International Interdisciplinary Virtual Conference on
'Recent Advancements in Computer Science, Management and Information Technology'
International Journal of Scientific Research in Computer Science,
Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Automation : Augment Essentiality of Security Measures

Dr. Reena Gupta[1], Dr. Bhaskar Seth[1]
[1]Associate Professor
Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India

ABSTRACT
The desire for the quickest, easiest ways to do any work has increased along with living standards. Automation modifies people's work schedules to accommodate current demand. The importance of the automation is increased by this thing. However, it is essential to preserve socialism's fundamental aims and requirements. This paper covers security issues that necessary in today's automated society. These security measures were created with the use of digital image processing, biometrics, and artificial intelligence (AI).
Keywords: Automation, Security, Authentication, Verification, Biometric Science, Fingerprint

I. INTRODUCTION

Security must be a realistic challenge in the real world. Security can be defined in following manner, as Personal Security, Currency Security, Security of Privacy, Security against fraud, Security of information and many more. Security tasks can be provided to the persons by the help of either person-to-person interaction like in guarding operation or person-to-machine interaction like in Surveillance Camera mechanism.

Person-to-person interaction for security point is considered in the scene of person or nation or currency security where human being needed as a guard. Guard operation is very difficult and hazardous. If consider security against fraud, then we need authorization or verification operation. This task is not only difficult but also time consuming, fatigue and non-reliable. If consider security of information, then this task is very costly with full of tension.

Person-to-machine interaction for the security purpose is easy, effortless, non-hazardous, less time consuming and reliable task in compare to above. This type of security options are totally based on computer system. Tools that is required for establishing a security system either in home or enterprise area. These tools are sensors, cameras, storage area, monitoring device like desktop, laptop or mobile, alarms etc. [1]. Software is basically an application program which is used to manage security operations. Required hardware tools and security-based software applications such as- Antivirus Software, Anti-Spyware Software, Password Management Software, Tracking Software, Authorization Verification Software, Cryptographic Software[1] etc. are shown in below figure 1.1.

