Handling the Problems in Biometrics

Varun Mamillapalli

Foundations of Information Assurance

November 30, 2014

Table of Contents

Illustrations

I. INTRODUCTION

"You may already have the solution to all your security needs right in the palm of your hand-or, more likely, at your fingertips", Mike Hogan wrote in *Entrepreneur* [19]. Biometrics is often remarked as the highest level of security or access control with accuracy more than 95% [1] [2].

> *"Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice."*[20]

During the 1880s, Alphonse Bertillon, a European police officer, was evidently the first person to create an identification system which is based on the measurement of various physical characteristics. This technique is called anthropometry. Fingerprint is the most commonly used Biometric Identifier. Sir Francis Galton first began observing fingerprints as a means of identification. Juan Vucetich, an Argentine police official developed further on Bertillon system and Galton pattern types and devised the first functional system of fingerprint identification, and used it in a murder investigation in 1892[27]. Today, Biometrics is used extensively where unique identification of an individual is required. As of January 2014, the Unique Identification Authority of India (UIDAI) issued 560 million Aadhar cards which involves biometric information like fingerprint and iris images [28]. This is the world's largest Biometric database.

In spite of its accuracy and high level security, Biometrics is widely used for unique identification rather than physical security or access control. This is because of the challenges faced in this field. Providing solutions for these challenges may result in the widespread adoption of Biometrics. But, of all the access control methods, why Biometrics? What are the advantages of Biometrics over the rest?

All the authentication methods can be summarized into three types –

- Something you know (e.g. a Password)
- Something you have (e.g. a Smartcard)
- Something you are (e.g. a Biometric) [3]

In the first type, a person is expected to remember something which he might forget. In the second type, a person is expected to possess something. It is possible that he might lose this possession. But the third type of authentication is "Something you are" i.e. physiological

characteristics of a person. "An employee may not be able to remember a dozen passwords and PINs, but is very unlikely to forget or misplace his or her thumb," P.J. Connolly wrote in *InfoWorld* [21]. Some characteristics are unique to every person and are difficult to spoof, which forms the basis for Biometrics and also makes it more effective. It is not easy to guess or steal the data unlike passwords or tokens. Many forms of biometrics exist and the best suited option can be adopted.

The reason for not using Biometrics for security purposes is that there are more problems than there are advantages. While public acceptance is the primary problem to deal with, other problems include fake biometrics, theft of biometric data, ease of use, environmental factors etc. So, finding solutions to these problems may make Biometrics universal.

II. BACKGROUND

Operation of a Biometric System:

To understand the obstacles and their solutions, the basic understanding of a Biometric system is essential. Any Biometric system typically operates in three phases- Enrollment and Identification/Verification. In the enrollment stage, a person provides an identifier (e.g. Passport, Driving License) and his/her Biometric is linked to the identifier provided [14]. This Biometric is stored in the form of a template. The Quality Checker or the Sensor module captures the Biometric data of an individual from the user interface. From this information, the salient features that are uniquely used to identify an individual are grabbed by the Feature Extraction module. The System Database Module is then used to store the Biometric templates. During the Verification or Identification phases, a Matcher module is used to determine whether the user is valid.

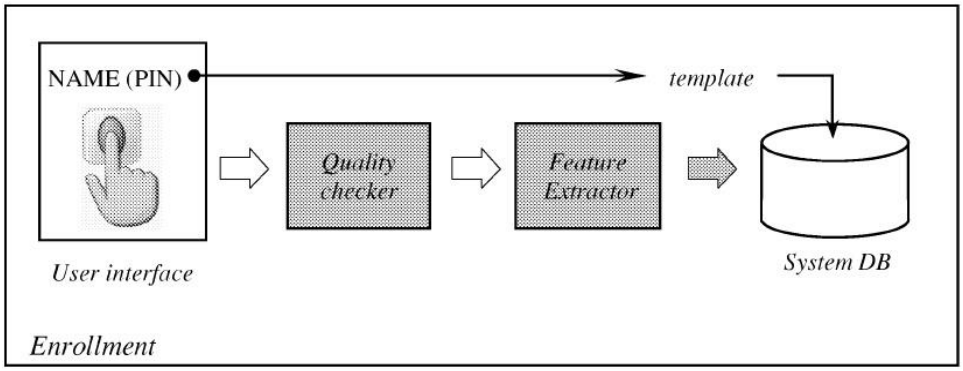

Figure 2.1. Block Diagram of the Enrollment phase

In the Verification mode, a person provides his identity and a Biometric which is compared with his/her reference template. The user claims his identity through a User name, PIN, or Smart card and is verified to check whether the claim is true. The comparison here is one-to-one. A template is loaded from the System Database and then checked against the sample template. Two kinds of errors are possible during the verification phase. The False Reject Rate (FRR) or False Non Match Rate (FNMR) is a condition in which a legitimate user is rejected by the user. The False Accept Rate (FAR) or a False Match Rate (FMR) is the likelihood of an impostor being accepted by the system as a genuine user [26].

