International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 2, ISSN No. 2455-2143, Pages 318-327
Published Online June 2020 in IJEAST (http://www.ijeast.com)

DEEPBSA- SURVEY ON APPLICATION AND DEVELOPMENT OF BIOMETRIC SECURITY AUTHENTICATION

Kailash C
B.Sc IT data science
iNurture Educational Solutions, Bangalore

Shebana M
B.Sc IT data science
iNurture Educational Solutions, Bangalore

Mohammed Harun Babu R
Assistant Professor, Data Science & AI
iNurture Educational Solutions, Bangalore

***Abstract*-- As everyone knows, technology rules the universe now. There are a lot of components are used in this technology and one important system is Security. This paper aims to give a clear result about the technology used for the safety of people's information. The system called Bio metrics plays an important role in the sector of security. It consists of both psychological and behavioural recognition systems.**

The definitions, methods and drawbacks about such applications are explained in this paper. As coin has two sides, this Bio metric Science also has some negative qualities. In order to list that, this paper describes the advantages and disadvantages of Bio metric Authentication.

Keywords- Security, Bio metric Authentication, psychological and Behavioural recognitions.

I. INTRODUCTION

Medicine and Agriculture are the main back bones of the world. In medical field, there are a lot of new surgical technologies and injections and in case of Agriculture, there are so many tools are invented for the planting of crops. Not only these two sectors, but all business in the world was developed rapidly when compared to the development of last century. Asia would have the highest economy rate in 2019[1]. The literacy level and economic growth of the countries were growing drastically. Some countries which have the low development in few years ago have reached the well developed ratings in 21st century. Most of the people are started to explore the new innovations in the world and the awareness among the people are also raised highly. All this happened because of only the reason 'Technology Development' [2].

Either into deep oceans or air-free Space, Technology is ruling the universe. At the current stage, people can interpret the language of any creatures and can communicate with space organisms. The reason behind all these development was the technology of Computer Science and Networks. Technology has a lot of categories involved in it. They are Speed, Efficiency, Mobility, Storage, Automation and Security [4].

In these components, one of the main and important sectors is Security. This paper will clearly explains the Security systems invented in this growing technology.

II. BACKGROUND

Even though the efficiency and production level of the computer technology raised greatly, there was always some negative issues in that and that is 'In-security'. In the history of technology, people suffered a lot of problems related to Security [1]. The information about the institutions has been stolen by unauthorized access and their platform has been hacked by unknown persons. This causes a lot of loss in their business and it also become a threat in technology development.

Many scientist and web developers are tried to create a perfect Security system for the user. After a lot of researches and innovations, they come up with the idea called "Biometric Science" [2]. The term Biometrics has been derived from a Greek word which means bio-life and metric-To measure. It is the process of identifying the user with the help of their physical appearance and characters. This security system reaches the lot of responses from the user side because it was very user friendly, reliable and simple [5].

Usually, every human wants to keep their information safely and secured. This system is not only for an individual use, but also for the security of the big institutions to identify their employers [13]. This technology was mainly focused on the person's facial features, voice, body language, structure of the body to identify the real one. One surprising fact about this technology was it can even describe the individual characters of identical twins [10].

In the basis of bio-authentication, this system has been divided into two categories. They are psychological systems and behavioural systems. In these two divisions, there are a lot of subcategories. This paper claims to interpret all those systems with their functions. Figure 1 clearly lists some biometric systems which are used in the security sector [4].

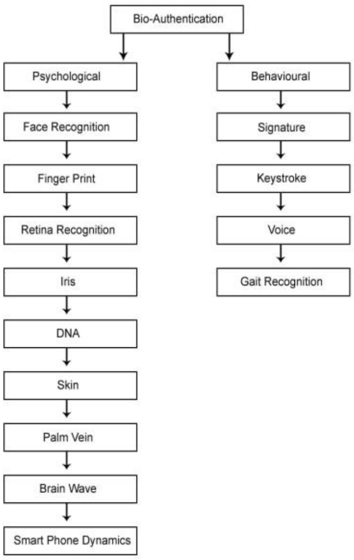

Fig. 1. DWT Decomposition model

III. METHODOLOGY

PSYCHOLOGICAL RECOGNITIONS:

Physiological biometrics technology measures the unique pattern of a user's automatic bodily functions for purposes of identification, authentication etc. Eye reactions, finger print ridges, heartbeat even body fragrance can be used as a factors of recognition [8]. Heartbeat and brain wave biometrics are the hot topics that have been discussed in this paper. They are used in consistent health maintenance and financial privacy. Physiological biometrics allows connected cars and work spaces which monitor the user's health continuously [9]. There are many systems involved in psychological sector and that has been listed in figure 1.