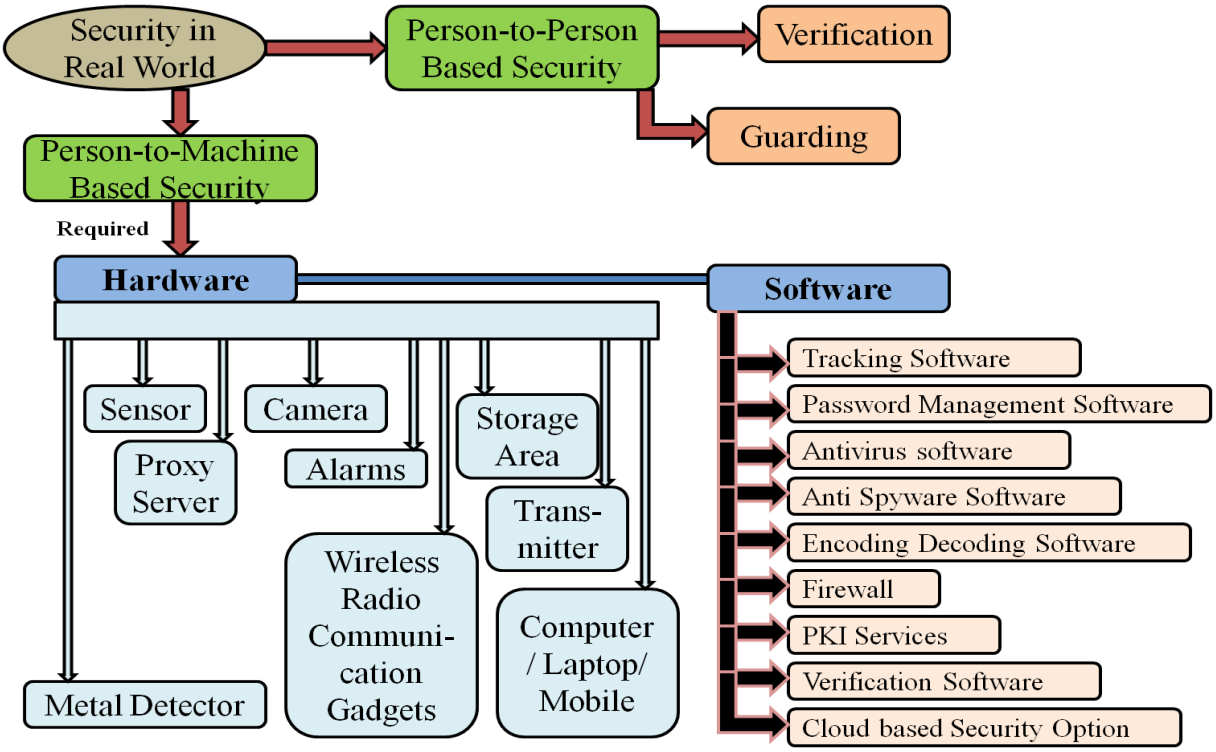

Figure 1.1: Security Measures with Required Hardware and Software Tools

Security Software

Software tools those are required to perform security operations are called security software which are designed for monitoring, provide authorization, maintain confidentiality, investigate authentication and ensure availability and many more operations [2]. Security software is based on image processing, cryptography, computational science, artificial intelligence etc.

Need of Security Software

Internet is the backbone of the digital world. Every person use internet to complete his task. Dependency on the internet is increased as a spider web. Task like question answering, searching, writing, designing, developing, communicating, and all other daily routine work are affected from this. So that's why it is very important to keep us safe in various manners -

a) **Threat of Private Information Loss** – When personal data like identity card number, phone number and many more are leaked to unknown person. This act is very dangerous for the person because unknown person may steal their identity and misuse it.

b) **Threat of Unauthorized Access** – If any unknown person enters in the authorized area without permission or accessing power then this act is more dangerous and become a cause of information and data loss.

c) **Threat of Fraud –** If any unknown person cheats any individual in terms of money loss, then this act come under fraud.

d) **Automated Infection –** When system accepts any unwanted data which is harmful, that time your system become a spreader. Harmful content can spread in other systems in a few seconds.

e) **Unfriendly Code–** When some codes are run in our system without our knowledge and that are harmful for us. But it needs to be executed.

f) **Unfriendly Physical Environment**– When our personal devices like laptop, mobile may be lost or stolen by someone, at that time, condition of physical attack is increased.

In the digital world, security is seeing in many ways as in [2] and it's shown in table 1.1.

Table 1.1: Types of Security

Security Name	Target	Relates to
System Security	Security for design system	Authentication
Information Security	Secure the data or information	Cryptography
Access Security	Security regarding Authorization	Authentication
Privacy Security	Keep hide personal information to others	Information Hiding
Cyber Security	Keep safe the information in a network from information breach and malicious attack [3]	Cryptography
Network Security	Secure the computer network from the intruder [4]	Cryptography

Security Policies

Every individual and organization define their requirements regarding security from the computer in person-to-machine interaction or digital world scenario. These requirements show the importance of digital security. These rules define as security policies which are described here and shown in figure 1.2.

a. **Confidentiality** – security that provide assurance of not to leak information or data to someone other than authorized individuals. Guaranteed that no one can break the personal privacy rule [5].

b. **Integrity** – maintain the authorization by giving permission to someone from administrating. System can't pass any unauthorized and improper information to all[5].

c. **Availability**– to design a system in a way that it can be accessible by all in a prompt manner.

d. **Accountability** – designing a system in a way that it can maintain a record of individuals that access the system.

e. **Cost Effective** – easily carried out by the general people.

f. **Unbreakable** – designed system in a way that it can handle any type of intruder attack and percentage of damage is null.

g. **Fully Communication System** – if any changes or threat is discovered, then pass the information to everyone, who use that system.

h. **Durability** – system design for the long-term period so that person take the functionality at once and remain stress free about security for long time period.

i. **Easy Maintenance** – system designed in a way that it can easily accept the changes and update itself.

