Chapter 21
Ethical, Legal, and Social Implications of Biometric Technologies

Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, and Mohammad S. Obaidat

1 Introduction

Personal identity of a human being is important due to several reasons. From a group point of view, as we narrow down the regions from a country to village routing, cities, and districts, individual communities desire to have their independent identities [1], whereas from an individual point of view, as the population is increasing, an individual tries to locate himself in the stereotype locations. This type of desire indicates his individual identity. However, another level of identity is also existing, which includes the validation of the identity. For any situation, this is very important in almost all situations like mobility domain, stationary domain, hospitals, residential areas, industrial areas, educational areas, and political, financial, and legal areas [2].

S. Tanwar (✉)
Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India

S. Tyagi
Department of Electronics & Communication Engineering, Thapar Institute of Engineering and Technology Deemed to be University, Patiala, Punjab, India

N. Kumar
Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology Deemed to be University, Patiala, Punjab, India

M. S. Obaidat (✉)
ECE Department, Nazarbayev University, Astana, Kazakhstan

King Abdullah II School of Information Technology (KASIT), University of Jordan, Amman, Jordan

University of Science and Technology Beijing (USTB), Beijing, China

Fordham University, New York City, NY, USA
e-mail: m.s.obaidat@ieee.org

M. S. Obaidat et al. (eds.), *Biometric-Based Physical and Cybersecurity Systems*,
https://doi.org/10.1007/978-3-319-98734-7_21

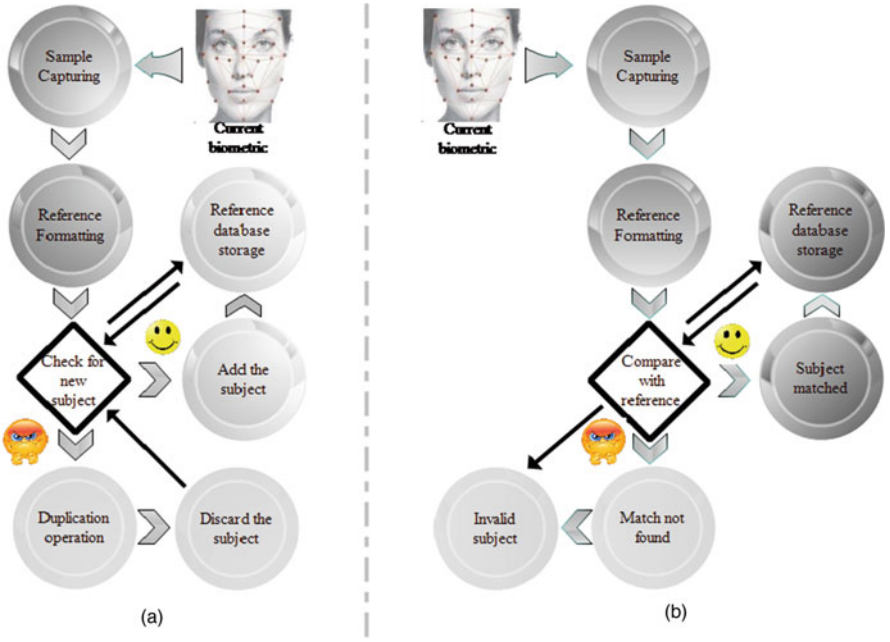


Fig. 21.1 The use of biometric technology. (**a**) Enrollment process. (**b**) Matching process

One of the interesting aspects in biometric schemes is how to execute the entire process. A detailed execution is illustrated in Fig. 21.1. Two segments have been shown, where Fig. 21.1a shows the performing of enrollment process and Fig. 21.1b shows the matching process. Enrollment process maintains a biometric data record and stores the same in a reference database. In this process, biometric sensors scan the current biometric and do the reference formatting. Now task manager checks to find out if the current subject is new or already exists. For existing subject it activates the duplication action that is discarded by the task manager, whereas new subject is stored in the reference biometric database. On the other hand, for matching process and after biometric scanning, the system performs capturing and reference formatting [3]. Now, verification compares captured/formatted biometric samples against previously stored biometric samples. Identification compares on one-to-many basis. If there is a match, this means that we have positively acknowledged and, for the situation where match is not found, this means a negatively acknowledged situation signaled to the task manager [4] on the basis of which appropriate action can be taken. Sometimes mismatch may occur due to poor performance of biometric sensors; therefore advanced check may be applied before taking the final decision [5, 6]. This process extracts a unique biometric identifier like face capturing from the raw biometric data. Different biometric identifiers are also available and are represented in Fig. 21.1.

