IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

Comparative Study on Various Biometric Methods Available for Secured Cloud Authentication

G. Kishore Kumar[1], Dr. M. Gobi[2]

Research Scholar, Department of Computer Science, Chikkanna Government Arts College, Tirupur, TN, India[1]

Assistant Professor, Department of Computer Science, Chikkanna Government Arts College, Tirupur, TN, India[2]

Abstract: Cloud Computing is a fast-growing area and its security issues block the prevalence widely in various areas; wherein the data protection is one of the critical/important among these. Guaranteed data protection is required to have data transfer from organizations to cloud for ensuring security in various aspects. Security is the primary concern in all areas of applications wherein still many challenges are there, even after proposing/recommending many techniques. Biometric is a most prevalent technique, which can be used in addressing these security issues. This paper enlightens about various biometric authentication methods available for cloud security, in which our research would be focusing on, by using any of the cryptographic methodologies.

Keywords: Cloud Security, Authentication, Biometrics, Identification, Verification.

I. INTRODUCTION

A. Cloud Computing

Cloud Computing denotes to the usage of a network, which contains remote servers that are hosted on the internet. This will be used for various purposes such as processing, managing & storing data. This is an example of internet based computing, which provides shared resources and data to other devices required on demand. It is a pattern for enabling a shared pool of configurable computing resources as on when requested and global access such as computer networks, servers, storage, applications and services.

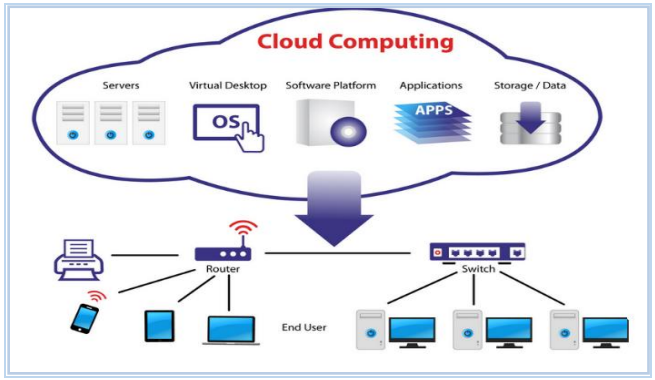

Fig. 1 Cloud Computing Overview

Cloud characteristics are given below:

- On-Demand self-service
- Ubiquitous network access
- Location-independent resource pooling
- Rapid elasticity
- Measured service

Cloud delivery models are given below:

- Application/Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

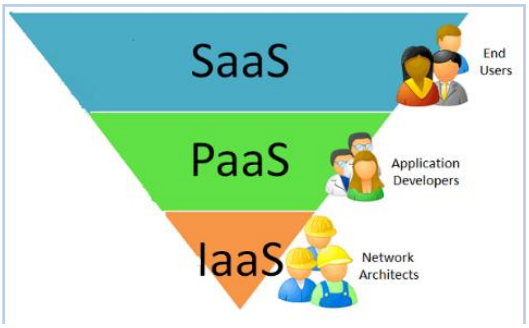

Fig. 2 Cloud Delivery Models

Cloud deployment models are as given below:

- Private
- Public
- Community
- Hybrid
- Virtual Private Cloud[3] - A virtual private cloud (VPC) will reside or within a public cloud environment which contains set of configurable group of computing resources on demand and allocated within a public cloud environment. They will provide a certain level of isolation between the different organizations, which are nothing but users.

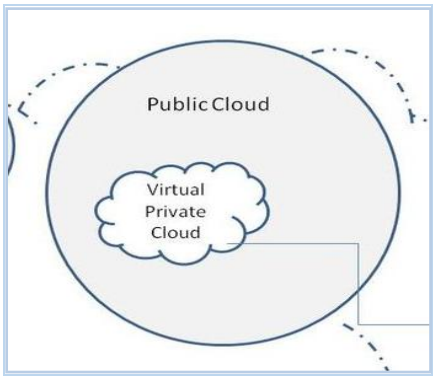

Fig. 3 Virtual Private Cloud

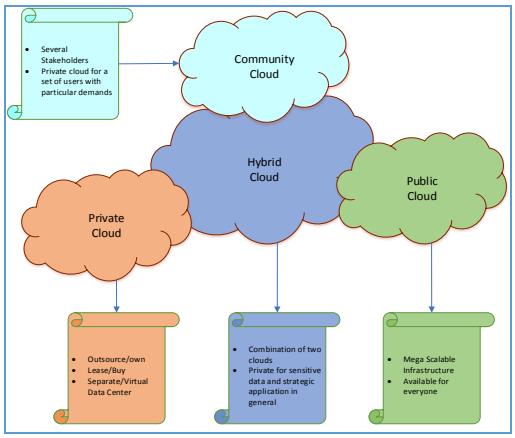

Fig. 4 Cloud Deployment Models & Properties

B. Cloud Computing Security[4]

In general, security is extremely tough to define. The objectives of information security are Integrity, Confidentiality, and Availability. Wide set of policies, controls and technologies are installed in Cloud Computing to protect data, applications and its infrastructure, which is a sub-domain of computer security, network security, and information security as well.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

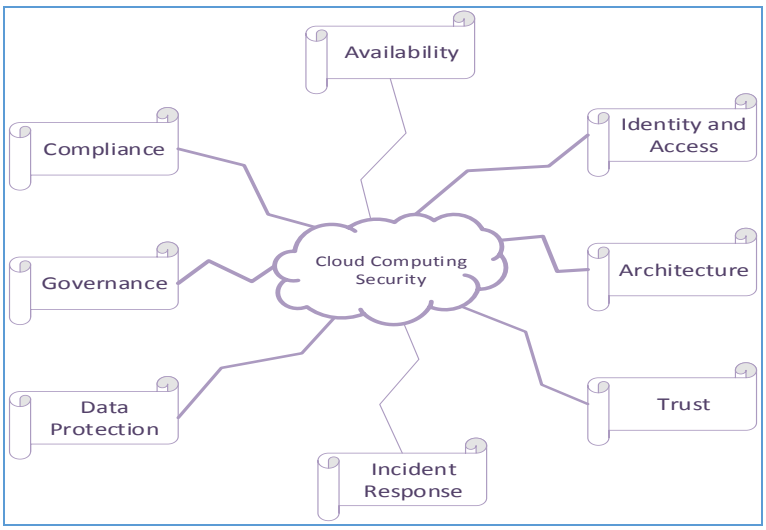

Fig. 5 Cloud Computing Security

The below diagram illustrates about various parameters that affect cloud security:

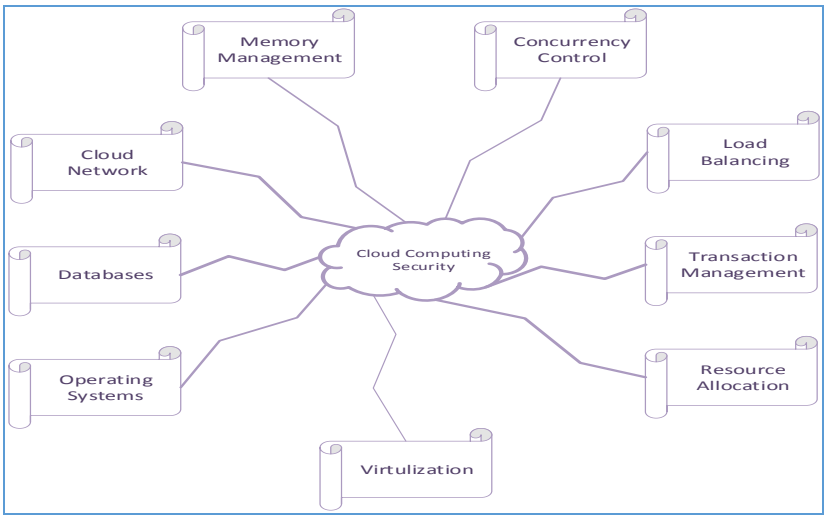

Fig. 6 Parameters that affect Cloud Security

II. BENEFITS OF ENCRYPTION IN CLOUD ENVIRONMENTS[4]

The below given are the few benefits of encryption in the cloud environment, which would help to

- Ensure privacy of the organization data, where in the data will be encrypted such as transmission, in use and storage as well.
- Achieve Secure Multi-Tenancy in Cloud. Encrypting data in the cloud and keeping the encryption key by which data owner can block in accessing the data by cloud service provider.
- Provide a Safe Harbor from Breach Notification, if a data breach occurs and personally, identifiable information is lost, the breached party must notify all individuals who are impacted.
- Confidence on safety of data backups in cloud environment to be provided from the breached party.
- Expand revenue potential to customers with sensitive or regulated data by maintaining the key by cloud data owner and gives cloud service providers a competitive edge.

III. BIOMERTICS

A. Introduction

Biometric means, bio indicates life and metric indicates measure and this is derived from the Greek words. It can be defined as "life - measure" as well. Biometrics are useful in identifying a person's physical and behavior characteristics.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

It is used in security and access control applications to access measurable physical characteristics of a person that will be checked on an automated base. This identification method is chosen above traditional methods, which includes PIN numbers and passwords for its accuracy and case sensitiveness.

This can be used as either identification or authentication system based on the requirement/design, which will be further divided into various types such as fingerprint, DNA, IRIS etc. Biometric data are isolated and distinct from personal information. Biometrics helps in recognizing a person based on a behavioral or physiological characteristic, which are automated methods. There are various unique identifiers are available in biometrics such as Fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, Signatures etc.

B. Biometric Authentication

Biometric authentication is a security process that depends on the distinct biological characteristics of an individual for verification. This is used to manage access for physical and digital media resources like buildings, server rooms, computing devices etc. The authentication is used in identity verification process, which contains biological input or scanning or analysis from some body parts.

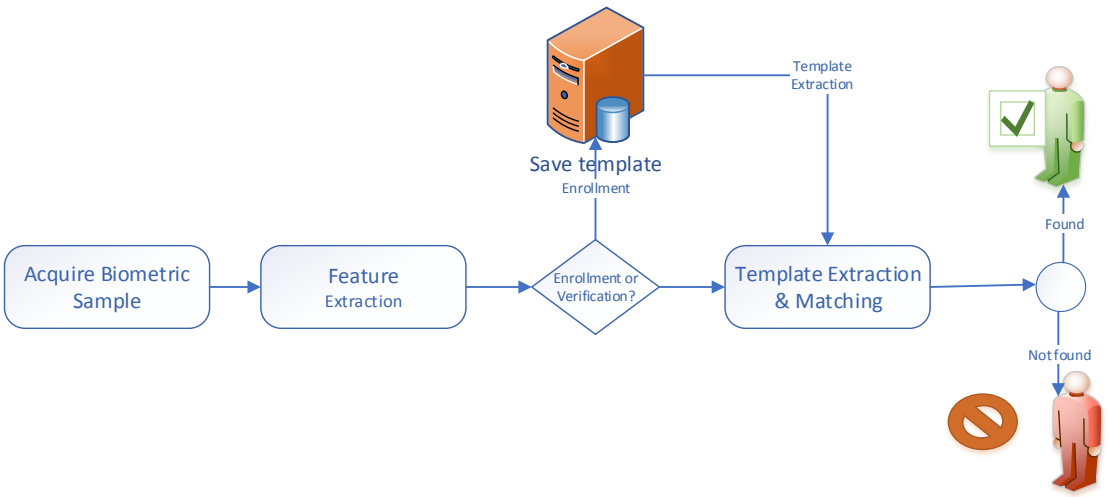

Fig. 7 Block diagram of Biometric Authentication

IV. TYPES OF BIOMETRICS

Based on the requirement/design, the biometrics system can be used either as an identification or authentication system. These are further divided into various types as follows, Face recognition, Fingerprint identification, Hand geometry, biometrics, Vein, eye, Retina scan, Iris scan, Signature, Facial thermograms, Tooth, Ear, DNA, GAIT, Footprint, Mouse dynamics, Hair, Keystroke dynamics, nose, Voice analysis, Palm print[8], Odour/Scent[8]
The Biometrics is divided into two broader categories:

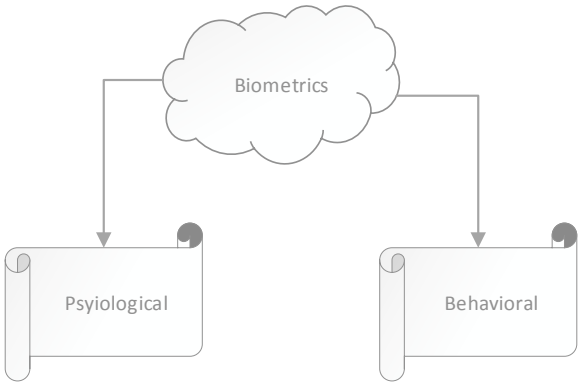

Fig. 8 Types of Biometrics

Physiological types are shown as below:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