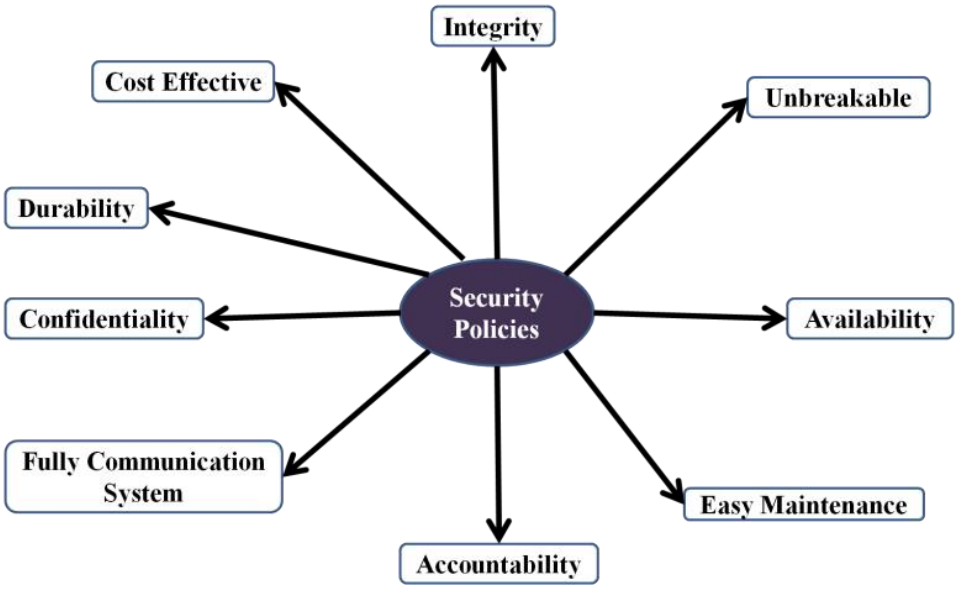

Figure 1.2: Security Policies

Computer Based Security

Person-to-machine interaction in term of security increase the demand of designing a secure computer system in which system contain all security measures with other task applications. These types of computer systems have high computational rate, large database, fast speed and high memory capabilities, which made it more powerful. The most important features which are required for it, is highly secure environment where it used and highly secured technique for securing data present in it.

Both features are related to the security issues. Highly secure environment means the place where system will be established in secured area, where no one comes without administrative permission. It is said in this way that only authenticated person can access that environment.

Highly secured techniques for securing data means system developer has to use these types of techniques by which entered data is safe. If in one case, someone enter the secure environment and stole the data or in other case, data stolen by any authenticated person, at that time no one can understand the data. This terminology is used in the cryptography field.

1.1 Highly Secure Environment or Authenticated Premises

Working environment means the place where human beings perform their specified task. Now in term of person-to-machine interaction, highly secure environment means a place where various computer systems are situated and only authenticated person or persons with administrative permission can enter the premises. After

entering the premises, persons can start their computer system when they prove their identity in front of system. The main goal of this feature is authentication of a person or an individual.

Authentication Process

Authentication process is a process which is designed to check the authenticity of the individual. This process is split into two phases–

i) **Registration Phase** – In the registration phase, user has to register himself in the computer database by giving his identity.

ii) **Authentication Phase** – Authentication phase is designed to check the identity of an individual. If he/she wants to come in the authenticated premises, then he/she have to give their identity to the computer when it asks. After providing the identity by the individual, computer checks their identity in the database. If the record is found, then computer will permit an individual in the premises otherwise deny him.

Authentication phase accomplish its task in two ways which are considered as Authentication Methods [6] –

Authentication Methods -

i) **Identification Method**- Identification method is a method which is based on the 1: N comparison where N is the total number of persons present in the database. Authentication process run and check user identity, when user give their ID proof to the admin and admin checked it with the database which contain names of the authorized individuals [6].

This method is very time consuming because this method uses the linear search approach which has $O(n)$ time complexity. Figure 1.3 represents registration method in which method (A) store the data in standard manner and method (B) store data with unique ID.

ii) **Verification Method –** Verification method is a method which is run with the help of Indexing technique, in which database generate one unique number to each entry as an identity number or index number (ID) in the registration phase and also give the same ID to the user.

In authentication phase, when searching algorithm is applied, then user gives their ID and admin only check that particular ID related entry record. If the user details are matched with the database entry, then user is authenticated. This method has performed1: 1comparison [6].

This method is very fast because comparison operation takes only $O(1)$ time complexity, which makes this method very reliable and robust [6].Figure1.4 represents verification method where method(A) shows 1-to-N process for verification and method (B) shows 1-to -1 process for verification.