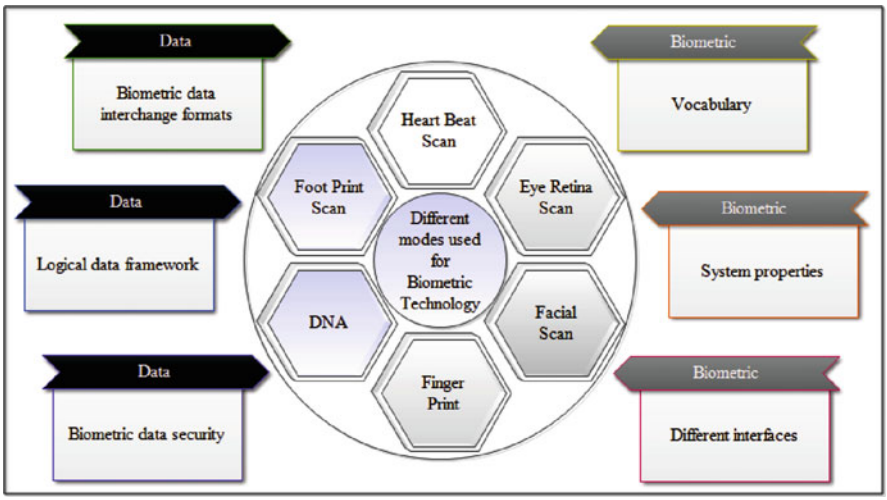


Fig. 21.2 Different modes used for biometric technology and essential stack

Fingerprint scanning, facial scanning, DNA, and eye retina scanning are frequently used biometric scanning schemes. Figure 21.2 shows different biometric scanning schemes. Fingerprint and facial scanning are most popular among the smartphone users, as using special characters and remembering lengthy password is a tedious task. The smartphones of Samsung Galaxy, Moto series of Motorola, latest version of iPhones, Oppo, and some other popular smartphones have the security option of fingerprint and facial scanning. Smartphone fingerprint readers are usually placed at the backside of the handheld device so that single-handed biometric authentication can easily be done [7]. A front-end camera has been used for the facial scanning. Out of these two, fingerprint scanning as a biometric authentication is a very easy and secured option and is considered an effective replacement to traditional password, whereas on computers and laptops, this is not a new concept; in fact banks are using this technique very commonly these days [8].

The iris of the human eye is a very interesting component of the biometric scanning technology. In medical science the circular region between the sclera and pupil is known as the iris. The iris is one of the stable biometric techniques [9] as it is stable over the long life of a person starting from childhood. The iris has very high pattern changeability between the twins and even two eyes of an individual. Due to this feature, nowadays, smartphones are also using this biometric technique for authentication access. However, this facility is available to the smartphones having high quality of front camera because iris recognition system has also a lot of challenges.

DNA has the structure, which is responsible for the body, cells, tissues and organs, and body components. Every individual has a unique composition, and verification sample can be taken from any part of body, like hair, blood cell, or nail, for the DNA testing. Definite areas of DNA contained chain that repeats it on

regular interval, and interestingly different persons have a dissimilar number of repetitive sections. The least building block of DNA is called the nucleotide [10], and every nucleotide has a dioxide ribose base and phosphate group. When one is analyzing the structure of DNA for identification, then we look at the sequence of bases. Heart beat scan and footprint scan are also two possibilities for biometric scanning methods, but their applications are less as compared to the other schemes discussed above. Two important stacks data and biometric are shown in Fig. 21.2. Appropriate data acquisition system is required for proper formatting. Logical stack is required for perfect matching as false matching will create the security issue. In Fig. 21.2 meaning of vocabulary is biometric samples of different subjects.

2 Legal Implications of Biometric Technologies

In order to prevent the fraud, now governments are using biometric technologies like fingerprint, face recognition, and iris, which can be used in government official documents such as LPG gas services and Passport Seva Kendras. The latter is an Indian service that aims at delivering passport services to citizens in a timely, transparent, more accessible, and reliable manner and in a comfortable environment.