A. Finger Print Recognition

Basically a finger print is an impression of friction ridges in our part of finger skin. The ridges are raised on the palm, sole and digits or gaps between fingers. Finger prints differs in all human beings. Even from pre-historic periods, finger print stamps were used to identify a person and it acts more than a signature to human beings. Chinese parents who had more number of children used finger prints to identify their child. In 1788, German anatomist J.C.A Mayor stated that finger prints never duplicated in two persons, nevertheless the similarities are closer among some individuals. This greatly added to the uniqueness of finger prints [3].

Fig. 2. Image of Finger Print

Even though it was invented in late 1700's, the real time use of this system was introduces by Sir William Herschel in India to record the finger prints of Civil Service employees which was useful to identify them during paydays in the year 1858. This technology came up with new method called 'Minutae'. This term was proposed by 'Sir Francis Galton'. Later, the inspector general of police in Bengal, India 'Sir Edward Henry' used this method to identify criminals.This system reaches an important mail stone in the history of Security. That's why it has both traditional and modern methods. In traditional methods the finger print is taken on a paper and is scanned by a machine to load information or extract details about the person. New methods involve immediate scanning of finger prints over a silicon panel and laser to scan the parts of fingers placed on the panel. Finger prints have two important features such as 'immutability' refers to unchangeable behavior in course of period and 'uniqueness' refers to the ability to be distinguished [13].

The finger print recognition system has been used in three ways and they are Minutae based, Correlation based and Pattern based. This refers to Identification of Minutae points along with their relative position on finger, Useful in low quality gray scale data detection and the comparison of two finger prints respectively. In spite of being all these possible qualities, this system has some negative issues. The drawback is that, the finger moisture determines the sensor's bitmap reading. So people with too dry or wet hands won't provide sufficient information. Cuts, scars on the finger are obstacles for this method. Using wax technology this method could be easily cheated. Moreover this method needs more time to compute and is easily worn out. So, the biometric system has been developed more to introduce new technology [9].

B. Face Recognition

Face recognition is the dynamic and emerging method that is nearly used everywhere by common people even at their households. From a simple smart phone to a big door uses this technology to identify the person and provide access to whatever the system is protecting. The size of the face, location of eyes and other physiological attributes such as lips, nose are taken into account and registered as the characteristics of a human. Either digital image of the person or the video of them is required to precede facial recognition [14].

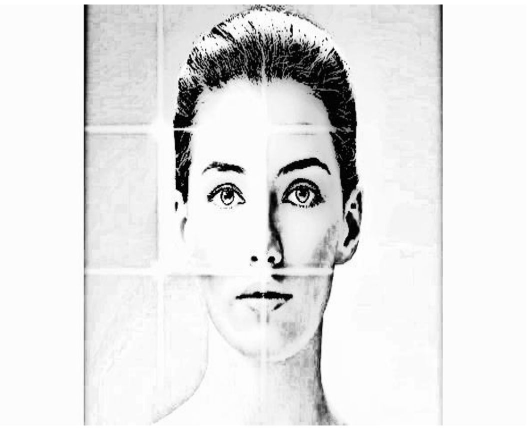

Fig. 3. Image of Face

There are three important methods are used in the process of Face recognition. They are Facial metric which deals with location and space between facial attributes are taken and processed, Eigen metric refers to the overall face image is scanned and processed and then Skin texture analysis which deals with Unique spots such as moles, wrinkles and patterns are verified. The face region is covered by a pre-defined size of 150-100 points known as canonical images. Normally the size required to store a face data is 3 to 5kB. Eigen face is a method of arranging the details into 100 – 150 set of Eigen images. These images are arranged in specific pattern to identify the location of hair, eyes and other facial traits. About 40 images, Eigen pictures show 100 percent high degree accuracy when others give 99 percent or less [8]. The main drawback of this method is only that it can be easily faked with a picture or video. The accuracy of face recognition system tends to be increasing day by day but still it has no solid idea. People who change their beard style often seem to face problem with these because the system cannot recognize him as the same person. In case of twins distinctiveness is not guaranteed all the time. Privacy abuse is a greater threat and very bright light, facial gestures make the sensors unable to read.

C. Retina Recognition

This method is based on the person's retinal patterns of the eye. Retina is the thin tissue that is made up of neural cells and is present in the innermost part of the eye. Retinal patterns are exquisitely unique, even identical twins won't have the same pattern. The identification of unique patterns of blood vessel at the rear of the eye which covers 65% of inner part of the eye was the algorithm used behind this technology [15].