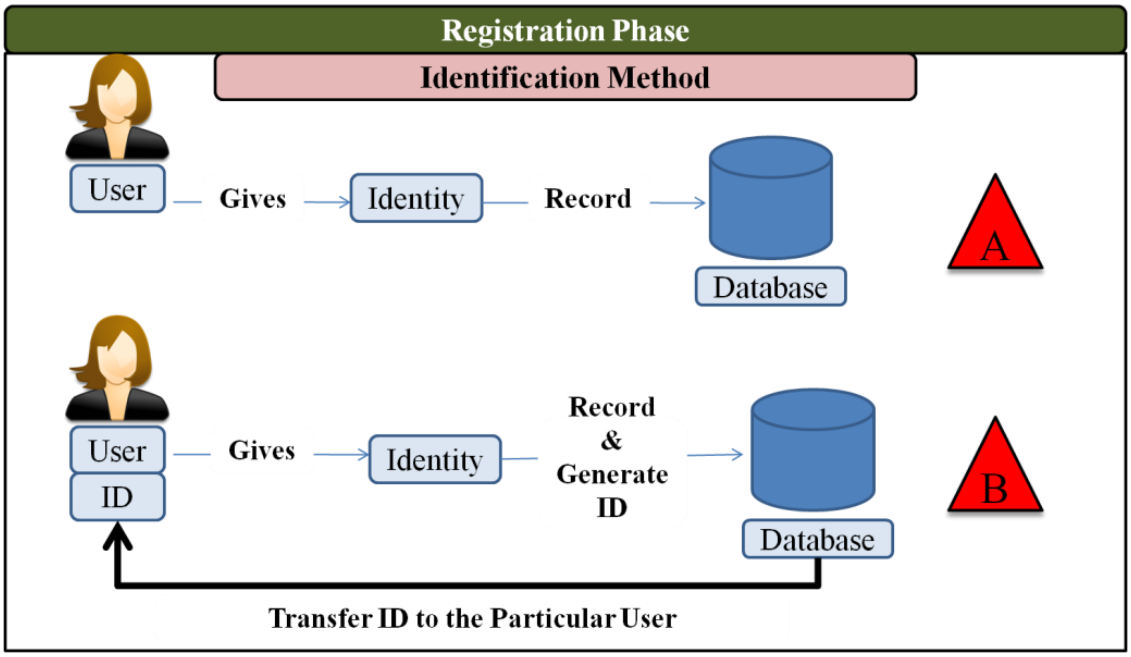

Figure 1.3: Registration Method: A) Standard Data Registration B) Data Registration Done By ID

