Manuscript Received: 20 March 2023, Accepted: 12 May 2023, Published: 15 September 2023. Journal of Engineering Technology and Applied Physics, 5(2), 85-90.
[15] Thakur, Gesu, Yogesh Kumar, and Gunjan Bhatnagar. "Challenges and Opportunities Presented by the Internet of Things (IoTs) in the Hospitality Industry." Mathematical Statistician and Engineering Applications 71.4 (2022): 2582-2597.
[16] Chauhan, Abhilasha, et al. "Intrusion Detection Systems Apropos of the Internet of Things (IoT)." Internet of Things and Cyber Physical Systems. CRC Press, 2022. 167-182.