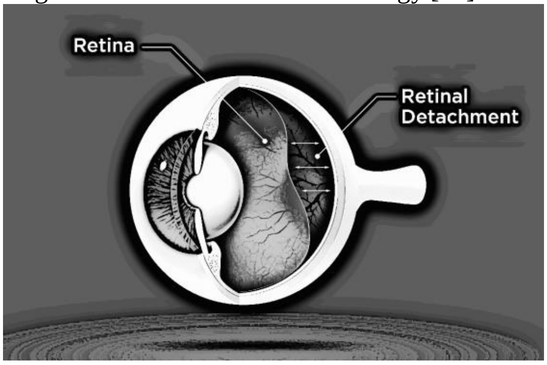

Fig. 4. Image of Retina

In spite of scanning the eye part, this system is differs from Iris recognition. It requires low intensity infrared lights to see the retinal patterns of blood vessels. Their patterns are recorded and transferred to the database in the form of digital codes. It usually requires 40-96 bytes of memory to store the information.This technology gets a huge response from public. But, some physically challenged people cannot be able to get into this system. Users who are victims to diabetes, glaucoma, cataracts find this method not very friendly. Enrolment and scanning processes are slow. Equipment cost is high and subject's patience for the scanning to take place is important. The drawback in this method is that it is not that much user friendly. It requires at least 15 seconds of stillness on the user's side or else it will tend to deny access [4].

D. Iris Recognition

Iris is the colored area that surrounds pupil. Iris allows the light entry to our eye and it is constant throughout life with unique patterns that are obtained through video based image acquisition. Even left and right eyes have different patterns. This pattern is due to filaments, corona, freckles, pits present on the iris. Faking a person's complete iris is impossible. Even after the person's demise, the iris decays fast so there is no possible way of cheating this method unless directly using the eye when it is still functioning [13].

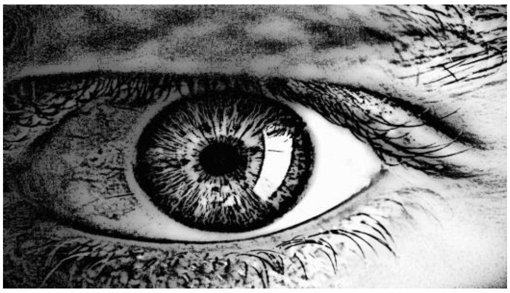

Fig. 5. Image of Iris

A special gray camera is used to scan iris pattern from a distance of 10-40 cm. A high end designed software checks for an iris in the image and determines lines over which the patterns could be sought out. As size of iris differs based on size of the eye, a special contractor device makes sure that the iris is fully captured. The captured lines of iris are converted to digital iris code and stored for recognition purposes. This method is the best for individual identification systems.

Still there are a lot of positive features, there are some medical issues like diabetes and much severe ones can cause changes in the iris. Just like retina scan far distance, bright illumination can cause the malfunction of the sensors. The scanning is obscured by long eyelashes, contact lenses and reflections. These devices are relatively expensive and are prone to cheating by very high quality images [1].

E. Palm Vein Recognition

The vein recognition system is one of the recent biometric systems. It focuses on the veins on user's hand. Veins are blood vessels which carry blood to the body, unique pattern of these nerves are seen in every individual. Like the finger prints both left and right have different nervous structures. It is much preferred by biological researchers and it is highly secure. This process is very admirable and user-friendly [12].

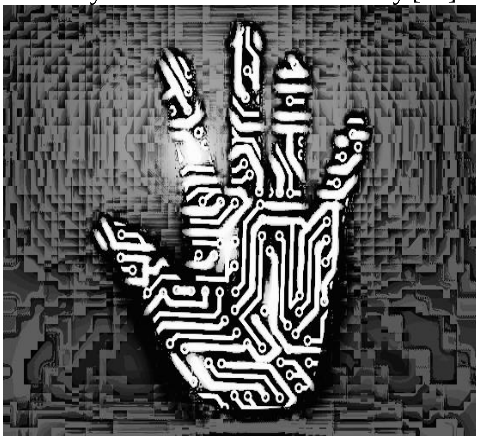

Fig. 6. Image of Palm Vein

Veins of the each finger are directly connected to the brain of the human body. British Technology Group's Vein check system is the first hand vein detection system. Infrared lights or near infrared lights using high resolution cameras are used to get the pattern of veins. It requires 50 bytes space for storage of the digitized patterns. In the system using pattern matching method identification is done. The infrared lights scan for the blood hemoglobin in the hands which is greatly helpful in medical research.