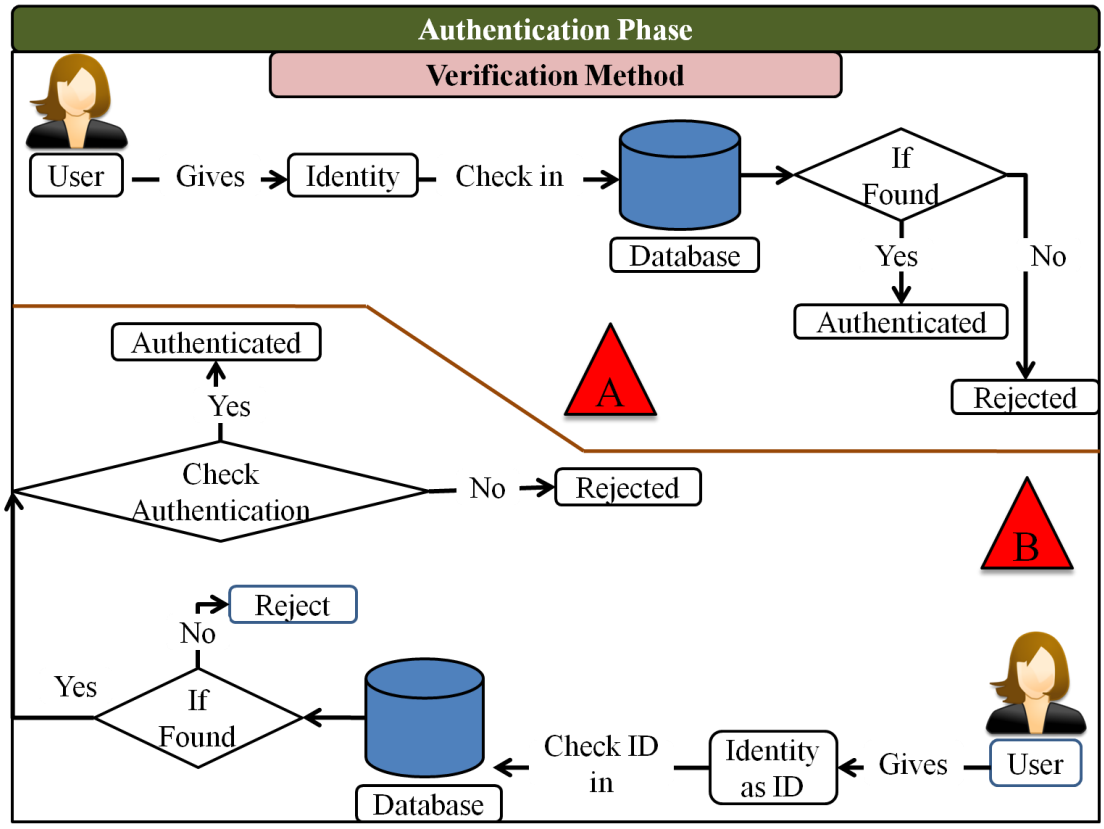

Figure 1.4: Verification Method: A) Verification by 1-to-N method B) Verification by 1-to-1 method

1.7.1 Authentication Techniques

In the real world, it is compulsory to know that how many techniques are available in the world for proving the identity of an individual. If considering about the last century, then there were various techniques for proving the authentication of an individual. These techniques are mainly doing its task on two bases [7] as -

i) **Knowledge Based Techniques –** Knowledge based techniques are those techniques which rely on the individual's memory. For this technique, individual have to use his remembering power and remember his passwords, permanent identification numbers (PINs), secret codes [7] [8] etc. and whenever someone need to authenticate you, you have to provide it.

This technique is totally based on the human brain capacity. If someone's brain doesn't remember any identification mark, then he/she cannot use that premises. For example, if a person has one digital locker and he/she stored some important documents in it. If person forgets the password, then he/she cannot access their locker again. And in future it may be very hazardous for them.

ii) **Token Based Techniques –** Token based techniques are techniques in which each user or individual has his own identical token which proves his identity. This identical token can be anything like Driving License, Passport, Aadhar Card, Smart Access Card, Pan Card, Voter ID Card, Cash- Machine Card, ID badges etc. [7] [8] [9].

In this technique, when someone wants to enter in the authorized premises, then he/she must provide their specified token like passport to the administrator and admin check their specified token number in the database. If token number is found, then person is authenticated otherwise not.

This technique works very well in all scenarios but there are two major problems discovered -

i) In the case where token-based authentication technique is used to prove individual's identity, then individual must go personally to confirm his identity. This method is not convenient in the emergency and pandemic situation.

ii) Stolen identity i.e., someone steal the identity token of any person and put himself in place of him by the help of stolen token.

If both conventional methods are weighted in the scale of security, then both are declared as insecure methods [7] [8] [10] because forgotten their password/ PINs/ Secret code, misplace their identity card, some identical relations swap their photo identity card, password may be guessed, Card cloning, are considered as threat.

In the digital world, both conventional methods are non-reliable in proving the identity of an individual.

Due to the above listed security problems; today's digital era is not accepting the conventional methods for personal authentication process. It is essential for us to design some special and effective authentication system which can handle the security issues of digital era. Biometric science has emerged as an alternative solution of this problem.

Biometric Science

Biometric Science includes the science of evaluating body characteristics [7, 9]. The most important point about human being traits is that every individual has his identical and unique features which are helpful in

differentiating an individual with others. This identical information can be classified further into two parts because of its nature. ***Physiological traits*** – human body traits which belongs to the physics of the human being is known as physiological traits. Physiological trait are observable characteristics of the humans [11] such as – fingerprint, iris, face, retinal patterns, ear, dental, palm print, hand geometry, lip print[8] [9] [10] [12] [13].***Behavioral traits*** – A human body trait which belongs to the expression or action or activity of the body, generated because of nervous system [7] are known as behavioral traits. These traits are voice recognition, keystroke dynamics, handwritten signature dynamics, gait, walking pattern, typing pattern etc. [8] [9] [10] [12].