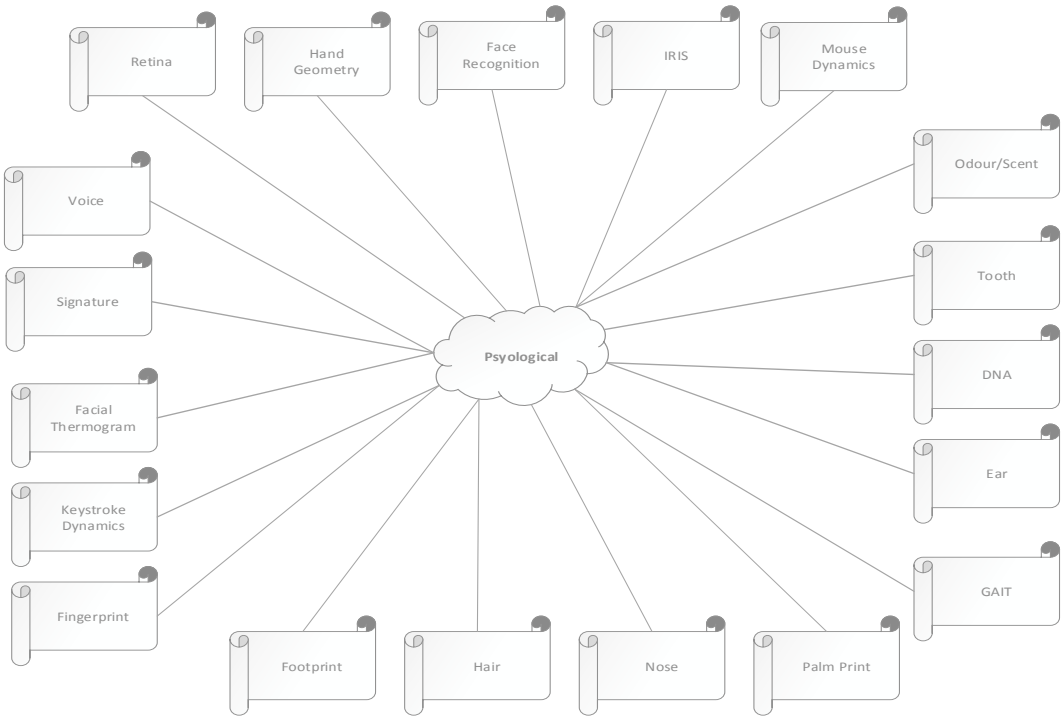

Fig. 9 Physiological Biometrics

Behavioral types are shown as below:

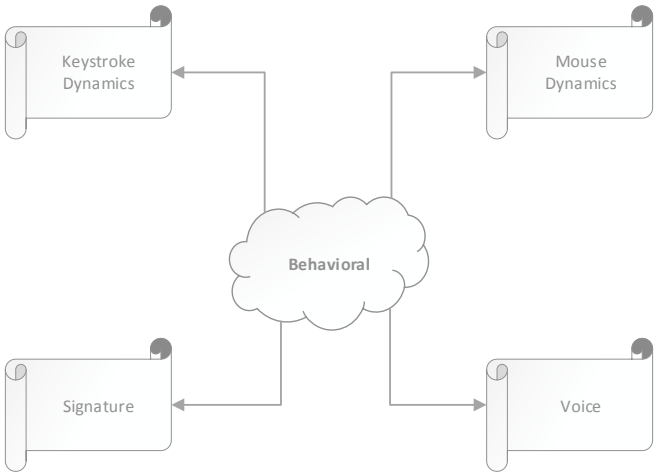

Fig. 10 Behavioral Biometrics

V. BIOMETRICS AUTHENTICATION METHODS[7]

The below section explains various biometric identification methods available with the block diagrams:

A. Face Recognition

Among the various biometric identification methods, face recognition is one of the most flexible method wherein it will be working even when the subject will be unaware of being scanned. This process requires just few seconds only wherein people spend very less time, like in front of the camera/scanner. The Face Recognition systems working principle is to analyze common features/nodal points like distance between eyes, position of cheekbones, jawline, width of the nose, chin and so on. These numerical measures are combined into a single entity, which will identify the person uniquely.

The following diagrams illustrate the mechanism & process flow:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

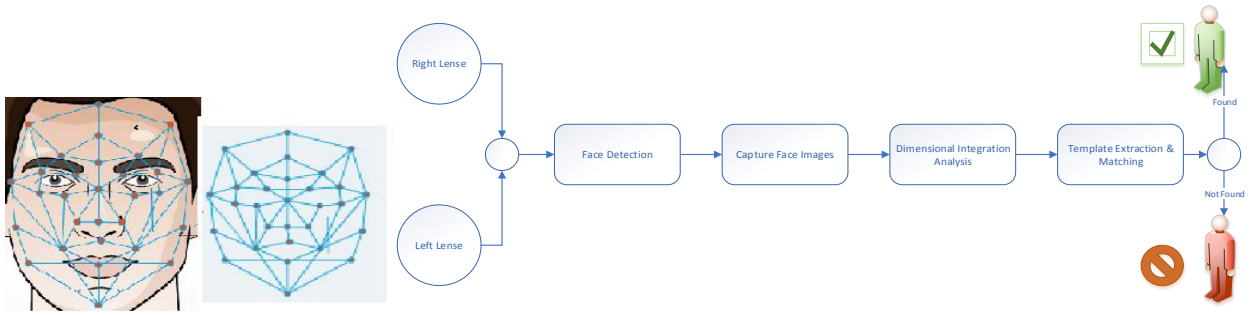

Fig. 11 Face Recognition

B. Fingerprint Identification

Fingerprints remain constant throughout the life wherein the fingerprint comparison never produced alike when two are compared over 140 years of fingerprint comparison worldwide. The scanning technology has also become easy as nice fingerprint scanners can be installed in PDAs like the iPAQ Pocket PC except that this might not work in industrial applications wherein this requires clean hands. The Fingerprint identification method involves comparing the pattern of ridges and furrows on the fingertips, and the minutiae points as well (ridge characteristics that occur when a ridge splits into two, or ends) of a specimen print with a database of prints on file.

The following diagrams illustrate the mechanism & process flow:

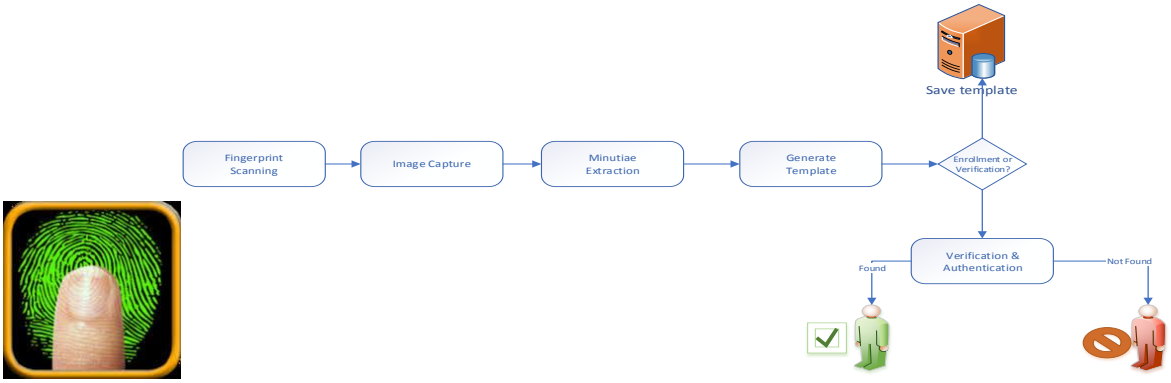

Fig. 12 Fingerprint Identification

C. Retina Scan

The retina cannot be replicated in any known ways. The blood vessel pattern resides at the back of the eye is always unique and remains same for a lifetime. The only exception in this type is it would require for about 15 seconds of careful concentration for a good scan. This type is a standard in military and government installations as this type is most accurate and reliable in biometrics.

