e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

BIOMETRIC IN HEALTHCARE SECTOR : A REVIEW

Sushama Narsale[*1], Ketki Palekar[*2], Rudrakshi Padole[*3], Abhishek Raykar[*4], Prof. Pooja Sonavane[*5]

[*1,2,3,4]Student, Department of Computer Engineering,
Shri Chhatrapati Shivaji Maharaj College Of Engineering, Nepti, Ahmednagar, India

[*5]Professor, Department Of Computer Engineering,
Shri Chhatrapati Shivaji Maharaj College Of Engineering, Nepti, Ahmednagar, India

ABSTRACT

Technological advances have implications for the efficiency of the global health care system. It is not possible to deny the basic safety procedure to the patient records. Medical records matter to all patients and health professionals. Only an authorized person can have access of patient records, if an unauthorized person has access to a patient record can cause the wrong drug or even the death of the patient. The identification of an individual is a significant challenge. In this article we examined the various physical features as well as biometric behavioural techniques explained differently. We concluded that advanced security, identification and protection of health care information is at most necessary to prevent unauthorized access and threats to records.

Keywords: Biometric authentication, fingerprint authentication, facial authentication, hand details, iris, retina, signature, voice, biometric keystrokes.

I. INTRODUCTION

Biometrics authentication process is typically found in security processes that authenticate a user using unique biological traits such as physiological and behavioural traits. Because every individual is special in their own unique characteristic bodies the level of information protection associated with individuals get increases. Biometric authentication systems store this biometric information for the purpose of verifying the identity of a user. Since this data is proprietary to individual users, biometric authentication is more secure than traditional types of multi-factor authentication. In general, a word biometrics are formed from two words, that is, bio means life and metric means measure. This means that it measures an individual's unique biology. Biometric authentication is the process in which biometric traits are identified on physiological and behavioural traits.

Biometrics authentication is now being used by the health sector to secure patient and staff data. In today's Internet age, intelligent device security intelligence is frequently compromised. To build safety knowledge in health care, many traditional approaches have been implemented, such as paper verification, PIN verification, etc. But the big problem is that in the simple password technique, it can store in the memory. Second, it can be lost, misused and could be exchanged between co- workers. Therefore, safety cannot be ensured.

Patient safety data is the more important factor. Through biometrics, these issues can be resolved, staff authentication and patient record privacy can be protected against unauthorized access. Therefore, to fight with these problems of biometric identification is the most appropriate choice. Biometrical authentication is complete on behavioural and physiological traits. Physiological features include fingerprinting, facial recognition, iris scanning, retinal scanning, and hand geometry. Behavioural traits include voice recognition, signature checking and keystroke dynamics.

II. WHEN DOES BIOMETRICS BEGIN?

The term biometrics refers to the measurement of a person's unique characteristics for safety. Even if, until 1980, the word biometric did not exist initially. The first biometric reference was found in 1981 in a New York Times paper. Ancient Assyrians, Babylonians, Japanese and Chinese people used fingerprints to sign official documents. There is archaeological evidence that the Assyrians and ancient Chinese civilization used fingerprints as a way of identifying 7000 to 6000 BC. In India, fingerprints were used in July1859 by Sir William Herschel. In 1936 the ophthalmologist Frank Burch applied the concept of iris pattern to detect vision, individually. In 1965 North American airlines developed the first signature recognition system. In 1974 the University of Georgia began to use hand geometry. They use hand geometry in their food supply areas. The first retinal scanning

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

programs were used in 1985 to detect the discovery of the DOD at the Naval Postgraduate School. In 1964 and 1965, Bledsoe, as well as Wolf and Bisson, began using computers to see human faces. As a result, biometrics have been introduced and, over time, has acquired nearly all sources of information. In health, biometrics is used in the same way as in other domains.

Biometric detection has different characteristics that can be measured for everyone. It is also broken down into two categories: physiological and behavioral traits.

III. PHYSIOLOGICAL TRAITS

Physical attributes include:

A. Fingerprinting:

Fingerprint recognition refers to the automatic method of identification or authentication of an individual based on the comparison of two fingers. The reasons for fingerprint recognition are so popular that they are easily accessible, developed and accepted with respect to other biometric data.

The three basic models of fingerprint hills are arc, buckle i.e. loop, and verticilla i.e. whorl.