1.2 Biometric Science – An Alternative of Authentication Technique

Biometric science is a science in which we can study those human features that are identical or unique property i.e. these biometric traits are good alternative for proving individual identity and cloning or stealing of these features is not an easy task. For the digital world, bio-information or biometric science is emerged as a good authentication technique with easy maintenance, reliable services, and robust system.

Working of Biometric Science for Authentication Process

Biometric information of an individual is captured by the help of sensor, or scanner or any acquisition devices and copy & save that information in the computer memory. When the individual comes and asking permission for entering in premises, computer asks for the biometric information. When individual scans their bio-information, computer compares that scanned information with the registered data which is stored in the computer memory. If the comparison is successful, then computer permit him otherwise entry is denied [9]. Figure 1.6 represents biometric based information registration and authentication process.

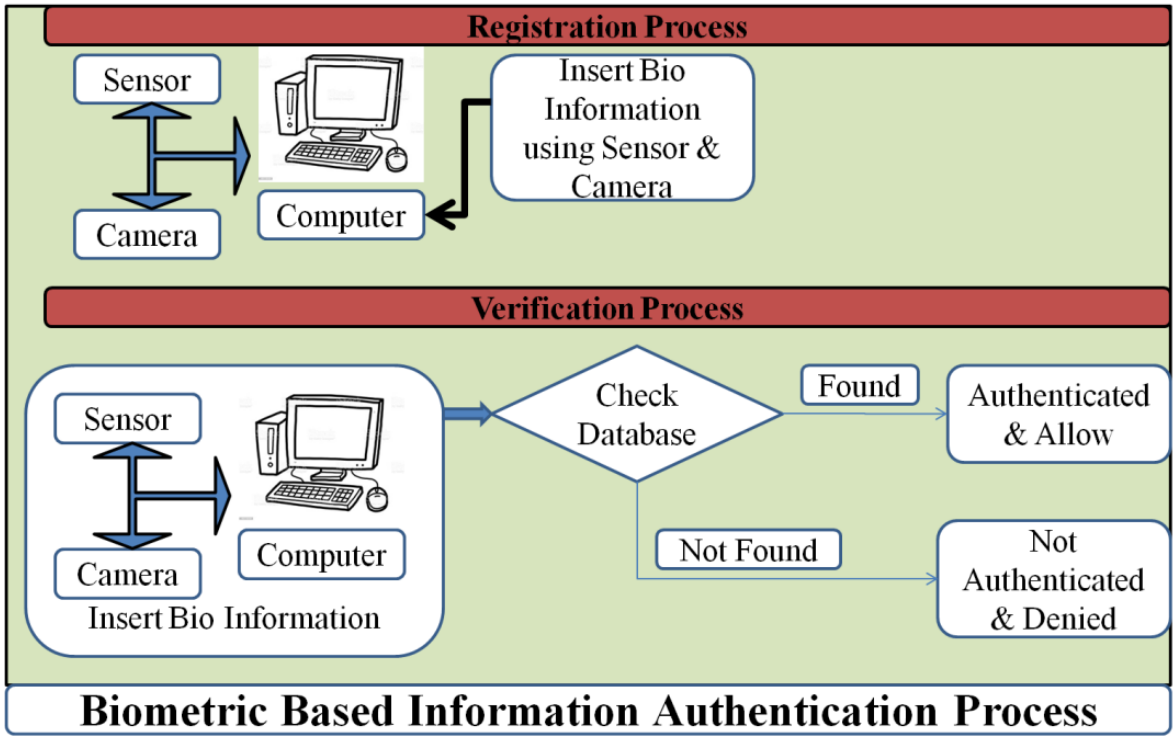

Figure 1.6: Biometric Based Information Authentication Process

Biometric Information

Human body has much identical information like fingerprint, palm print, eye retina, iris pattern etc. According to the nature-based classification of identical features, few features are described below as-

Fingerprint

Fingerprint, which is unique feature of human being, has very easiest way of use and long-term stability. Generation of fingerprint is completed at the time of birth. Generating process is based on the genes and environmental conditions during pregnancy. So that twins who have same DNA also had a different fingerprint pattern. So, it is the most reliable, secure and robust method for individual's identification, it can be easy to say that fingerprint is not affected by the genetic [6] [16].