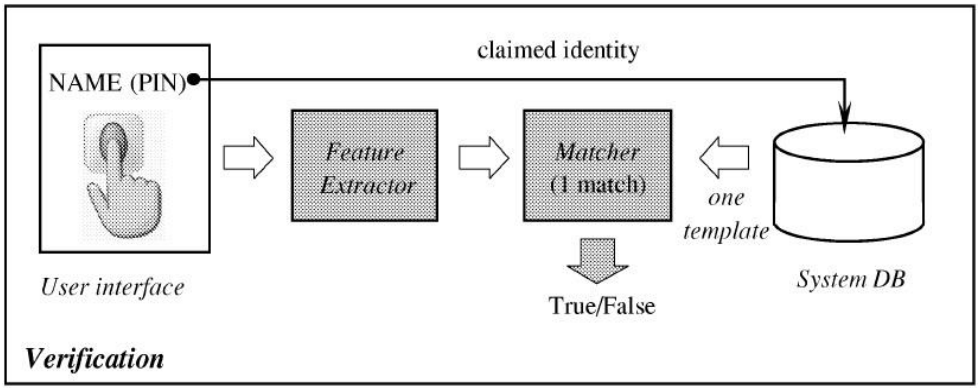

Figure 2.2. Block Diagram of the Verification phase

In the Identification stage, a person's Biometric is compared with all the stored templates for a match. The user need not provide an identity. The comparison here is one-to-many [26].

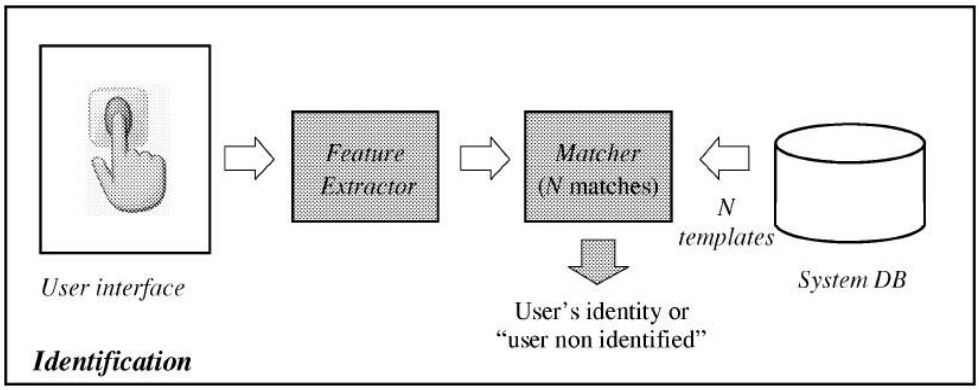

Figure 2.3. Block Diagram of the Identification phase

Source: All three illustrations are adapted from JAIN *et al.*: An Introduction to Biometric Recognition. IEEE transactions on circuits and systems for video technology. Vol 14.1 (2004), 5.

There are many kinds of Biometric technologies and each Biometric has its own advantages and limitations. The choice of using a specific Biometric depends on the application. Any single Biometric cannot meet all the requirements of all the applications. Following are some of the commonly used Biometrics:

DNA:

Deoxyribonucleic acid (DNA) is the unique code for identifying an individual except for the fact that it's same for identical twins. It is mostly used in forensic applications for person recognition. The major limitation is that a DNA sample can easily be stolen from a person without getting noticed [26].

Face Recognition:

Facial images are the most common Biometric characteristic. Humans are personally recognized through their face. The most popular approaches for face recognition include the location and shape of facial attributes like eyes, eyebrows, nose, lips, chin, and their spatial relationships [26].

Hand and Finger Geometry:

This kind of recognition is based on a number of measurements taken from the hand, which might include the shape, size of palm, and length and thickness of the fingers. This technique is simple, easy to implement, and cost effective [26].

Fingerprint:

Fingerprints have long been used by humans for personal identification because of its high accuracy. It's the pattern of ridges and valleys on the surface of the fingertip that are taken into account. It's also inexpensive and easy to use. This is the most widely used Biometric recognition of all. Multiple fingerprints of an individual provides more information and security [26].

Iris:

It is the annular region of the eye surrounded by the pupil and the sclera on either side. During the first two years of life, the visual texture of the iris is formed. A fully developed iris carries very unique information useful for personal recognition. But the system might be expensive and usage might be complex [26].

Retinal scan:

The retinal vasculature is claimed to be the most secure Biometric since it's not easy to change or replicate. The image acquisition requires a person to peep into an eye-piece and focus on a specific spot so that the retinal vasculature can be imaged.

No single technique can outperform all the others in all operational environments. In other words, there is no "optimal" Biometric characteristic [26].