- Each pattern where a space between a side of the hand, finger and exits at the center to form an arc.
- With a loop the back enters a side of the hand, finger, then makes a curve, and then exits on the same side of the finger you entered. Loops are a very common pattern of fingerprints.
- Finally, a swirl is a pattern where the hills form a circle around the centerline.

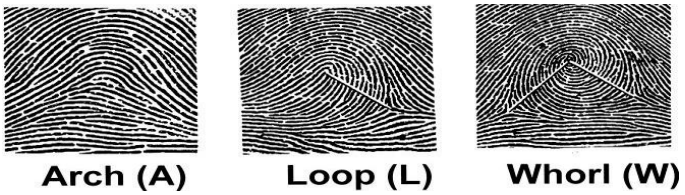

Fig.1. Arch and Loop and Whorl structure of a hand finger

B. Face recognition:

Faces are used extensively to distinguish individuals, and the biometric verification system plays an important role in the identification of an individual identity. A facial recognition technology widely used because it is inexpensive. Secondly, it's one of the invasive biometric methods available, because it doesn't require physical contact such as retinal scanning or fingerprinting.

Facial recognition works in all four steps:

1. A facial image is a form of photography or video. Your face may show up alone or in public.
2. The facial recognition program reads the geometry of your face. Key considerations include the distance between the eyes and the distance between the forehead and the chin. The program identifies facial markers and therefore the result is your facial signature.
3. The signature of your face, which is a math formula, is compared to a database of familiar faces
4. The decision is then taken.

Fig.2. Face Recognition

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

A. Iris Scanning:

The iris sweep measures various patterns on irises, circles that are colored in the human eye. The iris biometric scanner works by brightening the iris with invisible infrared light to capture unique models that are invisible to the naked eye. The iris reader detects and excludes eyelashes, eyelids and light which blocks certain parts of the iris. The result is an array of pixels containing only the iris. Then, the motif of the lines and colors of the eyes is analyzed to extract a small motif that incorporates details into the iris. This small model is entered into a computer and is compared to the models stored in a database of validation (matching individual models) or identification (matching one model at a time).

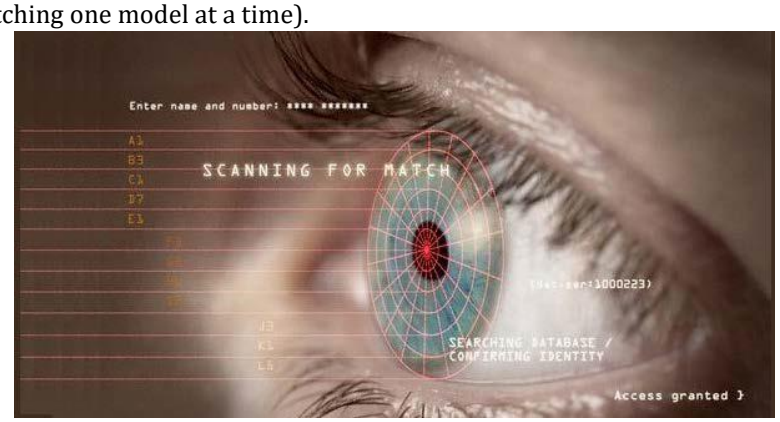

Fig.3. Iris Scanning

B. Retina Scanning:

Retinal scanning is a biometric system where a human retina blood vessel model is used. Retinal scanning utilizes infrared light for mapping. There is a great deal that affects the human retina, such as pregnancy. Everybody has a different retinal model. Even the same twins didn't have the same retinal model.