This system was more preferable by public. That's why it has a less number of drawbacks. The issues which threatening the usage of Palm vein Recognition system was it is quite unfamiliar for the users because entire hand needs to be placed over the instrument for detection and the quality of the image is affected by body temperature and defects in IR lights[17].

F. DNA Bio Recognition

DNA is genetic material that is responsible for the hereditary traits that humans assume. Basically it a polymer made up of Adenine, Guanine, Cytosine, and Thymine. Using modern technology, DNA identification is now done within 10 minutes. This method is not widely used by commoners but used by secret government agencies in crime detection forensics. This technique also provides high accuracy [2].

Fig. 7. Image of DNA

The chance of having same DNA is less than in a 100 billion. DNA sequencing or genetic profiling is the data that is collected from an individual, CODIS is the database used for identification of the person. This method is different from others because a concrete physical sample is needed for processing. A device known as Ion-Selective Field-Effect Transistor (ISFET) is used to detect the features of DNA molecules in recent tests.

For the DNA pattern identification, one most important terminology is used and that is 'DNA Sequencing'. There are four methods involved in this process.

a. Separation of DNA samples from blood, saliva, hair, semen and tissue etc.

b. Separating DNA samples into smaller segments or fragments (identically repeated sequences)

c. Organization of segments/ fragments of DNA by size.

d. Comparison of segments/fragments of DNA from different samples.

This technology reaches the top most level in the security sector of the technology. But, there are some circumstances in this system. So, they come up with the new idea. The issues raised in this technology are sample acquisition time is very long. Privacy issues, storage space, high cost are the main let downs of this method. Instant matching of samples is not possible. The result is affected when the sample is contaminated or degraded [3].

G. Skin Recognition

Skin is the layer that provides protection to internal organs of the human body. It is mixture of layers which has different optical and morphological properties. Skin's two layers are internal layer dermis and external layer epidermis. Skin has two properties, light and electrical namely using these authentications is done [16].

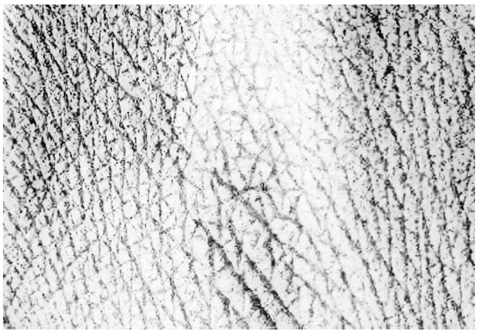

Fig. 8. Image of Skin

Based on the size and thickness of the skin cells this method can be moved on. Every person has a different composition of these cells. Using ultrasonic spectrum imaging, the hands or fore arms of people are done their images are seen to check the composition of dermal and subcutaneous regions. Also lights at different wavelength are sent into human skin through various LEDs and the scattered lights are read by photodiodes.

There are two distinct reflections from the skin. They are Seculars or interface reflection component which occurs at surface, in only one direction and Diffuse or body reflection component that can be returned by some of the incident lights after scattered by internal organs. These lights contain information about the individual's skin color, unique 'spectral signature' [13].

H. Brain Wave Recognition

The recent emerging research and promising area of bio metrics identification of human's brain wave. It is also known as cognitive biometrics. Each human's brainwave is different and features are unique. Using these properties a Brainwave Electroencephalogram (EEG) can be used to measure brainwave activity. The main advantages of this method are difficulty in eavesdropping on personal brain data; brainwaves express an individual's activities [18].

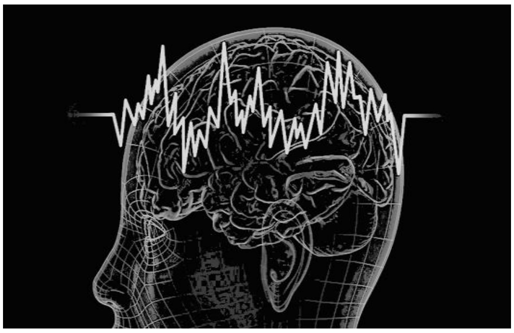

Fig. 9. Image of Skin

In this technology, there are three main approaches are proposed. They are Alpha and gamma rays based brainwaves research, Motor imagery or working activity of brain and Near Infra Red spectroscopy (NIRS). It was the more surprising technology in this world that can be also applied in blue brain technologies.

These eight Bio metrics applications are the most useful technologies in the current situation. This application can also deals with behavior of the humans. Those Bio authentication technologies are called Behavioral Bio-metric Authentication [2].