III. DECIDING TO USE A BIOMETRIC TECHNOLOGY

There sure are many advantages of biometrics. It doesn't change over time and cannot be lost or forgot. It is next to impossible to forge a Biometric. It provides a very strong access control security solution satisfying confidentiality, integrity, authentication, and non-repudiation. Aspects like accuracy, reducing costs, user friendly devices, and universality add to the advantages. The user need not remember or carry anything with him which is a great reason to use Biometrics. However, a lot of parameters are to be evaluated before adopting or changing to Biometric system.

A detailed cost-benefit analysis should be performed [29]. All the estimated costs for installing, deploying, and educating the people should be accounted. The different kinds of benefits should be documented. The system should be adopted only if the benefits outweigh the costs. An organization should discuss with their employees, about the effects on privacy and convenience. Everything should be transparent. An employee will accept the system only if he/she has a clear idea of what's going on. Since user acceptance is the major challenge, educating the people about the technology and making them confident should be the company's top priority.

All the type of systems should be taken into consideration and the system which best fits into the organization can be adopted. For example, it won't be feasible to use fingerprints scanning for a job involving usage of gloves by the employees. The employees will have to remove the gloves every time a scan is needed. Also, employees should feel that Biometrics are easy to use and not complex. The Biometric information shouldn't be misused by the organization. Employees should be well aware of how the data is being stored and used. The organization should abide by all the policies and regulations written by the government. The policies should, at minimum, cover Collection, Encryption, Storage, Disclosure, and Protection of Biometric data [2]. The Health Insurance Portability and Accountability Act (HIPAA) [30], the Privacy Act of 1974[31], and Text of the Biometric Information Privacy Act [32] are a few. The importance of the assets which are

being protected should be documented. Biometrics is mostly used in the areas requiring high level of security but is not confined to it [29].

The organizations and public are slowly leaning towards using Biometrics due to the security breaches and inefficiency of the current security measures. Many surveys are being conducted to know the public perceptions about the usage of Biometrics in common places like office, ATM, and for computer logon. The following are the results obtained by Janette Moody in her survey [33].