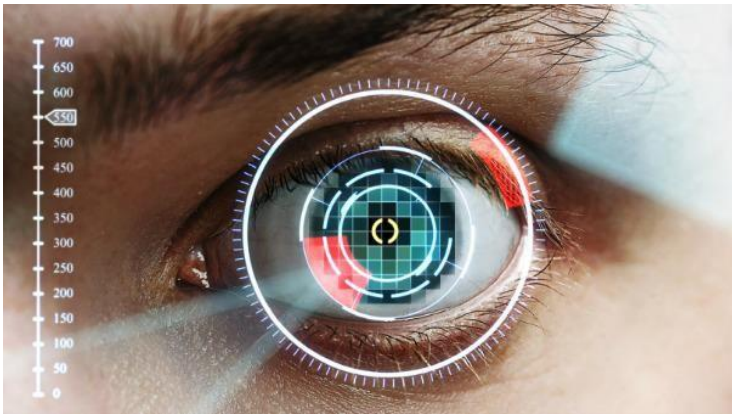

Fig.4 Retina Scanning

C. Hand Geometry:

Hand geometry another type of biometric method that enables users to be identified by the shape of their hands. It is a system of uniqueness whose recognition system is designed to measure the shape of the hand like its angles, width, length and distance between the limbs. In the first phase of the image processing, it is prepared to get the details from the hand. However, a hand is different from a background. Background illumination effects and noise create bad pixels in the picture. In the second step, the Filter function is used to suppress those pixels. Now the hand boundary is merely available.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

Fig.5. Hand Geometry

IV. BEHAVIORAL TRAITS

A. Voice Recognition:

Biometric voice authentication is the most widely used forms of authentication today. It is divided into two stages of extraction of the function and the stage corresponding to the function.

Voice authentication provides a cryptographic scheme, high-level security, and voice authentication requirements. The proposed voice authentication system to validate the user, and the user's voice is then encrypted through the Arnold card method and the Baker card.

Biometrical voice authentication is a cost- effective and accurate authentication method. A transaction performed by the biometric server, and the single voice pattern individuals stored in the database. The authentication initialization configuration requires the user to speak any random string of the digit, and then after the human speech capture and extraction function sent to the biometric server, Next, the biometrics server matched the incoming voice with the voice model stored in the biometrics server database. If the match is found, the identity of the user is verified. It helps to better identify users and avoid fraud.

Fig. 6. Voice Recognition

B. Signature Verification:

Signature verification is an individual behavior. It can be dealt with in a couple of different ways

- Static: This way, users register their signature on paper, then digitize it with a camera and a scanner. Pending verification is also known as offline check.
- Dynamic: For stronger authentication, users write their signature onto a tablet that makes it digital. This method of identification is also known as the Internet.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

Fig. 7 Signature Verification

C. Keystroke Dynamics:

Keystroke's dynamical capabilities require no special equipment. Keystroke dynamics is a process used to measure the speed of a human keystroke on digital equipment. That depends on the duration of the stay and the plan. Session time is when an individual presses a key while stealing the amount of time between releasing the key and the next press key.

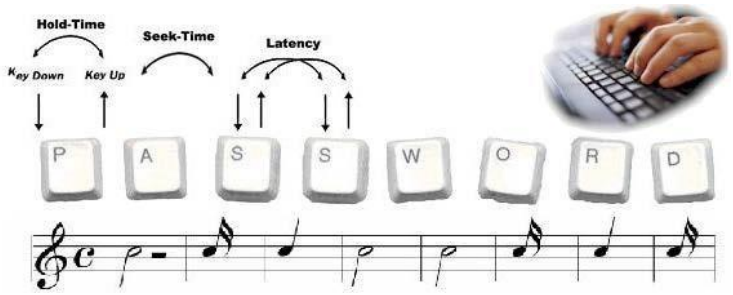

Fig.8. Keystroke Dynamics

V. IMPLEMNTATIONS OF BIOMETRIC IN HEALTHCARE SECTOR

Biometric features are being implemented in many areas of the healthcare industry, such as encryption and authentication, to enhance security. Healthcare Systems have secured network data transmission for telemedicine, patient identification and verification, medical record protection and disease diagnosis procedures. We are now going to look at the implementation of biometric authentication.

A typical biometric system requires all three steps to implement:

A. Enrollment:

Biometrics allows a person to be enrolled in a system by scanning and obtaining the person's characteristics, which are then stored because the model is in the centralized database of the system. The acquisition results of each person's feature induce the system to extract specific items and generate consistent results. Unique patterns of the individual to make the ability to access the system.

B. Verification:

In the verification mode, the system establishes the identity of the person by analyzing the biometric data entered using appropriate biometric models already stored in the centralized biological databases. In this mode, the system performs an individual comparison to ensure that the assertion entered is correct or not using the positive acknowledgement.

C. Identification:

The biometric system may operate in identification mode, or the verification mode is validated based on device confinement. The identification mode matches the request line model with known models that are formed with multi personal models. In this mode, the system carries out an individual comparison to identify users. Thus, the relationship between biometric and electronic statistics enables the health organization to provide more reliable and efficient health services. It is unnecessary for biometrics have significant health care potential, facilitate reductions and improve the safety, quality and accessibility of information.