Fingerprint is a scanned form of fingertips of an individual, which has pattern of ridges and valleys. It is formed on the skin with the mixing of ridges and valleys, and it develops a unique pattern. An individual has unique pattern of fingerprint, and it has no changes throughout the lifespan of an individual. A fingerprint pattern (as shown in figure 1.7) has curvature, terminations, bifurcations, cross-over etc. shapes in high density, which makes distinctive regions based on ridges and valleys. These regions consist of various arch, tented arch, loops (left, right, twin), core, delta, and whorl topologies. Fingerprint pattern also contain the minutiae which has two main structures [6] [17]–

- *Termination* – small region where ridges lines end abruptly
- *Bifurcation* – ridges lines are separated into two branches

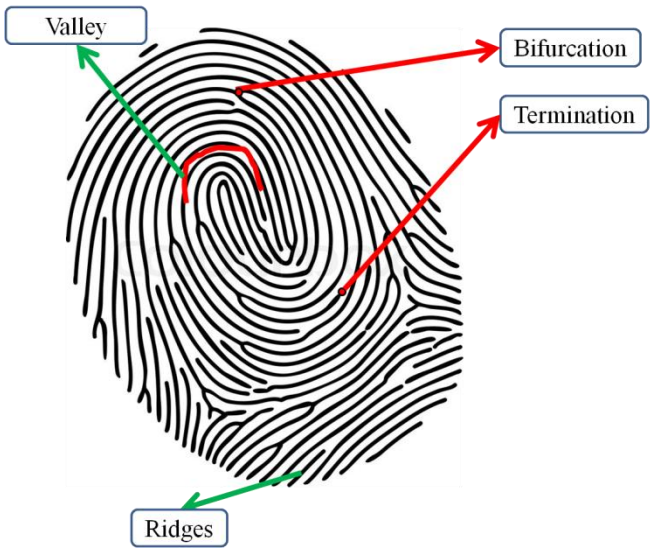

Figure 1.7: Fingerprint Pattern

1.12.1 Iris

Human eye image has different patterns in each person, formed by combined layers of pigmented epithelial cell, muscles for controlling the pupil, stomal layer consisting of connecting tissues, blood vessels and an anterior border layer [18] [19]as shown in figure 1.8. According to the medical science, iris patterns are stable

over time with uniqueness, time invariance and immovability features [12], and only minor changes happen to them in a lifespan of an individual. Iris structure is fully designed by ten months of age and remains same for the whole lifespan [12]. The other traits are changed with the time. Iris recognition system uses 240 reference point of iris for matching purpose. The iris is a circular diaphragm that punctured because of the pupil, and it lies between cornea and lens. How much light can enter through the pupil (a circular aperture area) is controlled by the iris .The pupil size can vary from 10% to 80% of the iris diameter where the diameter is approximately 12mm [12].

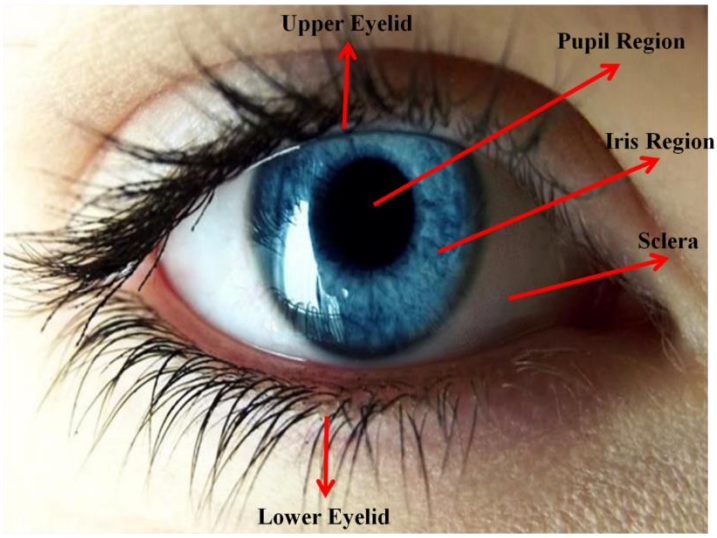

Figure 1.8: Eye pattern

Walking Pattern

Every person moves with their legs. But it is very unusual thing that pattern of walking of every person has unique features. And walking shows the behavior of the person. That is why it is considered in the behavioral trait in authentication process. Uniqueness consider in walking pattern depends on the footstep, pressure on the foot, sound generate by the footstep, angle made between thigh, knee and leg. All these are measured by the help of sensor and stored in the database for each person [20].