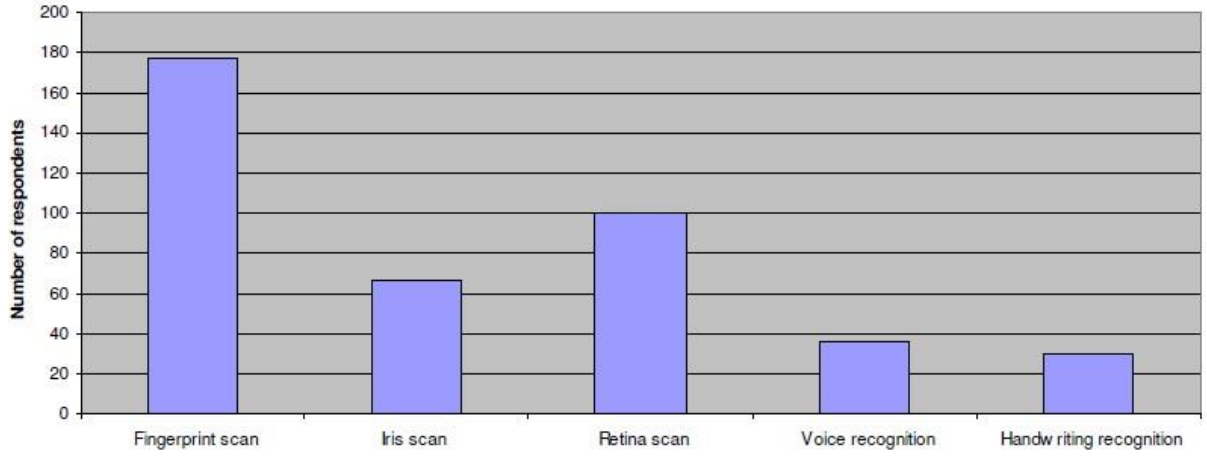

Figure 3.1. Acceptable Biometric for ATM

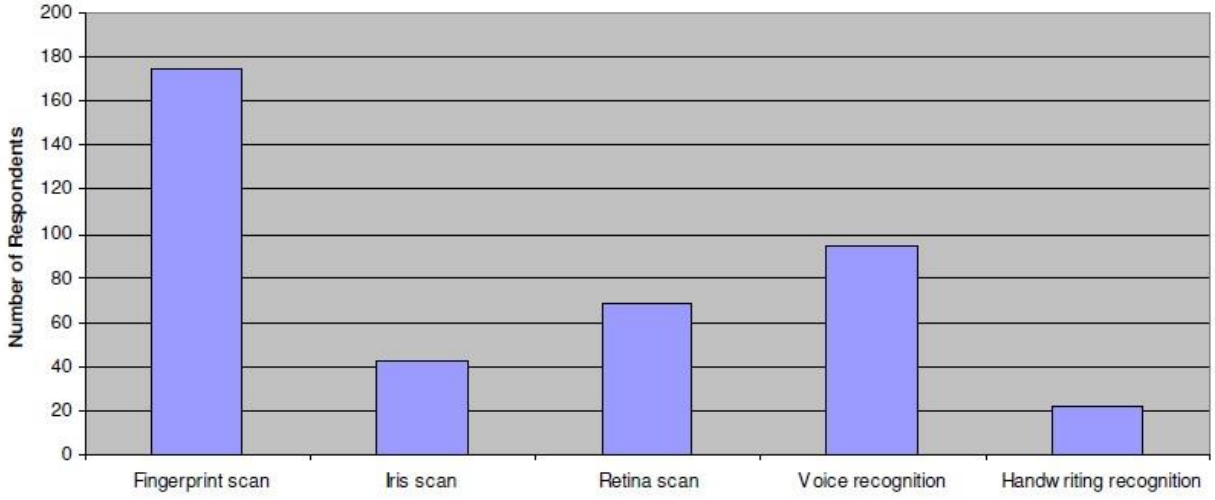

Figure 3.2. Acceptable Biometric for Computer Logon

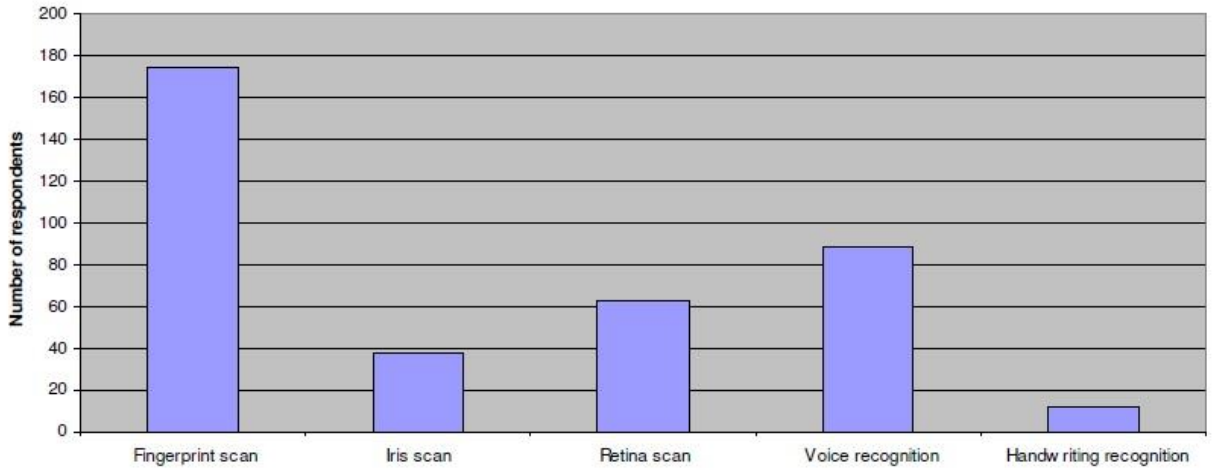

Figure 3.3. Acceptable Biometric for Office Access

From the information present in the above bar charts, it is evident that people are more comfortable using Fingerprint scan in the environments mentioned in the survey. This might be because of the public perception that it is the most easy-to-use Biometric recognition. It is also the most famous and oldest known Biometric. On the other hand, it is easy for the organizations to implement Fingerprint scan because of its accuracy and low expense.

Gone are the days where Handwriting is used for recognition. It is easy to forge and fake. So, there is no surprise that people are not comfortable in using it as a security control. They are also not interested in using iris scan and retina scan. This might be because of their perception that it is complex and that it might cause health problems or blurred vision if used regularly. Users need to expose their eyes to light rays for considerable time during the scanning process. It may be irritating too.

The following bar chart depicts the Biometrics which are considered most uncomfortable to use. In this too, people are uncomfortable using iris scan and retina scan. Next in line is handwriting and voice recognition. People are more comfortable using fingerprint scan like in the previous cases. But the public opinions are diverse and contradictory. This is due to the misinformation and ignorance of the public towards this technology. Some of the respondents have never used Biometrics in their life.