BEHAVIOURAL RECOGNITIONS:

Behavioral biometrics is a technology that identifies users based on patterns in their behavior. It authenticates unique, individual regularities in the ways that people work on their keyboard, how they walk and etc. Behavioral authentication checks continuously, evaluating the user's ongoing interaction with their mobile device or computer in real time. Behavioral biometrics identifies patterns in the ways that particular bodies perform particular tasks like walking, speaking, typing, or even touching the screen and mouse behavior. These patterns are difficult to replicate and they change in course of time [6].

For example, Biometric data from smart phone, wearable accessories, smart speakers. Voice and speech recognition, lip and eye motion tracking, gait, hap tic and touch. In 2018, the profit of this technology is 871 dollars and it will be expected to reach the level of 2.5 billion in 2023[7].

A. Smart phone dynamics Recognition

The main idea of this technology is based on two aspects. They are method to use the device and how the device responds to the user. While using mobile devices, most people may follow certain individual habits unconsciously. Running as a background service, the software exploits the user's app usage and interacting behavior with each app, and uses the motion sensors to measure the device's reaction [19].

Fig. 10. Image of Smart phones

Correlating the user action and its corresponding device reaction, then establishing a unique biometric model to identify the role of current user is the main task done in this method. Tiny perturbation of the whole device will be captured by motion sensors when a user touches the screen. The amplitude of such tiny perturbation depends on the user's holding gesture, the touching pressure and co-ordinate.

To establish the user behavior model, for the owner there are abundant behavior information. For a guest, the collected behavior information may be very limited. In addition, in motion scenarios, some interacting features will be dumped by the motion from the perspective of sensory data, which greatly increases the difficulty of accurate authentication. The framework model consists of two basic phases: Training and Identification [22].

The training phase is conducted to build a behavior model when the user is interacting with the device, and the identification phase is implemented to distinguish the identity of the current user based on the observations of each individual's interacting behaviors. When a guest user is observed, privacy protection mechanism will be triggered automatically. After the guest leaves and the owner returns, privacy protection will be reset for the owner's convenience. The pictures of the pretender or unauthorized user may be shown to the original owner. With users accessing smart phones constantly, there is a need to offer a continuous authentication mechanism in order to reduce the frequency of entering PINs or drawing patterns. Continuous authentication can be based on two of behavioral biometrics: app usage and touch based. With wide spread use of apps (the number of mobile app downloads expected to reach tremendously.

B. Signature Recognition

Signature biometrics is a behavioral biometric and uses the pattern of signature to identify the individual. The individual's way of signing his or her name is the distinct feature of that individual. More emphasis is on the behavioral pattern of how the signature is signed rather than the appearance of the signature. It is operated in two ways – Static and Dynamic signature recognition [20].

Fig. 11. Image of Signature

In the static or off-line method, the signature is put in the paper and it can be digitized through camera or an optical scanner. The signature is recognized by the system with the help features of signature such as velocity, speed and pressure. In the dynamic or on-line method, the signature is acquired through digitized tablet in real time i.e., capturing behavioral traits such as speed, pressure, direction of stroke, size of signature and time duration.

The behavioral patterns for signature verification includes the pen's angle, pauses, the time duration, the speed, the pressure and direction of strokes while signing. The graphical appearance of the signature can be easily duplicated but imitation of the signature with same behavioral traits of the person while signing is very difficult. The size of signature should be small enough as well as big enough to fit on the tablet for acquiring adequate data, quality of the tablet for generating template during enrollment and the verification must be done in the similar environmental backgrounds as that captured during the enrollment time[25].

Professionals can easily deceive the system by forging the hand writing. If the user has inconsistent signature or constantly changing signature patterns, this method will be difficult to handle. If a sudden change in behavior while signing like unusually less stress different angling, the system will be unable to proceed for further processing.

C. Key stroke Recognition

At World War II, Military Intelligence used a technique called "Fist of the Sender", that uses the rhythm of typing to check whether the Morse code was sent by ally or enemy. The rhythms with which one types at a keyboard are sufficient to form the basis of the biometric technology known as keystroke dynamics. A keystroke is behavioral biometric technique and it offers sufficient differentiable information when each individual type on a keyboard in a characteristic way. The person's typing pattern, the rhythm, and the speed of typing on a keyboard are analyzed by this biometric [11].

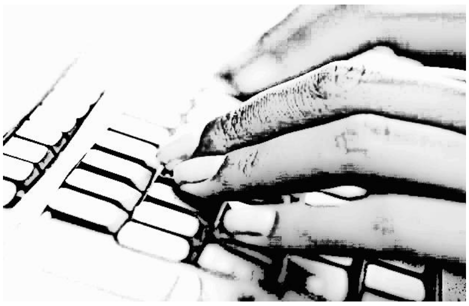

Fig. 12. Image of Keyboard

The typing dynamics may not be interesting to many of the researchers for identification. But the studies have revealed that the two factors, namely, dwell time, the duration of time for which a key is pressed and flight time, the elapsed time between releasing a key and pressing the following key or inter-character timing can give 99% accurate identification of the person who is typing.