II. CONCLUSION

The demand for security software is boosted due to increasing rate of automation and digitalization. In the current world, security can be provided in a variety of classic and contemporary ways. The conventional approach relies on human memory, statistics, patterns, etc. However, modern methods use biometric science in designing security software. one of the most reachable security software in based on automatically identified individuals by a computer system using their own particular biometric traits.

III.REFERENCES

[1]. https://blog.devolutions.net/2018/02/4-types-of-security-tools-that-everyone-should-be-using

[2]. Butler W. Lampson, "Computer Security in the Real World", IEEE, pg -1-20

[3]. https://www.javatpoint.com/cyber-security-tools

[4]. https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security

[5]. https://www.pmi.org/learning/library/importance-of-security-requirements-elicitation-9634

[6]. Satish Kumar Chavan, Parth Mundada, Devendra Pal, "Fingerprint Authentication Using Gabor Filter based Matching Algorithm", published in "2015 International Conference on Technologies for Sustainable Development (ICTSD-2015), Mumbai" 978-1-4799-8187-8/15, Feb 04-06, 015

[7]. Wayne Thompson, Hui Li, Alison Bolen, Article: "Artificial Intelligence, Machine Learning, Deep Learning and Beyond: Understanding AI Technologies and How They Lead to Smart Applications" published in SAS Insights, Jul 5, 2021. https://www.sas.com/en_in/insights/articles/big-data/artificial-intelligence-machine-learning-deep-learning-and-beyond.html#/

[8]. https://en.wikipedia.org/wiki/Sophia_(robot)]

[9]. Robert J.Fischer, Edward P. Halibozek, David C. Walters, "Holistic Security Through the Application of Integrated Technology", Chapter 17 in "Introduction to Security (tenth Edition), Elsevier, pg- 433-462, 2019

[10]. https://www.tutorialspoint.com/artificial_intelligence/artificial_intelligence_quick_guide.htm

[11]. D. Marr, "Artificial Intelligence – a Personal View" published by Massachusetts Institute of Technology, Artificial Intelligence Laboratory, AIM 355, March 1976, pg. 1-11.

[12]. Tania Johar, Pooja Kaushik, "Iris Segmentation and Normalization using Daugman's Rubber Sheet Model", published in "International Journal of Scientific and technical Advancements", ISSN: 2454-1532, vol .1, issue. 1, pp. 11-14, 2015.

[13]. Joanna Isabelle Olszewska, "Automated Face Recognition; Challenges and Solutions", "Intech Openscience| openminds" Chapter 4 from Pattern Recognition –Analysis and Applications, pg – 59-80, 2016, http://dx.doi.org/10.5772/66013

[14]. Marvin Minsky, "Steps Toward Artificial Intelligence", http://web.media.mit.edu/~minsky/papers/steps.html

[15]. Marvin Minsky, "A Selected Descriptor-Indexed Bibliography to the Literature on Artificial Intelligence", HFE-2, March 1961, pp 39-55

[16]. Anil K. Jain, Salil Prabhakar, and Sharath Pankanti, "On the similarity of identical twin Fingerprints," Pattern Recognition, vol. 35, no.11, pp. 2653–2663, 2002. (reference of ch2-26- 2)

[17]. N. K. Ratha, K. Karu, S. Chen, and A.K. Jain, "A Real-Time Matching System for Large Fingerprint Databases," IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 18, no. 8, pp.799-813, 1996.

[18]. F. H. Adler, Physiology of the Eye. St. Louis, MO: C. V. Mosby, 1965.

[19]. R. P. Wildes, "Iris Recognition: an Emerging Biometric Technology," Proceeding of the IEEE, vol. 85, no. 9, pp. 1348-1363, 1997.

[20]. Md. Navid Rahman, Kazi A Kalpoma, Tabin Hasan, "Automated Person Identification System Using Walking Pattern Biometrics" published in "International Journal of Scientific& Engineering Research", ISSN: 2229-5518, Volume 6, Issue 8, August 2015.