As time passes corporations in city are also using biometric technologies for their services in order to provide better services to the citizens of country in a timely and uninterrupted manner. Business organizations can also use the biometric technologies in their workplace to provide secure access control. But there exist the legal challenges while using the biometric technologies by both public institutions (government, corporations, etc.) and businesses. In Europe, with the use of biometric technologies, the most important legal challenges are in the extent of conformance to privacy and data protection mechanisms. To overcome it, the European Bio Sec consortium is working to develop a legal framework that ensures use of biometric technologies with full compliance as per European regulations to protect data.

Legal issues include the lack of precedence, ambiguous processes, imprecise definitions, and logistics of proofs and defense, as shown in Fig. 21.3. Main problems here are the type of information collected about individuals and how this can be used. Moreover, the ability to access information and reparation inaccuracies,

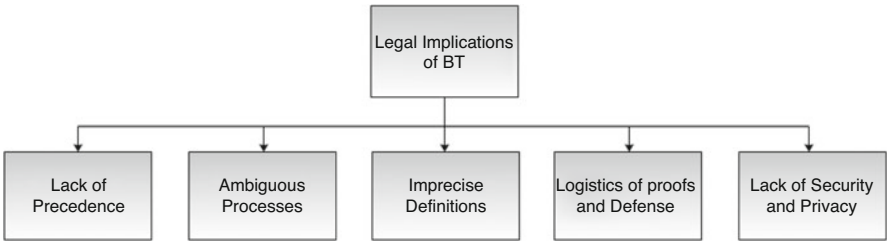


Fig. 21.3 Legal implications of biometric technologies

and providing secure mechanisms so that information related to the users cannot be compromised, especially while enrollment process of biometric schemes going on and throughout data transmission over public networks. Approaches used for storing biometric templates remain a critical issue, because RFID chips are used by users to process their information on smart card. Some challenges such as emergency procedures used during the time of failure in automatic technology processing need to be taken care.

Even though many biometric legal proceedings have been showed at global level, so far there are a few large-scale schemes operating in full swing. In some of the cases that have been conducted, they actually have been found to be illegal and in breach of users' fundamental rights. For example, if biometric project given to any data protection agency for use of biometrics stored on physical devices and for controlling physical access to the secured areas in some predefined applications (like airport, hospitals, etc.) were in proportion with the use for which the data was collected, it may be feasible that the collected data can be used for time and attendance control in that application was in breach of its data protection laws. In another example that highlights the legal challenges in the use of biometrics in ID cards for overseas residents, here one can claim that the technology targets a specific group. Another legal challenge associated with use of biometric technology is ensuring that rights can be given to citizens to correct information held about them, because biometrics contains mechanisms for identification and authentication purposes. Individual identity theft is a rising problem, and, even though the bulk of such theft is still done using offline methods, the probability of online identity theft is increasing rapidly. Without providing appropriate solution, the owner of the data has fear that his/her data is not safe and he could not get back the control of his identity and feels that the biometric data fall into the wrong hands. Further details regarding the legal issues in the use of biometrics can be found at [3].

Each citizen of the country has the right to decide in principle which personal information related to his/her can be posted on the social sites. The processing of data needs to be based on legislations. It is always advisable to use the personal collected data for specified purposes; data must not be processed to any third party without taking the permission from the user; otherwise it clearly violates the rule of personal privacy [47]. Moreover, there should be significant restrictions for the use of "personal/sensitive" data. For example, there exist some standard legal challenges, which can be followed by each country of the European Union. All security applications cannot be just based upon the collected data because preventive police measure will also play an important role here along with or without notice period. Keeping above points into consideration, there is an urgent need to fix up the legal boundary over the processing of biometric data. Like in Germany [11], it is very difficult to predict the usage of existing police system, and the data protection laws allow the ease use of biometrics in structured manner. In contrast, this may be feasible during the investigation of criminal case using fingerprints of persons individually.