The time taken to find the right key, the flight time and the dwelling time are differentiating the individual in the way they type on the keyboard. Also there is variation in the speed and rhythm of typing. The keystroke recognition can be classified into two types. They are Static which refers to one-time recognition at the beginning of interaction and Continuous which refers to recognition throughout the course of interaction [21].

The main drawback of this system is Diseases, time gaps, tiredness usually lead to retarded keystroke movements. This is a major demerit faced by this method as the system only recognizes a user at full energy or potential. Although taken for unique characteristic this method does not provide much discriminating data.

D. Voice Recognition

The voice recognition biometrics is most promising research zone [8]. Voice biometrics also known as speaker recognition biometrics. They are used for the applications based on telephone. Almost, human voice features are distinct for every individual as well as for twins also and voice could be replicated perfectly. For every individual, unique voice patterns are produced by the combination of physical and behavioral factors. The vocal tract, lips, nasal cavity and shape and size of mouth are the physical characteristics and the pronunciation, emphasis, speed of speech, accents are the behavioral characteristics [7].

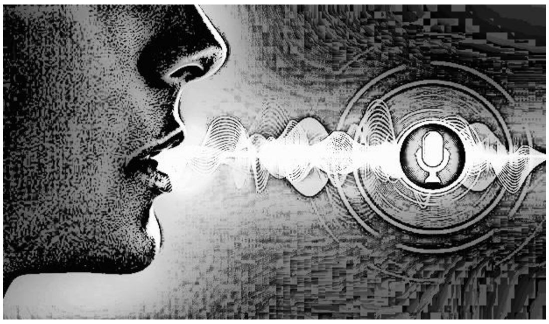

Fig. 13. Image of Voice variation

The voice recognition relies on how the person speaks and the focus is on the speech produced by the vocal features not on the pronunciation or the sound. The acoustic pattern traits of the speech are used by voice recognition to differentiate the individuals and these patterns consists of both behavioral patterns (speaking style, voice pitch) and physical (shape and size of the throat and mouth) .The vocal tract is not affected even by cold and so there will be no adverse impact on the accuracy[9].

During enrollment time, the individual is asked to repeat the short phrases to prevent the unauthorized access. Audio devices such as microphones, telephones and PC microphones can be used to capture the voice. Using Analog to Digital ADC converter, the generated electrical signal from the microphone is transformed into digital signal and recorded as digitized sample. The matching algorithm or system compares the input voice and stored digitized voice for identification.

There are several types of voice recognition systems. They are Speaker dependent and Speaker independent is the two types of voice recognition. Speaker dependent system depends on the knowledge of individual's particular voice traits. The system has to be learned and trained those traits through voice training, in particular accent and tone. Speaker independent voice recognition can able to recognize the speech such as words and phrases from various users with the restriction in the context of the speech [25].

No need to train the system. Text dependent, Text prompted and Text independent are the three styles of spoken input employed by the voice system. It is very hard to design the speaker dependent voice recognition. The various factors such as ambient noise, variation of speaker as well as in the tone of the same speaker, sensitiveness of phonetic input systems, distance and regular variations are used to analyze the performance of speech recognition system.

The voice recognition systems are used in healthcare, government offices, banking, entertainment applications, PIN smart cards, access control, customer authentication and other security purposes. Due to age factor, the change in voice needs to be addressed by the system. There is a significant difference between Speaker recognition and Speech recognition. The voice or speaker recognition which recognizes the person WHO is speaking and used to identify an individual by tone, accent and voice pitch [22].

The Speech Recognition - assess WHAT spoken and used in menu or map navigation and hand free computing. Even though, it possess a lot of drawbacks such as the performance is dependent on the microphone used. External noise, serious illness, problems in throat affects accuracy of the system. Easily cheated as technology has improved and has high rate of mismatch and error.

E. Gait Recognition

Gait Biometric recognition is an individual's walking style. The Gait can be described as the human locomotion causing coordinated and cyclic sequence of movements. It is almost latest technique comparing to the conventional approaches such as fingerprint, face etc. and has 90% accuracy. Commonly, a person is identified by recognizing their walking style such as posture of body, swinging hands and walking distance between the two feet. Gait biometrics has several attractive characteristics [23].

Fig. 14. Image of Leg Posture

Capturing of individual's gait can be done very easily without their co-operation or even awareness. Some research is going on visually-based systems to analyze the each part of body's movements using video cameras. The individual's gait is frequent events with each gait cycle called strides and it has two stages – one foot in the ground (Stance Phase) and the other foot not in the ground (Swing Phase).