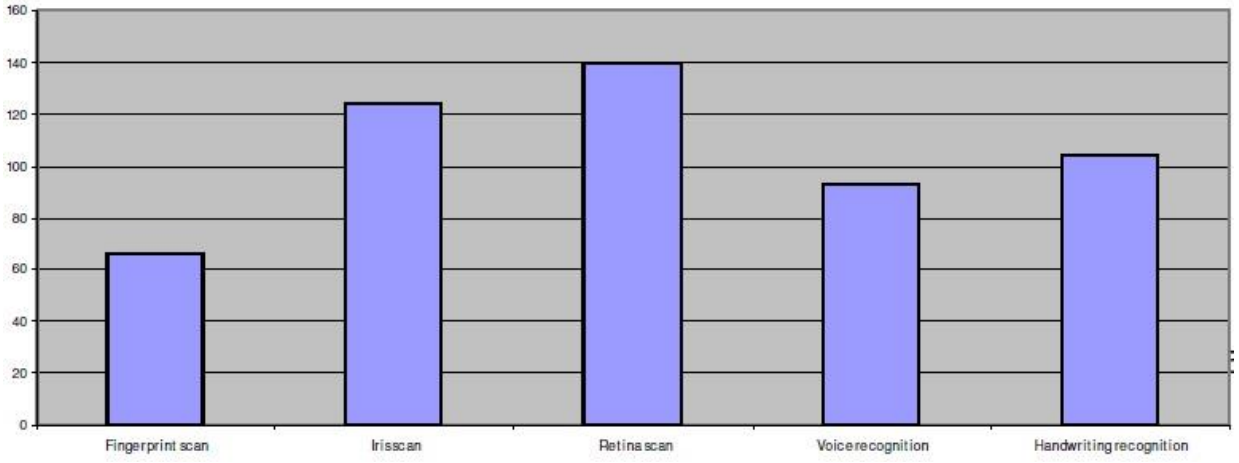

Figure 3.4 Uncomfortable using these Biometrics

Source: All the four illustrations are adapted from Janette Moody: "Public perceptions of biometric devices: The effect of misinformation on acceptance and use." Journal of Issues in Informing Science and Information Technology 1 (2004): 753-761.

IV. CHALLENGES FACED

Privacy and Public Confidence:

Public acceptance is the main reason obstructing the growth of Biometrics. There exists fear among people that usage of Biometrics may lead to invasion of their Privacy (freedom from observation). Different organizations store the information about different Biometric identifiers of people in their databases. They are afraid that some organizations might use this information to track their movements and behavior and also share this information with other organizations for various reasons.

People also think that the government uses this information to track their daily actions and control them completely in the name of fighting crimes and terrorism [2]. This kind of misuse of personal information violates the user's privacy and civil liberty [4]. It is exposed through media that Biometrics are complex and are used only in military organizations requiring high level security. They feel that this level of security is unnecessary in their everyday life due to its complexity. Acceptance of Biometrics may also depend greatly on the culture. In order for Biometrics to gain public acceptance, the hurdles of privacy and its perception are to be conquered [5].

Fake Biometrics:

It is difficult to fake Biometric identifiers but not impossible. Behavioral Biometrics like signature and voice can easily be stolen compared to physiological Biometrics. Although signature is seldom used for security, a person's voice is commonly used. Voice can be mimicked. Fingerprint scanners can be tricked with a silicone finger. A mold or cast of hand can be used to fake hand Biometrics. An image/photo of the face and iris can be used to deceive the Biometric scanning systems. Iris can be faked using a contact lens also. All these techniques of faking Biometrics should be eliminated.

Biometric identification consists of two stages – Enrollment and Verification [6]. The Biometric is converted to a template using an algorithm and then stored. In the verification stage, a person presents his identity and the Biometric. During the enrollment stage [14], a person can provide fake documents as identifiers and once the new fake identity has been accepted by the system, a person can engage in a lot of illegal activities.

Theft of Biometric Data:

Theft of Biometric data is another serious problem. The advantage in using Biometrics is that the Biometric identifiers don't change over time. Ironically, the advantage of Biometrics can become its greatest disadvantage. Biometric data once compromised can be a serious issue through the life time of an individual because it is difficult to replace a Biometric unlike a password or a credit card. Biometric is nothing but a binary file which is stored in the database and can be stolen by a hacker like any other file. The attacker can use it anywhere else. If Biometric data of a person is stolen, the organization should replace the entire Biometric system (e.g. fingerprints to iris) just for a single user to avoid security breaches. Replacing a complete system is time consuming and expensive. Another drawback is that a person has only limited Biometric Features.

Ease of Use:

This problem is closely related to the public acceptance of Biometric devices as security systems. One advantage of Biometrics is that a person need not remember or carry anything with him/her. But, user acceptance can only be obtained if the Biometric devices are convenient to use and operate. This convenience should not be provided at the cost of security [2]. An administrator

must know the functionality of a Biometric Device. He/she should be able to solve minute problems that occur at the time of authentication.