In defensive situations, such as the scanning of baggage at the airports and personal monitoring as well as tracking of visitors through smart CCTV systems,

however, no final outcome about any criminal person is established before processing his personal data. It has been noticed from the literature that upgrading in biometric systems emerged to new challenges for personal privacy and protection of data. These new upgrades highly depend on the new used technical design. Biometric technology helps the enforcement officers to take appropriate decision on the accused, based on automated collected biometric data. Enforcement officers also proactively collect the information about the unspecified group of persons, whose activities are not normal. Hence, the complete society will be under trouble without proper legal and technical safeguards. Further, data collection centers may require proper attention to the data so that user can decide when and at what situation he/she behaves freely without worrying about the interpretation of that behavior at the other end of the surveillance system.

2.1 Legal Perspective of Biometrics with Reference to Enforcement Officer

Error rates can be taken into consideration by the users of the biometric technologies for law enforcement purposes. From this it has been clear that police measures on the basis of biometric can not only play final role to put any person under suspicion, but police legislator along with the view of executing officer plays final role to put any person under suspicion.

The function of the law – particularly the fundamental rights to privacy and informational self-determination, as well as the respective data protection acts – needs to be the protection of the personal rights of the data subjects. To this end, specific provisions for certain application scenarios may be necessary in the future. Furthermore, a legally compliant technology design is able to significantly reduce privacy and data protection risks.

2.2 Main Legal Issues Associated with the Use of Biometrics

The main concern associated with the use of biometrics is the violation of privacy. Citizens of the country who had undergone to the biometric scan feel that such procedures are disturbing because they involve scanning of body parts. Another major concern is the matter of information security. Collected biometric data are usually stored in databases/clouds that can be accessed by the employer of the company, if the data is related to the organization, and can also be accessed by the government officials. But the question that comes here is what is the secrecy of this data, as this contains private information such as medical history of patients and bank data. If any person raised any legal issue regarding process of security of biometrics, then it is usually resolved using a traditional balancing test. Outcome of

this test is the privacy rights. A court will consider the person's belief of privacy versus the public need to obtain such information. For example, consider a court that wants to analyze any person's handwriting skills for national security reasons. As the public concern for national security has high priority, then a judge might conclude that it is essential to assess the handwriting skills of that person in order to protect the security of the nation.

2.3 Futuristic Vision of Biometrics

Biometrics is rapidly changing from fiction to fact. Consider that Fast Identity Online (FIDO) Alliance, which has members like Google, Microsoft, Visa, and Mastercard, recently came with a final draft regarding its biometric standards; final note of this draft is that "today, we celebrate an achievement that will define the point at which the old world order of passwords and PINs started to wither and die." Progressively, Microsoft's new Windows operating system – Windows 10 – may drain passwords altogether and rely on biometric technologies, like face, iris, and fingerprint recognition, that are used to not only log you into your machine but also to "authenticate apps and websites without sending a password at all" [12].

For example, consider any person holding a glass of water for your biometric data. We can say that your body parts are your password; demanding a glass of water (user voice recorded), picking up the glass of water (user fingerprint captured), drinking the glass of water (the DNA in user saliva saved), and then walking back to your four-wheeler parking (user face captured by camera) are all possibly near to handing out user password on a business card to everyone that passes by.

The other legal issue associated with the biometric technology, consider that a hacker during the press conference has taken the photos of Cabinet Minister of any country from 8 feet way with high-resolution camera and was perfectly able to reproduce the fingerprints of Cabinet Minister, or consider a criminal who was sentenced on DNA that was taken from the armrest of the chair where he was sitting during the period of interrogation. It will be crucial for the law officer to keep the collected biometric data to be properly secured because large segment of the people wants to keep the DNA profile private. People want to conduct their biometric impressions in a secure environment. In a society, your biometric collected data and potentially your identity are at the danger of being exposed. For the abovementioned reasons, biometric data needs to be properly secured.

2.4 Category of Biometric Security

According to legal perspective, two categories of issues for biometric security can be explored. First, level of extent to which user wants to secure his biometric data? Consider an example, if the employer of an organization provides me the access of

local cloud drive that contains some confidential documents and also secures that account with a password. If I pass this password to my department colleague in the organization, then after sometimes several security issues could arise. But, at the same time, if employer secures the account with my fingerprints or iris, in this situation employer is thinking that his system is safe until unless I do not misuse the system. But at the same time from my prospective, I have to be more focused about duplication of my fingerprints and picture of iris. Therefore, in order to maintain the security of the organization, I may have to wear the gloves and required the goggles all the time in my office. Second, at what extent can the users be granted to secure their captured biometric data? Consider an example, when you are in market your picture can be taken. But at the same time, can the freedom available to you force the person to stop taking your picture or force them to destroy all already taken pictures based upon your choice for protecting your collected biometric data?