The shape and dynamics are the two aspects for the gait biometrics. The configuration or different gait phases performed by the shape of the individuals is referred as the shape and the rate of change of one phase to another phase is referred as the dynamics. Both shape and human motion research has to be synthesized in the research for the growth of gait biometrics.

Gait biometrics can be classified into behavioral and physical biometrics. The human walk is the behavioral biometric and anatomy of the feet and body's weight is physical biometrics. The individual's gait is unique to some extent only. With the help of a camera video image is captured and recorded. Then, by using appropriate segmentation and motion detection methods, the walking persons are detected and segmented from the background and then gait features are extracted by creating a mathematical model [13].

The identification can be done by comparing the similarity measures between extracted gait features and the stored features in gait database. The important step in gait recognition is to extract discriminative feature. First of all it is not a reliable technique. It lacks accuracy and as the equipment required to compute the movements is high this is an expensive method.

IV. ADVANTAGES AND DISADVANTAGES OF BIO METRICS

A. Benifits

Biometrics has been a key to removing the inconvenience and risks of physical forms of authentication such as drivers' licenses, passports, ID books etc, especially for customer on boarding, access control, border control and policing [22].
The main advantages are:

1. Contact centers where voice biometrics is extremely effective in displacing security questions that makes uneasiness for users and agents, and weakened due to the easy availability of the biographic information upon which these questions are based, due to large scale data breaches, phishing.
2. Notebooks and PCs possess mobile computers are now equipped with cameras and fingerprint sensors, and PC's, especially those in government departments, are hooked up with external fingerprint sensors that are used for login and various workflow authorizations[24].
3. Mobile Devices are including by sophisticated fingerprint sensors and high-resolution front cameras on most modern smart phones, manufacturers have removed the cost barrier to biometrics. This has resulted in increased user familiarity with biometrics, and a major step in adoption and user adoption for

phone unlocking, mobile-app login and even transactions authorizations.

As organizations take the 'digitize or die' route to growth, Biometrics will remain to be a topic of interest for the time being and forward [25].

B. Threats

In comparison to the inconvenience, declining reliability and increasing cost of biometrics appeared to be the savior; especially for organizations wanting to digitally transform with urgency. Influenced by science fiction and clever marketing, many implementations deployed biometrics as an only way of authentication method. Not only did this meet internal resistance but attracted wide ranging criticism from a variety of criticizers who were able to find cause in a number of biometric limitations [22].

Some disadvantages are as follows:

1. Environment which has different biometric methods is not suited to certain environments. For example, voice doesn't work well in noisy areas, facial struggles with in poor lighting, fingerprint readers are remarkably affected by dirt and dust.
2. Twins and Impersonators(cheaters)which is a problem across all biometrics, in very much the same way that humans could be duped by twins and impersonators who can use voice, facial and other disguises[24].
3. Synthesis and Spoofing where the fight between the scientists, vendors and security professionals, and hackers, fraudsters and mischief makers is inevitable.
4. Privacy and Irrevocability where some biometrics, such as facial and to a certain extent voice, can be used to recognize an individual. Consumers who choose to be anonymous or pseudonymous are uncomfortable with providing biometrics that can be linked back to them. Also, unlike PINs and Passwords, which can be changed, biometrics is more permanent in nature. This is an interesting consequence as it is this very permanence makes it suitable for authentication [25].

V. Conclusion

Biometrics is a great way of authenticating users. The user is authenticated by a workstation during the logon, by a smartcard to unlock the private key, by a voice verification system to confirm a bank transaction or by a physical access control system to open a door. Very promising are solutions where the cryptographic functions as well as the biometric matching, the feature extraction and the biometric sensor are all integrated in one device [13].

This system helps the people to secure their information and give guarantee for their belongings. Finally, this paper fetches some important characteristics of Bio metrics [5].

They are:

1. Different biometric samples of the same person will never be same [2].
2. Biometric systems make errors.
3. Biometric data are not secret.
4. The role of the input device is crucial, and this device must be trusted or well secured.
5. The biometric system should check user's liveliness.
6. Biometrics is good for user authentication. The methods cannot be used to authenticate data or computers.

VI. References

[1] Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. International Journal of u-and e-Service, Science and Technology, 2(3), 13-28.

[2] Sabhanayagam, T., Venkatesan, V. P., & Senthamaraikannan, K. (2018). A comprehensive survey on various biometric systems. International Journal of Applied Engineering Research, 13(5), 2276-2297.