Some users might not be comfortable in using their physiological characteristics as a source of authentication. Some think that the radiations and light beams that are emitted during the scanning of fingerprints, hand, face, iris, and retina are harmful for the skin and might affect ones hygiene. The Biometric devices on which the fingers and hands are placed may contain germs and might cause health problems. Since, everyone uses the same Biometric device, disease from one person might be transferred to others as well. So, the public might not be ready to use the device. People might not know the working process of Biometric authentication and may think that they are too complex to use. They might also feel that the devices are not secure unless they know the storage procedure. The devices may not work properly all the time due to various reasons and the user might need to make numerous attempts before getting authenticated, which is annoying. In case of retina or iris recognition, the user may need to keep his/her eyes open for 10 to 15 seconds while being exposed to light which may be uncomfortable [15]. These types of recognitions are time consuming also and may not be encouraged.

Environmental Factors:

The working of Biometric devices may be adversely affected by the environmental conditions. For voice recognition, the surroundings must be noise-free. For fingerprint recognition, the fingers must be clean. Sweat and/or any other material like food, drinks when present on the fingers/skin might hinder the performance and efficiency of fingerprint/hand recognition devices. Humidity and temperature might also play a part. Sufficient amount of light is to be present while scanning the face, iris, and retina [16]. If the threshold of the device is decreased to make it work in these kind of conditions, security might be breached.

Physical Factors:

There might be a case where the user might be unable to enroll in the Biometric device due to some disability or limitations in physical characteristics. This is called Failure to Enroll (FTE) [17]. In case of diseases like arthritis, where motion of the body parts is limited, a person might not be able to place his/her hand on the device [18]. People with wounds or bruises on their skin might also be denied access because of the inability of the scanner to scan.

A change in the physical characteristics of a person might affect the scanning procedure. A scanner might not recognize the person if his/her hairstyle, facial hair, headwear is changed. The position of the scanner should be altered based on the height of the person in case of face, iris, and retina recognition. A significant weight loss may drastically change a person's face [16].

V. SOLUTIONS

Educating Public about Biometrics – Solves Public Acceptance and Ease of Use problem:

As with the introduction of any new technology, user participation and acceptance is essential. Organizations deciding to install Biometric devices would be well served if they conduct a survey on their employees in advance, to determine where their misperceptions and apprehensions might exist, if any. After extracting the facts from this information, an education program could be undertaken to specifically address their concerns. Prior to investing in any new technology, it is sensible to determine not only if it is financially and technologically viable, but also if it is functionally appropriate. Educating the public about Biometrics will help greatly to solve many problems and help in the growth of this industry. The society's misconceptions about the security, privacy and working of the technology can be eradicated through providing adequate education regarding the technology. Education definitely improves public confidence and acceptance of Biometrics. People shouldn't feel that there are too many unanswered questions in using Biometrics [22]. People are understanding the wide use of technology and can introduce certain risks to individual privacy. So, the business organizations should understand this and introduce policies and develop some assurance models of privacy protection for their customers. This raises the need for understanding Biometrics from both the individual's and organization's perspective [23].

An informed public-policy debate about Biometrics is necessary. Clear discussions about the capabilities and limitations of every Biometric system should be made. Government and security organizations should make people understand where Biometrics should be deployed, and where they should be avoided. Biometrics is mostly used by the government and federal organizations which are bound by privacy laws and regulations. Public should be educated about these laws and should feel comfortable to cooperate [24].

Testing the liveliness of a Biometric – Eliminates Fake Biometrics:

Despite the fact that certain biometric devices can be broken under some conditions, it is implausible to fool the devices used today through simple forgery of a fingerprint, picture of a face, or a recorded voice [7]. All the modern day devices should make a provision for one more step in addition to scanning the Biometric to prevent forgery. Fingerprint or hand biometric devices may check for the blood flow or movement of fingers to avoid artificial devices. Devices may even check for the material (Skin, Silicone, and Plastic) used during verification. Voice recorders may ask the persons to speak random phrases which can avoid recordings. It is possible to mimic but impossible to exactly duplicate a person's voice. In case of face recognition, a person is asked to change their facial expressions or nod his/her head. During iris recognition, the brightness of the light can be varied to check for the pupillary response [8].

Centralized Biometric databases can also solve the problem of fake Biometrics. Different organizations use different kinds of Biometric authentications. If all the databases of these organizations are linked through certain policies, a person can be asked to submit one more Biometric trait (Multi factor Authentication) to invalidate fake Biometrics. The policies established should ensure privacy of people and security.

Encryption, Centralization, Multimodal Biometrics and Revising Algorithms – Solves the Problem of Theft:

The fact that a Biometric cannot be changed makes the theft of Biometric data a problem of top priority. Certain algorithms are used by organizations to convert the Biometric into a Binary file which is stored in a database. There should be people supervising and safeguarding the Biometric Devices and databases. These databases should be placed in inaccessible locations. Even if an attacker has the data, the corresponding Biometric cannot be regenerated with this data unless the algorithm is known. Once the attacker gets the algorithm used for conversion, he can make use of the stolen information.