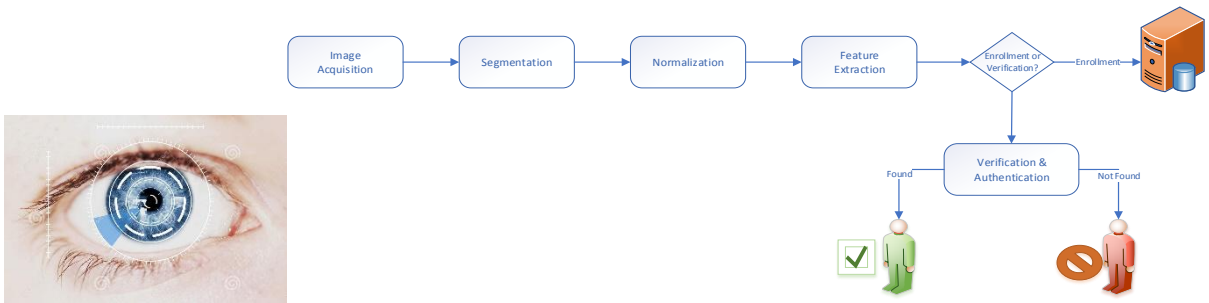

Fig. 13 Retina Scan

D. Iris Scan

The Iris scan also offers unique and reliable data, which cannot be duplicated and remains constant for a lifetime as like retina scan. There are various ways of encoding this iris scan biometric data, which can be securely carried around in a barcode format.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

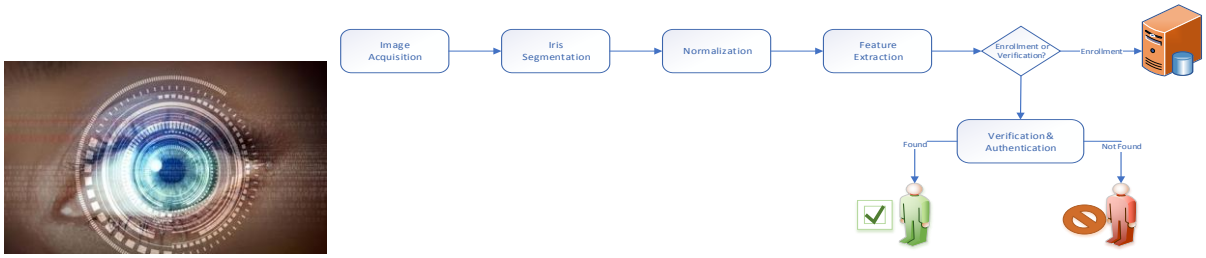

Fig. 14 Iris Scan

E. Signature

A signature is another type of biometric data that is easy to collect and is not physically invasive. Digitized signatures are sometimes used, but usually they have difficulties in authentication due to insufficient resolution. The advantages in this type is fast response and low storage requirements. In addition, the high compression does not affect shape/resolution of the signature.

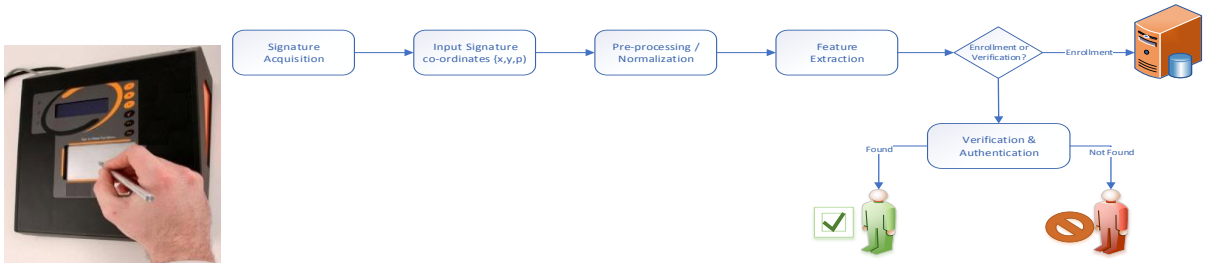

Fig. 15 Signature

F. Facial Thermogram[13]

A scientist Francine J. Prokoski demonstrated that facial thermograms are unique to individuals in the mid-1990s, which can be used for positive biometric identification. In general, thermograms are visual displays according to the amount of infrared energy emitted, transmitted and reflected by an object, wherein it will be converted into a temperature and displayed as an image of temperature distribution. The technology behind is, detecting the heat patterns that are emitted from the skin which was created by the branching of blood vessels, that are known as thermograms and unique obviously. Even the identical twins have different thermograms. Thermography functions like similar to facial recognition only except that the image capturing is done using an infrared camera. Prokoski also stated that this technology is more accurate and more robust among the lighting and environment conditions than the use of video images. The biosensor data is used for identifying individuals uniquely and automatically.

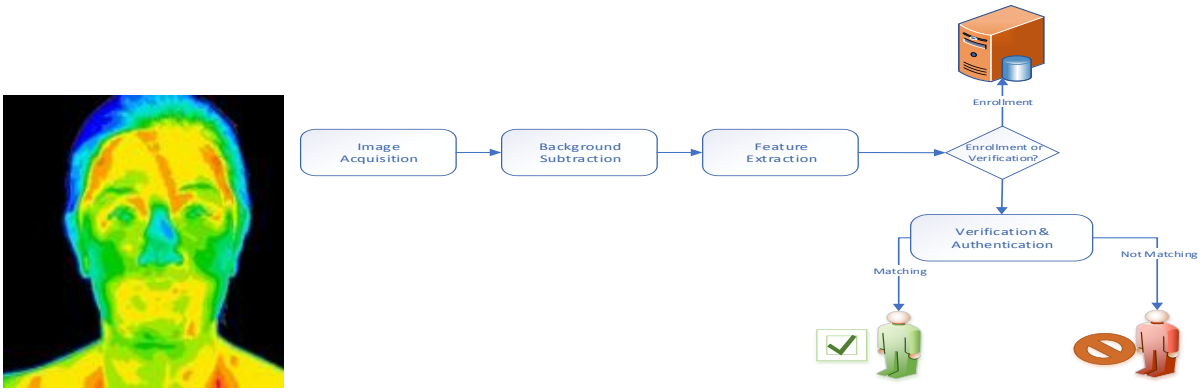

Fig. 16 Facial Thermogram

G. Tooth

Using dental radiographs biometrics, the human identification in forensic science. It provides information such as teeth shape, teech contour and relative position of neighbouring teeth and shapes of dental work like crowns, filling etc. To find an unidentified subject, Dental biometrics requires antemortem (AM) and postmortem (PM) radiographs which consists of three stages: Preprocessing and segmentation of radiographs, Contour extraction or dental work extraction, Atlas registration and matching. Teeth and jaw structure often used after the fact in human identification.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

[16] The SFE Biometric Identification profile includes a wide-ranging forensic x-ray of the teeth and jaw through which the image will capture dental work such as fillings or appliances and the root structure of the teeth as well critically important.