2.5 Biometric Data Protection

It is up to end user to decide the mechanism of how to protect the biometric data of end users. It is not easy to handle the legal issues associated with the biometrics, but the actual fact is that law is not alone adequate to address all the legal issues as mentioned in previous section. Companies need to set up their own policies and producers for preventing the collected biometric data from being misused. Possibly, the most critical question to be asked is: how can I provide security to the biometric data that give appropriate solution to my problems instead of creating new ones? For proper guidance regarding current or potential legal issues, you may contact respective attorney of your city as soon as possible to obtain proper advice, direction, and illustration.

3 Biometric Technology in Government Use

Nowadays, there is a rapid increment in the use of biometric technology by government agencies worldwide. Several components of biometric technologies like posture identification through facial recognition are very much popular and effective to identify the criminals in huge public places [13, 14]. With the utilization of this method, governments can upgrade their database by identifying people in different situations. In the USA after September 11 attack, security has become a primary concern as well as a challenging issue. At that time US Transportation Security Administration (TSA) has proposed a complete body scanning mechanism to be implemented on all international visitors. A detailed list of abbreviation and their meanings is given in Table 21.1. But this process violates the civil liberties. This process required the nude images of an individual and that should be stored somewhere to maintain the biometric database, and there is no guarantee that the

Table 21.1 List of abbreviations and their meanings

Abbreviation	Description
DNA	Deoxyribonucleic acid
UIDAI	Unique Identity Authority of India
LPG	Liquid petroleum gas
RFID	Radio-frequency identification
ID	Identity
CCTV	Closed-circuit television
BT	Biometric technology
FIDO	Fast Identify Online
TSA	Transportation Security Administration
BSSCs	Biometric social security cards
US	United States
EU	European Union
VIS	Visa Information System
EUROSUR	European Border Surveillance System
SIS	Scheme Information System
SIENA	Secure Information Exchange Network Application
INS	Immigration and Naturalization Service
BFA	Basic Facility of Aliens
DAA	Dutch Alien Act
DPDPA	Dutch Personal Data Protection Act
DPDA	Dutch Policy Data Act
CJCN	Criminal justice chain number
CJCD	Criminal justice chain database
BN	Biometric numbers
HF	Human factor
AU	Authorization unique
TBSP	Total Biometric System Performance
FC	Function creep
FRS	Facial recognition system
NBC	National Biometrics Challenge report
OECD	Organization for Economic Co-operation and Development
NSTC	National Science and Technology Council
IPTS	Institute for Prospective Technological Studies
UID	Unique identification
CIDR	Central Identities Data Registry
RoI	Resident of India
KYC	Know your customer
ABIS	Automated Biometric Identity Subsystems
BSP	Biometric service provider
RDD	Rural Development Department
CSs	Civil Supplies
CAD	Consumer Affair Department

(continued)

Table 21.1 (continued)

Abbreviation	Description
MOUs	Memorandum of understandings
CIDR	Central Identity Repository
CSF	Critical success factor
ATV	Ability to verify
3CFA	Credit Contracts and Consumer Finance Act
CGA	Consumer Guarantee Act
PA	Privacy Act
FTA	Fair Trading Act
CECMA	Contract Enforcement and Contractual Mistakes Act
Bio-Sec	Biometric-Security Project

images are always secured. Another possible solution in this area was to use the biometric social security cards (BSSCs) to prevent prohibited visitors to enter the USA. In case of fake BSSC, the culprit has to be punished like if visitor have the visa for his job, then job could be discontinued, and visitor has to leave the USA. In addition to this, visitors and US resident and citizens biometric database cannot be placed together as there is always a chance to misuse the same.