[3] Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. Symmetry, 11(2), 141.

[4] Nixon, M. S., Correia, P. L., Nasrollahi, K., Moeslund, T. B., Hadid, A., & Tistarelli, M. (2015). On soft biometrics. Pattern Recognition Letters, 68, 218-230.

[5] Nixon, K. A., Rowe, R. K., Allen, J., Corcoran, S., Fang, L., Gabel, D., ... & Ostrom, B. (2004, August). Novel spectroscopy-based technology for biometric and liveness verification. In Biometric Technology for Human Identification (Vol. 5404, pp. 287-295). International Society for Optics and Photonics.

[6] Bo, C., Zhang, L., Jung, T., Han, J., Li, X. Y., & Wang, Y. (2014, December). Continuous user identification via touch and movement behavioral biometrics. In 2014 IEEE 33rd International Performance Computing and Communications Conference (IPCCC) (pp. 1-8). IEEE.

[7] Khan, B., Khan, M. K., & Alghathbar, K. S. (2010). Biometrics and identity management for homeland security applications in Saudi Arabia. African Journal of Business Management, 4(15), 3296.

[8] Matyáš, V., & Říha, Z. (2002). Biometric authentication—security and usability. In Advanced Communications and Multimedia Security (pp. 227-239). Springer, Boston, MA.

[9] Sahoo, S. K., Choubisa, T., & Prasanna, S. M. (2012). Multimodal biometric person authentication: A review. IETE Technical Review, 29(1), 54-75.

[10] Karnan, M., Akila, M., & Krishnaraj, N. (2011). Biometric personal authentication using keystroke dynamics: A review. Applied soft computing, 11(2), 1565-1573.

[11] Shah, G., Shirke, S., Sawant, S., & Dandawate, Y. H. (2015). Palm vein pattern-based biometric recognition system. International Journal of Computer Applications in Technology, 51(2), 105-111.

[12] Dharavath, K., Talukdar, F. A., & Laskar, R. H. (2013, December). Study on biometric authentication systems, challenges and future trends: A review. In 2013 IEEE International Conference on Computational Intelligence and Computing Research (pp. 1-7). IEEE.

[13] Chang KI, Bowyer KW, Flynn PJ. An evaluation of multimodal 2D+ 3D face biometrics. IEEE transactions on pattern analysis and machine intelligence. 2005 Mar 7;27(4):619-24.

[14] Beenau, B. W., Bonalle, D. S., Fields, S. W., Gray, W. J., Larkin, C., Montgomery, J. L., & Saunders, P. D. (2006). U.S. Patent No. 7,121,471. Washington, DC: U.S. Patent and Trademark Office.

[15] Miller, P. E., Rawls, A. W., Pundlik, S. J., & Woodard, D. L. (2010, March). Personal identification using periocular skin texture. In Proceedings of the 2010 ACM Symposium on Applied Computing (pp. 1496-1500).

[16] Zhou, Y., & Kumar, A. (2011). Human identification using palm-vein images. IEEE transactions on information forensics and security, 6(4), 1259-1274.

[17] Thomas, K. P., & Vinod, A. P. (2017). Toward eeg-based biometric systems: The great potential of brain-wave-based biometrics. IEEE Systems, Man, and Cybernetics Magazine, 3(4), 6-15.

[18] Juefei-Xu, F., Bhagavatula, C., Jaech, A., Prasad, U., & Savvides, M. (2012, September). Gait-id on the move: Pace independent human identification using cell phone accelerometer dynamics. In 2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS) (pp. 8-15). IEEE.

[19] Maiorana, E., Campisi, P., Fierrez, J., Ortega-Garcia, J., & Neri, A. (2010). Cancelable templates for sequence-based biometrics with application to on-line signature recognition. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 40(3), 525-538.

[20] Saevanee, H., & Bhattarakosol, P. (2009, January). Authenticating user using keystroke dynamics and finger pressure. In 2009 6th IEEE Consumer Communications and Networking Conference (pp. 1-2). IEEE.

[21] Jain, A. K., Flynn, P., & Ross, A. A. (Eds.). (2007). Handbook of biometrics. Springer Science & Business Media.

[22] Wang, L., Ning, H., Tan, T., & Hu, W. (2004). Fusion of static and dynamic body biometrics for gait recognition. IEEE Transactions on circuits and systems for video technology, 14(2), 149-158.

[23] Fan, C. I., & Lin, Y. H. (2009). Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics. IEEE Transactions on Information Forensics and Security, 4(4), 933-945.

[24] Bhatia, R. (2013). Biometrics and face recognition techniques. International Journal of Advanced Research in computer Science and Software Engineering. 3(5).