The following are the strengths for biometric identification:

- The x-rays will be having unique patterns for each individual, even though the teeth has been lost or extracted or extensive dental work is done etc.
- The identity can be confirmed in a very few hours by an expert.
- This method is proven as best method as this is useful in identifying by skeletal remains.
- This is useful as opposed to DNA is it is not recoverable due to decomposition in a body.

Except that, the limitation is with some countries wherein the dental and healthcare is of low quality.

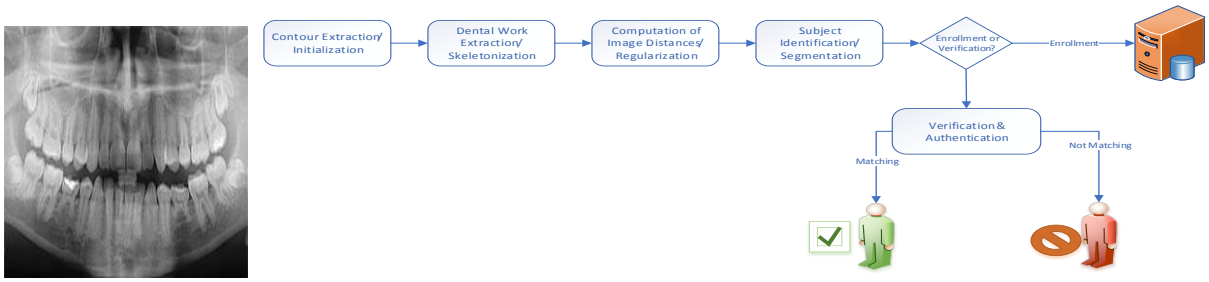

Fig. 17 Tooth

H. Ear [11, 12]

UK researchers claim that a new type of ear-shape could realize ear biometrics as surpass face recognition as an automatically identification method. This can be used to identify the people from CCTV footages, or incorporated in mobile phones, by Mark Nixon from University of Southampton who is a biometrics expert. Ears are remarkably consistent and unlike faces, they the shapes are not changed with different expression or age. They remain fixed in the middle of side of the head against a predicted background. According to Nixon and David Hurley's survey, this method was 99.2% accurate involving 63 objects. In case of hair, infrared image can be used to eliminate them. [12]

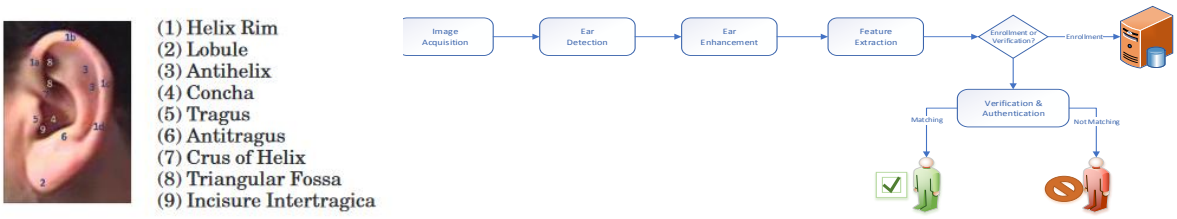

Fig. 18 Ear

I. DNA [14]

DNA is becoming popular/useful biometric and most often in Forensics and Healthcare domains. The short tandem sequences (STR) are measured in forensics in the nuclear or mitochondrial DNA. DNA provides most reliable personal identification among the various available types of biometric personal identification systems. This system does not change during a person's life or after his/her death in nature. DNA can be considered as a blueprint of a human body, which is folded inside the nucleus of each cell.

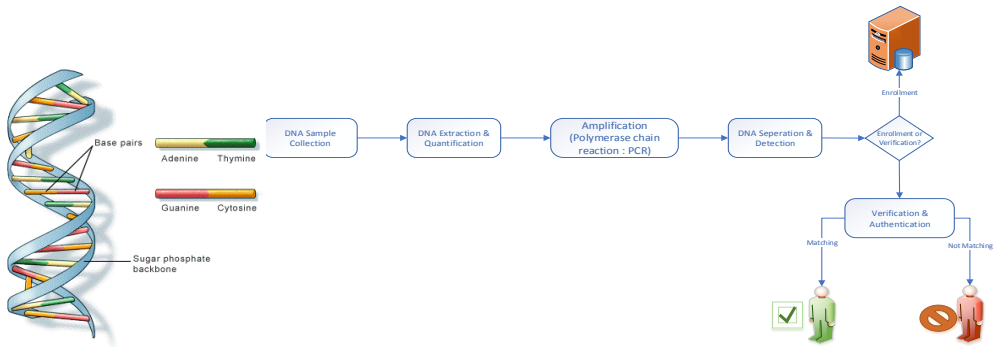

Fig. 19 DNA

DOI10.17148/IJARCCE.2017.6930

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

J. GAIT[15]

In human recognition systems, this biometric has demonstrated potential promises as an alternative identifier. Still important aspects of gait being measured using one or more several analysis techniques as no single measure encompasses full set of complex dynamics reflected what is being considered as human gait. The visual approach uses cameras by which differing angle of gait from a particular distance and sensor approach as well.

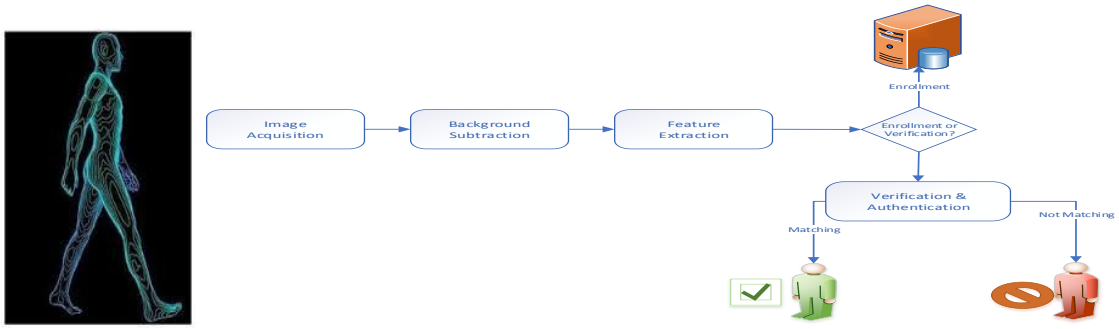

Fig. 20 GAIT

K. Footprint[17]

In Footprint identification method, the footprint features are measured for a user's identify recognition. A footprint is an universal and easy way for capturing identity which will not be changing much over a period of time. Footprint-based measurements establishes one of many new possibilities to grasp biometric authentication. This is currently under research as being an experimental technology. This is projected as an emerging alternative to access control in wellness domains like spas, thermal baths etc. In addition, this is recommended to identify newborn babies in hospitals. It is difficult for hackers to acquire footprints for forgery attacks due to the habit of wearing shoes. In addition, the storage does imply security threats as there are not intended to support large-scale high security applications. This technology would examine friction ridge, texture and foot shape and even foot silhouette. For verification, pair of footprints will be used as people stand in various positions with different distances, wherein the input footprints will be normalized in position and direction. [18]