3.1 The Social Implications of Biometrics

Let us consider the spectrum of all available security technologies. This comprises everything ranging from both perspective of hardware and software. For example, it includes hardware devices such as network connecting devices, switches, routers, smart cards, etc. Regarding software, it includes small patches, auto-upgrades, and antivirus mechanisms, among others. When both hardware and software items are positioned and installed, there is no query about their effect on the end user [15]. It is presumed that the end users will perform their related tasks and at the same time prevent the system from cyberattacks to occur. But, nowadays, after the inclusion of biometric technology in these systems, it often gets questioned, not from the angle of its capability to strengthen the lines of protection of a business, but also its effects to the end user. One of the popular and interesting questions can be asked at this step is what is the reason behind its popularity? What are the reasons of more concern of the individuals and what will be the next step after their fingerprint is scanned? The primary reason behind asking these questions has to do with our physiological or behavioral effects, which are being captured. We do not have any control over this, and actually, the individual/citizen does not know how this information is being processed by the biometric devices.

In real sense, it looks like a black box, where no knowledge about the process is happening in between, which results in hindrance in the acceptance of biometric technology, especially in the United States of America, where 9/11 attacks took

place. However, there are other countries in the world where biometric technologies are extensively adopted, especially in the lesser developed nations. The next section will cover the comparative study of acceptance rate of this technology in the USA and other parts of the world.

3.1.1 The Acceptance Rate of Biometrics in the USA Versus the Underdeveloped World

If any individual wants to know the trends of various biometric technologies on worldwide basis, then outcome is very clear: The rate of adoption of biometric technologies tends to be much lesser in the USA than other parts of the world, especially for developing nations. This segment can be better explained by considering the fundamental rights of an individual. As the citizens of the USA, fundamental rights of the individuals are secured by the constitution of country. Meaning, each and every citizen of the country will be considered as distinctive individuals in the eyes of the Federal Government [16]. If for any reason citizens are not considered as distinctive individuals, then at least in principle, there exist certain types of legal recourse that citizens can take. Due to existence of this, if there is something that goes against rights of citizens, then they can easily assert that there is a violation of constitutional fundamental privacy rights and civil liberties. This is the main issue regarding the social acceptance of biometric technologies. In general, the claims of constitutional fundamental privacy rights and civil liberty violations fall into three general categories as briefly explained below.

3.1.1.1 Anonymity

Citizens of a particular country have the conviction that when they register themselves into a biometric system by following enrollment and verification process like Aadhar registration process in Indian subcontinent, they lose their total sense of anonymity. However, this may not be true always as strong security systems can maintain it. On the other side, in absence of appropriate security systems, there is a chance of hacking the ID number, which is associated with the said biometric template [17]. As an example when the local citizens in the USA experience the discomfort for a situation, then they will claim their right to remain unidentified. However, governments may say that this is not possible technology for the security purposes.

3.1.1.2 Tracking and Surveillance

Another category of privacy right is tracking and surveillance, which is disliked very much by most people despite efforts to justify them by governments. In the USA, much of this terror looks like just watching the “Big Brother.” This tracking and

surveillance is also hint on in the book wrote by George Orwell, titled *1984*. The primary substance of this fear comes when the Federal Government is misusing the stored biometric information and data.

3.1.1.3 Profiling

One of the biggest fears of the American citizens is using any form of biometric technology. In similar manner to that of "Big Brother" watching, the anguish-provoking approach is known as the "mark of the beast." Here, the main focus is on recording and analysis of a person's behavioral and psychological characteristics or to help in identifying classes of people. However, the citizens of most developing nations of the world, like Africa and Asia, hardly even have a democratic constitution (or other similar documents) in which their rights are protected. This results in that the individual is not treated as unique person by the government. But, after using the biometric technologies, citizens of these countries have shown their existence. As a result of deployment of these biometric technologies, the governments have to consider this fact and also consider these people as unique citizens of the country. Therefore, the acceptance rate of biometric technologies is much higher, because it helps these people by giving new hope to them in having freedoms and rights.

3.1.2 Uses of Biometric Technology by the European Union

Lot of migrants and refugees are facing the safety issues in parts of African countries where the European Union (EU) is facing number of complicated challenges like how to determine entry or fight for the fraud identity. Therefore, biometric digital systems are suited significantly to locating the culprit migrants who crossed the territory illegally. In addition to this, the utilization of biometric-based digital systems can also manage effectively the movement of migrants. This can also aid in monitoring their identification as well as aid risk assessment systems for decision-making.