So, one way of protecting the stolen data is to use complex algorithms which are difficult to crack. It's also a good practice to change these algorithms at random intervals. Another way is to encrypt the saved data so that it'll be impossible for the hacker to decrypt and use it. Instead of saving the Biometric information as binary data, it can be hashed using any hashing algorithm and then saved as a reference string. While verification and identification, the sample template should again be converted into a hash value and then be compared with the reference value. Thus, the

direct access to binary data can be prevented. The branch dealing with the encryption of Biometric data is called Biocryptics [34]. Many ways to protect the Biometric Data have already been proposed (e.g. [10], [11], [12], and [13]). Multimodal Biometric systems [9] can also be used to solve this problem. These systems demand the user to submit more than one random Biometrics for authentication. This is similar to two factor authentication. So, the attacker should have all the Biometrics of a user in order to gain access.

One more solution is to centralize all the Biometric data which is mentioned in the previous section. Each organization has to invest a lot of capital to store the data and to secure it. Instead of maintaining separating databases, all the organizations can store the Biometric data in a single safe location. This location can be provided with the highest level of security. These organizations can be divided into groups and access to data can be provided based on these groups.

Ensuring Cleanliness before using a Biometric Device – Mitigates Environmental Factors:

People should be educated about the conditions in which a Biometric device can be used. An instructor should be present at the location where the scanning is being done and should ensure trouble free scanning. In the jobs involving usage of chemicals, construction work, or mechanical works, a person's hand will be smeared with dirt or grease. He should clean his hands before fingerprint or hand scanning. Notices and instructions can be put in an obviously visible position so that the user can go through them before moving forward for scanning.

Solving the problem of Physical factors:

There is no solution except to exclude a physically challenged person from the authentication process. He/she should be provided with some other means of authentication. It is important for the organization to make differently abled people comfortable so that they won't feel alienated. An alternative authentication process should also be installed for people with minor physical damages like bruise or wounds.

Advanced systems should be developed so that any changes in the physical characteristics like aging, hair, facial hair, and weight doesn't affect the scanning process. These kind of systems are already developed and in use. There are methods which can predict the changes in the characteristics of face with age [25]. Using some applications, faces can be identified even if there

is a change in facial hair, make up etc. These methods and applications can be used to develop the advanced Biometric devices.

VI. CONCLUSION

Biometric technologies are widely used in the public sector and the private organizations are yet to adopt it in large scale. With the problems faced in password based and token based security systems, Biometrics is definitely the future of security. But the Biometric system of the present day is still immature. Even though Biometrics is the principal method for physical security, research is still being done. It is being combined with other branches of security (e.g. Biocryptics) and a huge amount of money is being put in this field by the government. A lot of questions are to be answered for the technology to be universally existent. In this paper, I have tried to address some of the issues faced in this field. The factors responsible for these issues are analyzed to come up with the solutions. Though the solutions provided are not completely feasible and may depend greatly upon the application and organization, it can be a start for finding more concrete methods to overcome the problems. Advanced research is needed to improve the existing technologies and also invent new methods.

REFERENCES

[1] “Fast Facts”, Biometrics.gov, http://www.biometrics.gov/mediaroom/fastfacts.aspx (accessed October 11, 2014).

[2] Lee Eng Chuah, “The Future Challenges of Biometrics”, GSEC Practical Assignment Version 1.4 (July 25, 2002), http://www.giac.org/paper/gsec/2145/future-challenges-biometrics/103654 (accessed September 19, 2014).

[3] Coskun, Baris, and Cormac Herley. "Can “Something You Know” Be Saved?" In *Information Security*, pp. 421-440. Springer Berlin Heidelberg, 2008.

[4] El-Abed, Mohamad, Romain Giot, Baptiste Hemery, and Christophe Rosenberger. "A study of users' acceptance and satisfaction of biometric systems." In *Security Technology (ICCST), 2010 IEEE International Carnahan Conference on*, pp. 170-178. ieee, 2010.

[5] Mark W. Wolansky, “Stronger Authentication Methods: Biometrics and Public Accpetance”, GSEC Practical Assignment (Version 1.2b), http://www.giac.org/paper/gsec/628/stronger-authentication-methods-biometrics-public-acceptance/101398 (accessed September 17, 2014).

[6] Soutar, Colin, Danny Roberge, Alex Stoianov, Rene Gilroy, and Bhagavatula Vijaya Kumar. "Biometric Encryption: enrollment and verification procedures." In *Aerospace/Defense Sensing and Controls*, pp. 24-35. International Society for Optics and Photonics, 1998.

[7] Samir Nanavati, Michael Thieme, and Raj Nanavati, “Biometrics: Identity Verification in a Networked World”. John Wiley & Sons, 2002.

[8] Daugman, John. "How iris recognition works." *Circuits and Systems for Video Technology, IEEE Transactions on* 14, no. 1 (2004): 21-30.