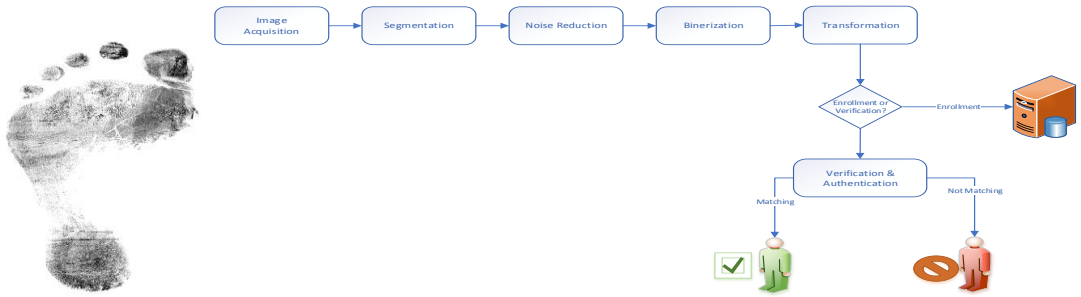

Fig. 21 Footprint

L. Mouse Dynamics [19]

Mouse is widely used, either touch board or mouse is essential in daily life. This method is very cheap and APIs were developed to capture the data. The password of the system would be action with mouse of an authenticated user. The system will accept only if the user perform right action, otherwise will be rejected. It is hard to mimic as the hacker must do a lot practice of that certain movement as same as authenticated user. In addition, the mouse also will not move as the hacker expects. The touch screen is also similar to mouse.

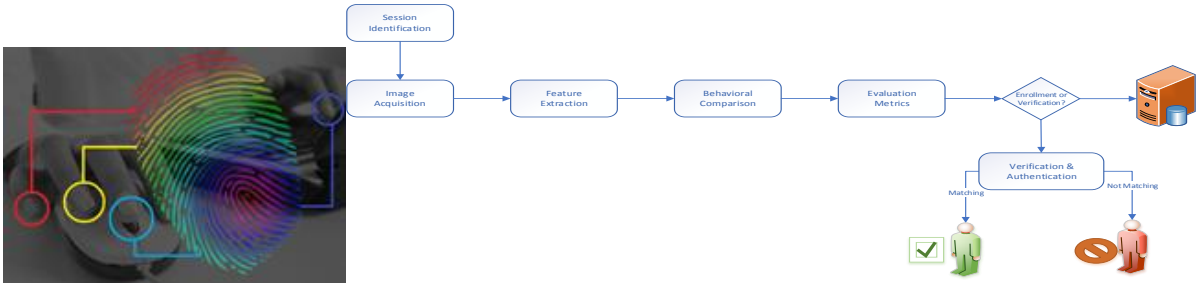

Fig. 22 Mouse Dynamics

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

M. Hair [20]

The Hair Protein might be next frontier in biometrics as among the available methods like Fingerprints, voice recognition, DNA, iris scanning are well established and effective as well. In a recently published article in scientific research website PLOS says "Demonstration of Protein-Based Human Identification Using the Hair Shaft Proteome", which shows the indication of hair protein becomes biometric authenticator. Based on a research analysis report, among the 76 hair samples analyzed, and found 185 distinct amino acid patterns, by which they were able to identify 98.3% of subjects and a false was under just 2%. Hair protein tests are able to discriminate one person out of 100,000, which shows around ten times as many as tests on mitochondrial DNA from hair.

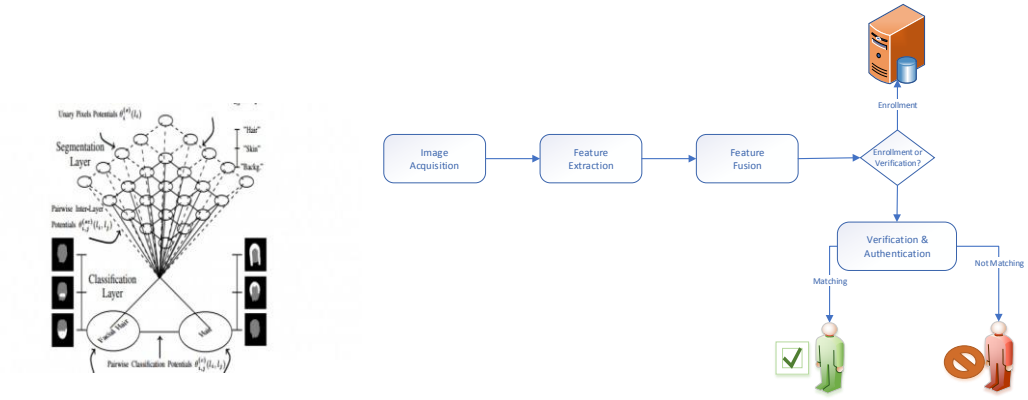

Fig. 23 Hair

N. Keystorke Dynamics [21]

This method is similar to signature, but uses a keyboard instead. This method is used to recognize the behavior of the person when typing on a keyboard. It is a cost-effective alternative method as this requires only a keyboard to acquire data for authentication, which a viable and practical way as being additional security for identity verification. In addition, this becomes more secure when combined with passphrases authentication. This method does not recognize the password type, but also measures intervals between the characters and overall speeds & patterns, which measures statistical patterns instead of features.

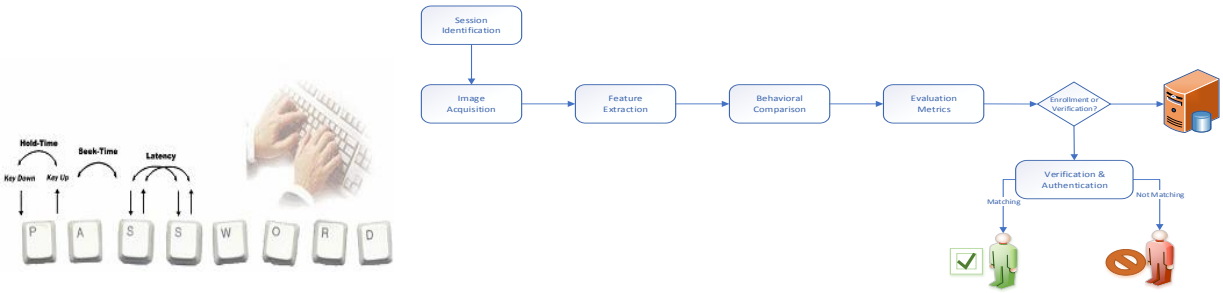

Fig. 24 Keystroke Dynamics

O. Nose [22]

Among the various face-based biometrics available like iris, ear, retina etc, the nose is hard to conceal and relatively invariant to expression. The shape of the ridge is important during the process and fixation points are provided. There are 6 types are identified such as Greek, Nubian, Roman, Snub, Tum-up and Hawk.