3.1.2.1 Digitization of Borders

Authorities of border control and law enforcement agencies can use biometric identification technologies to differentiate the local citizens from immigrants and refugees. The Netherlands is one of the active members of the European Border Surveillance System (EUROSUR) (EC/1052/2013). EU law (2013/1052/EC) has managed the flow of population in matters like the number of refugees and immigrants who have crossed the border in order to ensure security and minimize illegal migration and international crime and terrorism.

3.1.2.2 Identification

Proper and accurate identification is vital to border security agencies in any country [18]. Authorities managing the immigration task can either permit or deny the entry of travelers. Biometric-based recognition and identification systems play a vital role to verify the accurate identity of travelers. Recently, identity-based management technologies are working to form the instruments which are expected to confirm that the ID holder is having a valid ID and his entry can either be granted or refused.

3.1.2.3 Profiling

Profiling is basically used to prevent the situations like illegal migration, human trafficking, fraud identification, and other international crimes. Sometimes profiling is also used to find new criminals. Profiling works on the group rather than the individual travelers. Profiles are construed based on the historical characteristics of particular persons, like who is earlier found guilty under criminal record illegal entry to the country or who has previous record of identity fraud [19]. Based on the above historical characteristics, profiles can be applied on each traveler at border crossings like airports, shipyards, and a line of control. The profile characteristics of a person must be regularly monitored and updated to find the risk flag of that person. This is the reason that EU law has been created to check the risk profiling of every traveler at border control and immigration. According to Directive 2004/82/EC, [22], an EU law, authorities of airlines are required to provide the set of passenger data to border control authorities prior to their arrival.

3.1.3 EU System's Policy Domain of Migration

This system includes a wide range of networked databases and biometric digital circuits of extensive shared dataset. The standards used in EU networks in broader landscape are Scheme Information Systems (SIS I and SIS II), EU's Visa Information System (VIS) (European Commission, 2015), and Eurodac (Council Regulation (EC) No. 2725/2000). Eurodac is a centrally controlled biometric dataset of fingerprints of registered refugees. Secure Information Exchange Network Application (SIENA) (European Commission, 2015) is used by the Netherlands as the primary channel for law enforcement information sharing and exchanging of the surveillance information about illegal migration and cross-border crime at the EU's land, sea, and air borders. The following are the policy domains of migration used in EU systems.

3.1.3.1 Immigration and Naturalization Service (INS) Console

Residence permit of the citizen is formed by encrypting the registered data after enrollment of third-country national. Here the meaning of third-country national is a

Table 21.2 Standard decisions used in PROGIS console

Decision	Use of	Working
Decision-007	Hand geometry	Work premises control
Decision-008	Fingerprinting	Professional premises control
Decision-009	Hand geometry	School and restaurant premises control
Decision-019	Vein pattern recognition	Professional premises control
Decision-027	Fingerprinting	Used in professional laptops as the security concern

AU authorization unique

citizen not having Dutch, EU, Norwegian, Icelandic, or Swiss nationality. Basic Facility of Aliens (BFA) is a centrally controlled government agency, which includes the photographs and the fingerprints as the identity of all immigrants [20, 21]. This Dutch Personal Data Protection Act (DPDPA) applies to all collected data by INS. Dutch Alien Act (DAA) was also formed to update the identity and set a limit for 10 years. In order to use the INS console, all third-country persons should be enrolled under INS console. However, this is not practically possible.

3.1.3.2 PROGIS Console

PROGIS is defined in Dutch language as *Programma Informatievoorziening Strafrechtsketen.* This standard was used for law enforcement agencies. PROGIS was formed under Dutch Police Data Act (DPDA). In this standard each PROGIS ID contains two numbers, criminal justice chain number (CJCN) and biometric numbers (BN). These two numbers are stored centrally in a specific database, which is called the criminal justice chain database (CJCD). BN and CJCN work together here; BN signifies State ID and CJCN indicate the criminal fellow [22]. PROGIS console is popular and reliable as it performs the identification of an immigrant before a policeman. A list of standard decisions used in PROGIS console is summarized in Table 21.2. In addition to this, Table 21.3 represents the deliberation review of biometric system for 10 years CNIL's report.