[9] Ross, Arun, and Anil Jain. *Multimodal biometrics: An overview*. na, 2004.

[10] Hartung, Frank, and Martin Kutter. "Multimedia watermarking techniques." *Proceedings of the IEEE* 87, no. 7 (1999): 1079-1107.

[11] Ratha, Nalini K., Jonathan H. Connell, and Ruud M. Bolle. "Secure data hiding in wavelet compressed fingerprint images." In *Proceedings of the 2000 ACM workshops on Multimedia*, pp. 127-130. ACM, 2000.

[12] Gunsel, Bilge, Umut Uludag, and A. Murat Tekalp. "Robust watermarking of fingerprint images." *Pattern Recognition* 35, no. 12 (2002): 2739-2747.

[13] Jain, Anil K., and Umut Uludag. "Hiding biometric data." *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 25, no. 11 (2003): 1494-1498.

[14] Chinchilla, Regoberto. "Ethical and Social Consequences of Biometric Technologies". American Society for Engineering Education. 2012.

[15] "Retina Biometrics", Biometric Systems and Solutions, http://www.biometricnewsportal.com/retina_biometrics.asp (accessed October 16, 2014).

[16] Lease, David R. "Factors influencing the adoption of biometric security technologies by decision making information technology and security managers." PhD diss., Capella University, 2005.

[17] Ashbourn, Julian. *Practical biometrics: From aspiration to implementation*. Springer, 2004.

[18] "Arthritis of the hand", American Academy of Orthopaedic Surgeons (AAOS), Last reviewed December 2013, http://orthoinfo.aaos.org/topic.cfm?topic=a00224 (accessed October 15, 2014).

[19] Hogan, Mike. "Body Language", Entrepreneur, Entry posted March 15, 2001, http://www.entrepreneur.com/article/37810 (accessed October 10, 2014).

[20] "Introduction to Biometrics", The Biometric Consortium, http://www.biometrics.org/introduction.php (accessed October 10, 2014).

[21] Connolly, P.J, "Future Security May Be in the Hands, or Eyes, of Users—By Eliminating the Need for User Passwords, Biometrics Will Tighten Networks and Save Big IT Money", InfoWorld, Entry posted October 16, 2000.

[22] Green, N., and G. W. Romney. "Establishing public confidence in the security of fingerprint biometrics." In *Information Technology Based Higher Education and Training, 2005. ITHET 2005. 6th International Conference on*, pp. S3C-15. IEEE, 2005.

[23] Penny, Wayne, "Biometrics: A Double Edged Sword – Security and Privacy", GSEC Certification Practical 1.3 (2002), http://www.sans.org/reading-room/whitepapers/authentication/biometrics-double-edged-sword-security-privacy-137 (accessed October 16, 2014)

[24] Patrick, Andrew. "Acceptance of Biometrics: Things that matter that we are ignoring". National Research Council Canada. International Workshop on Usability and Biometrics. June 2008.

[25] Scherbaum, Kristina, Martin Sunkel, H-P. Seidel, and Volker Blanz. "Prediction of Individual Non-Linear Aging Trajectories of Faces." In *Computer Graphics Forum*, vol. 26, no. 3, pp. 285-294. Blackwell Publishing Ltd, 2007.

[26] Jain, Anil K., Arun Ross, and Salil Prabhakar. "An introduction to biometric recognition." *Circuits and Systems for Video Technology, IEEE Transactions on* 14, no. 1 (2004): 4-20.

[27] Ed German, "The History of Fingerprints", http://onin.com/fp/fphistory.html (accessed October 14, 2014).

[28] "Unique Identification Authority of India (UIDAI) issues 56 crore Aadhaar Numbers", Press Information Bureau, Government of India, Planning Commission, entry posted January 16, 2014, http://pib.nic.in/newsite/PrintRelease.aspx?relid=102540 (accessed October 16, 2014).

[29] Keith A. Rhodes, "Challenges in using Biometrics", Information Security, United States General Accounting Office, 2003.

[30] "The Privacy Rule", US Department of Health and Human Services, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/ (accessed November 10th, 2014).

[31] "Privacy Act of 1974". Office of Privacy and Civil Liberties. The United States Department of Justice. http://www.justice.gov/opcl/privacy-act-1974 (accessed November 10th, 2014).

[32] "Biometric Information Privacy Act". www.govtrack.us. https://www.govtrack.us/congress/bills/113/hr4381/text (accessed November 10th, 2014).

[33] Moody, Janette. "Public perceptions of biometric devices: The effect of misinformation on acceptance and use." *Journal of Issues in Informing Science and Information Technology* 1 (2004): 753-761.

[34] Mjaaland, Bendik, Danilo Gligoroski, and Svein Knapskog. "NISK2009-Biocryptics: Towards Robust Biometric Public/Private Key Generation." *Norsk informasjonssikkerhetskonferanse (NISK)* (2009).