VI. USE OF BIOMETRICS IN THE HEALTH SECTOR

- Patient identification - In an emergency, when the patient does not have an ID and cannot communicate, biometrics may also be a reliable way to diagnose.
- Patient Identification and Tracking - Biometric technologies are largely used to track and identify patients. The biometric technology utilizes the recorded information about patients to verify and verify their identity before they can see physical access during medical design or access to information. Thanks to the ease of use and precision of biometric technology, more and more health care facilities are using this technology to reduce the risk of hacking and fraud. Furthermore, biometrics help physicians follow up on patients' medical records and, as a result, complementary therapies are provided.
- Medical Records Security and Data Protection - Given the increasing availability of EHRs (electronic health records) in medical settings, the security of data or confidential patient records on the networks is a major challenge. In this respect, biometric technology provides precise, efficient and effective solutions for health care providers and medical data centres. Biometric technology ensures that access is only available to authorised individuals, particularly in the case of sensitive specimens in data centres, advanced patients and other patent studies. In addition, this technology makes all identification processes more efficient, reduces the duplication of medical records and eliminates the possibility of medical fraud.
- Accreditation of care providers - The verification of health care providers who provide services and the monitoring of patients are as important as the Identification of patients who receive those services. The potential for problems like inappropriate treatment of patients and piracy of medical data is largely due to unauthorized access to fraudsters. To reduce these cases, biometric technology is widely accepted in medical institutions.
- Home / remote patient monitoring - Biometrics technology plays a key role in the provision of quality care to patients receiving remote monitoring services. The use of unique biometrics functions in remote care applications helps manage the resources and timeliness of remote care services. It provides simplicity in measuring weight, striking hard readings and signature distance. As well, it provides patients with timely and safe professional health care.
- Pharmacy delivery - The administration of medicines is one of the most widespread biometric methods. Given the high rate of medication-related errors, authorities in several countries have put in place policies and supported an event for hospital procedures that use automation and computers to eliminate those errors. In addition, the different physical systems of hospital information systems play a major role in guaranteeing patients the right drug and the right dose.

VII. CONCLUSION AND FUTURE WORK

We conclude that biometric authentication can play a significant role in maintaining the privacy of the health system. We can create an existing health security system and prevent unauthorised access to healthcare facilities. A separate biometric system can enhance the safety of the healthcare system. The survey will help students gain insight into current biometric physical and behavioural strategies and challenges. Health care diagnosis and validation require correction to either of these biometric authentication methods or a combination of different biometric techniques. It can be used to ensure advanced security and protect against any threat to the safety of patient records.

VIII. REFERENCES

[1] Fatima, K., Nawaz, S., & Mehrban, S. (2019). Biometric Authentication in Health Care Sector: A Survey. 2019 International Conference on Innovative Computing (ICIC). doi:10.1109/icic48496.2019.8966699

[2] Nanayakkara, S. I., & Ganegoda, G. U. (2018). Biometric Traits in Enhancing Security of Healthcare. 2018 3rd International Conference for Convergence in Technology (I2CT). doi:10.1109/i2ct.2018.8529442

[3] Yang, W., Wang, S., Hu, J., Zheng, G., Chaudhry, J., Adi, E., & Valli, C. (2018). Securing Mobile Healthcare Data: A Smart Card Based Cancelable Finger-Vein Bio-Cryptosystem. IEEE Access, 6, 36939–36947. doi:10.1109/access.2018.2844182

[4] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjel_n7sufwAhUw 8HMBHezGBJgQFjAMegQIFhAD&url=https%3A%2F%2Fw ww.aware.com%2Fblog-biometrics-in- healthcare%2F&usg=AOvVaw06wAoLRxbZR-dc7zmlLZw5

[5] https://www.healthcareitnews.com/news/biometrics-entering- new-era-healthcare

[6] https://www.idrnd.ai/biometrics-in-healthcare-the-right-place-the-right time/#:~:text=Biometrics%20including%20voice%20and%20face,clinics%2C%20offices%2C%20and%20hospitals.

[7] https://www.aware.com/blog-biometrics-in-healthcare/

[8] https://www.healthcareitnews.com/news/biometrics-entering-new-era-healthcare