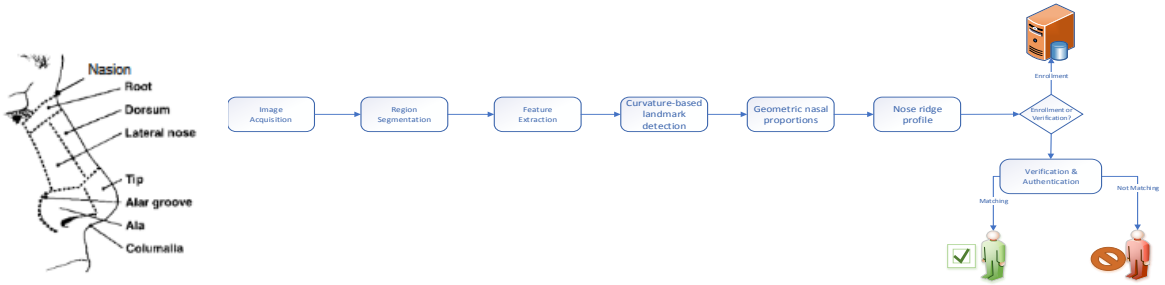

Fig. 25 Nose

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

P. Voice Analysis

Voice biometrics provide a way to authenticate identity without the subject's knowledge, like face recognition. It is easier to fake (using a tape recording), but it is not possible to fool an analyst by imitating another person's voice.

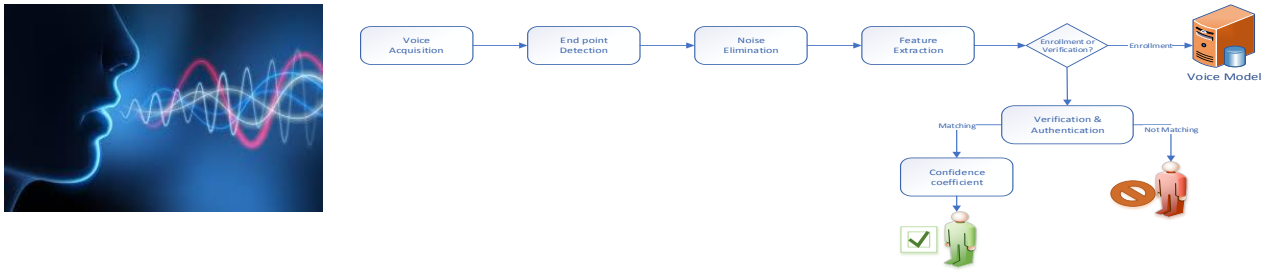

Fig. 26 Voice Analysis

Q. Palmprint [8]

An infrared beam is used to infiltrate the user's hand when it is waved over a sensor/system and the veins will be sent back as black lines. This authentication method is a high-level accuracy, as palm comprises complex vein patterns. In addition, the vein patterns cannot be imitated, as they are internal to body. Also in terms of hygiene, this is completely recommended for usage in public areas as being contactless.

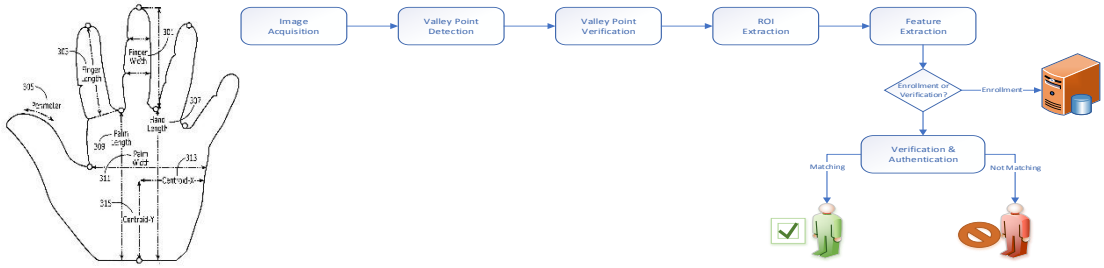

Fig. 27 Palmprint

R. Odour/Scent [8]

In general, it's obvious that people produce different body odours due to differing immunity genes. The automated detection and classification are done by using electronic/artificial noses that are developed as a system on odours, vapours and gases. Prometheus (Alpha Mos) is an example. Sensors are used to capture the body smell/odour from non-intrusive parts of the body such as back of the hand. But this method is a privacy issue as this contains extensive sensitive personal information.

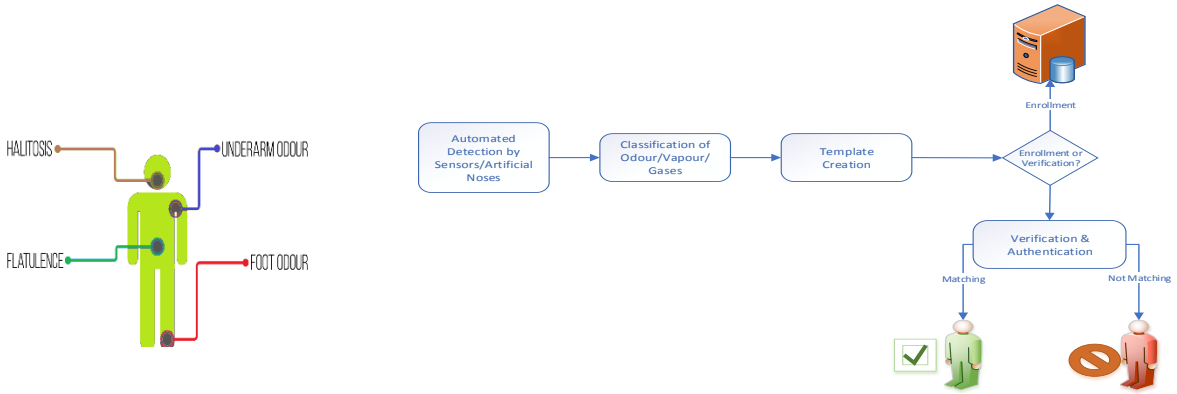

Fig. 28 Odour / Scent

S. Hand Geometry

Hand geometry readers work in harsh/critical environments, in which clean conditions do not exist, and forms a very small dataset. It is not considered as an invasive kind of test, but the choice of an authentication method in industrial environments.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

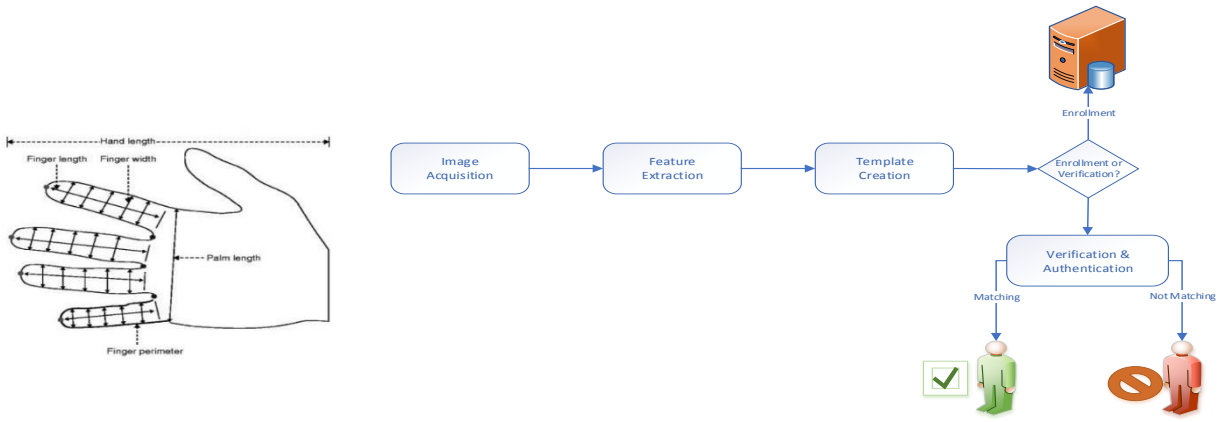

Fig. 29 Hand Geometry

VI. PROPOSED APPROACH / RELATED WORK

The following are the few research areas identified by the researchers in terms of security needs to more effective/efficient:

- Virtualization
- Cloud-mobile communication
- Security framework
- Secure data transfer
- Secure Stored Data
- User Access Control

Our future research would be focussing on implementation of the cryptographical methodologies in making enhancements to any of the above said biometric areas w.r.to the above said areas.

VII. CONCLUSION / FUTURE RESEARCH DIRECTIONS

As the usage of cloud is getting increased day-by-day, the need of security also being increased as it plays a vital /critical role extensively. On the other hand, Encryption Algorithms play an essential/critical role in overcoming the security issues by using the various cryptographic techniques available that would help in addressing the security issues in Cloud. Algorithms that are more efficient can be developed/enhanced which can increase the security level in the cloud environment. Biometric identification methods are most prevalent that can be used in addressing these security issues along with cryptography. This paper enlightens about various biometrics available in terms of security. Our future research would be focusing on ensuring high-level security in cloud by adding/enhancing the cryptographic techniques on any of these biometric identification methods in the various areas identified wherein the security is mandatory.

REFERENCES

[1] US National Institute of Standards and Technology (NIST, http://csrc.nist.gov).
[2] Cloud Security Alliance (CSA)
[3] Ali Gholami and Erwin Laure, "SECURITY AND PRIVACY OF SENSITIVE DATA IN CLOUD COMPUTING: A SURVEY OF RECENT DEVELOPMENTS",NETCOM, NCS, WiMoNe, CSEIT, SPM - 2015 pp. 131–150, 2015. © CS & IT-CSCP 2015 DOI : 10.5121/csit.2015.51611
[4] G. Kishore Kumar, Dr. M.Gobi ,"Current Trend in Cloud Computing Security & Future Research Challenges", INTERNATIONAL JOURNAL FOR RESEARCH & DEVELOPMENT IN TECHNOLOGY (IJRDT), Volume-7,Issue-6, (June-17)
[5] G.Kishore Kumar, Dr.M.Gobi,"Role of Cryptography & its Related Techniques in Cloud Computing Security",International Journal for Research in Applied Science and Engineering Technology,IJRASET,Volume 5 Issue VIII (August 2017)
[6] G. Kishore Kumar, Dr. M. Gobi,"Comparative Study on Blowfish & Twofish Algorithms for Cloud Security",International Journal of Current Trends in Engineering & Research (IJCTER), Volume 3 Issue 9, September 2017 pp. 1 – 11
[7] Rakhshanda Batool,Ghazal Naveed,Abdulhaq Khan,"Biometric Authentication in Cloud Computing",International Journal of Computer Applications (0975 – 8887) Volume 129 – No.11, November2015
[8] Aleksandra Babich,"Biometric Authentication. Types of biometric identifiers",Bachelor's Thesis, Degree Programme in Business Information Technology, 2012
[9] Akshay A. Pawle, Vrushsen P. Pawar,"Face Recognition System (FRS) on Cloud Computing for User Authentication",International Journal of Soft Computing and Engineering (IJSCE), Volume-3, Issue-4, September 2013
[10] Secure and Revocable Biometric Template Using Fuzzy Vault for Fingerprint, Iris and Retina
[11] https://www.newscientist.com/article/dn7672-ear-biometrics-may-beat-face-recognition/

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 9, September 2017

[12] AYMAN ABAZA,ARUN ROSS,CHRISTINA HEBERT, and MARY ANN F. HARRISON, MARK S. NIXON,"A Survey on Ear Biometrics",ACM Computing Surveys, Vol. 45, No. 2, Article 22, February 2013
[13] http://www.biometricupdate.com/201308/explainer-facial-thermography, Rawlson King
[14] https://www.intechopen.com/books/biometrics/dna-biometrics
[15] Rohit Katiyar, Vinay Kumar Pathak, K.V. Arya,"A Study on Existing Gait Biometrics Approaches and Challenges",IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013
[16] http://www.schwarzforensic.com/bi.php?pageid=245
[17] http://www.biometricupdate.com/201401/explainer-footprint-identification
[18] Kapil Kumar Nagwanshi,Sipi Dubey,"Biometric Authentication using Human Footprint",International Journal of Applied Information Systems (IJAIS) ,Foundation of Computer Science FCS, New York, USA,Volume 3,No.7,August 2012
[19] Xuantong Zhang"Human user authentication based on mouse dynamics: a feasibility study",Iowa State University
[20] http://www.biometricupdate.com/201609/study-finds-hair-protein-effective-as-identifier
[21] Syed Zulkarnain Syed Idrus, Estelle Cherrier,Christophe Rosenberger, Patrick Bours,"Soft Biometrics for Keystroke Dynamics",ICIAR 2013, LNCS 7950, pp. 11–18, 2013
[22] Adrian Moorhouse and Adrian Evans,Gary Atkinson, Jiuai Sun and Melvyn Smith"The Nose on Your Face May Not be so Plain: Using the Nose as a Biometric",ET 3rd International Conference on Imaging for Crime Detection and Prevention (ICDP-09), Kingston, UK.

BIOGRAPHIES

G. Kishore Kumar is a research scholar in Department of Computer Science, Chikkanna Government Arts College, Tirupur-641 602, India. He has completed Master of Computer Applications [MCA] in Alagappa University, Karaikudi, India. His major field of study is Network Security and Cryptography.

Dr. M. Gobi is an Assistant Professor in Department of Computer Science in Chikkanna Government Arts College, Trippur-641 602, India. He teaches courses for BSc Computer Science, BCA and Master of Computer Science (MSc). His research areas of interest include Cryptography, Java, Software Engineering and Information Systems Security.