4 Perception of Biometrics

The major factor that affects the social recognition of biometric technology is the overall perception that how an exact modality behaves on the first impression. This segment is best suited for a scientific study known as "human factors" (HFs). In the market of biometrics industry, huge pressure is created on the vendors to develop the fastest and powerful algorithms. Ultimate goal of this is to attract the persons and provide them the platform so that they can use the biometric systems without any difficulty. Therefore, biometric suppliers are more focused about the theoretical and practical features of the modality, which is developed by them. Whereas, less

Table 21.3 10-year CNIL's deliberation review with respect to biometric system

Deliberation	Duration	Objective(s) of the deliberation
n°57	16 November 2000	Controlling of the employees' working time
n°23	17 February 2005	Control accessing of staff to sensitive areas
n°031	17 February 2005	Working time management purpose
n°034		
n°035		
n°036		
n°037		
n°113	7 June 2005	Controlling the area of ID cards and passport collection
n°135	14 June 2005	Working time controlling of hospital staff
n°101	27 April 2006	To control the working time management of staff
n°051	21 March 2007	Accessing of sensitive areas of chemical plant
n°080	25 April 2007	Control accessing of operation rooms of hospital
n°146	21 June 2007	Control access to the specific casino
n°254	13 September 2007	Ecureuil lease society-based biometric system
n°256	13 September 2007	To control access of restricted areas
n°038	7 February 2008	To control the presence of mentally disabled persons at workplace
n°056	6 March 2008	Specific use
n°084	27 March 2008	For the experimentation purpose
n°178	26 June 2008	To control access of establishment
n°324	11 September 2008	Access control on accommodation center
n°328	11 September 2008	Specific use
n°492	11 December 2008	To control access of community home of small age workers
n°360	18 June 2009	Control access in examination rooms
n°526	24 September 2009	Control access to the hotel
n°033	11 February 2010	Simple biometric identification system
n°131	20 May 2010	Control access to the specific casino
n°464	9 December 2010	Control access to the satellite control posts
n°147	19 May 2011	Control access to the catering
n°185	23 June 2011	Specific use
n°223	21 July 2011	To control access of restricted areas
n°257	21 September 2011	To control the data processing center GROUPE MIT
n°280	21 September 2011	To control access to the specific site
n°282	21 September 2011	Specific use

(continued)

Table 21.3 (continued)

Deliberation	Duration	Objective(s) of the deliberation
n^0388	1 December 2011	To control access to the luggage storage
n^0423	15 December 2011	Automatic identification of a speaker or an author of a text
n^0236	12 July 2012	For the experimentation purpose
n^0322	20 Sept 2012	Upgraded version
n^0039	2 December 2012	For the experimentation purpose
n^0375	25 September 2014	For the experimentation of a system "talk to pay"

CNIL-The French data protection authority

attention is being paid on the comfort to have complete enrollment and verification processes. In fact, there is not much reported literature on the misconceptions of the biometric device by users as well as the tools and effects of external environment available to the individuals.

Hence, biometrics industry must ensure while developing a new biometric modality that time should be a crucial factor during enrollment and verification. Moreover, it should provide the equal priority as given to the HF variables. This approach has the type two-pronged approach and is known as "Total Biometric System Performance" (TBSP). In short it is defined as the incorporation of biometrics into wider range and must stand intelligently while taking the growth of such type of applications.

4.1 Function Creep

The main objective of biometric technology is to offer sources to verify the identity of an individual; for that any biometric scanning processes, as discussed above, can be used. This process is complicated and passes through enrollment and matching procedure, and finally it should be stored in the safe custody server. Most of the time, individuals are worried about the security of personal information, as it may be used either intentionally or unintentionally for any security reasons. This theory has been taken into consideration by US citizens who are worried as they do not know if their respective personal information is used or will be used for other purpose and even if their prior permission was not taken before using personal information for purposes other than what it is intended for. This phenomenon was known as the "function creep" (FC). In order to save time and money, if a facial recognition system (FRS) was used at the one entry point of a shopping mall, the same can be used for same individuals at another point of entry.

4.2 Fraud or Identity Theft

One of the major perceptions with the biometric technology is the belief that it is foolproof technology; actually it is not always 100% possible. Due to this weakness, there is always a risk of someone imitating an individual and stealing his ID by capturing some database. Expectation in terms of accuracy from the biometric database is huge, as database has the unique qualities of an individual [23]. At the same time, there is no guarantee from the biometric technology to prove the innocence of an individual. Considering the situation of changing the passwords in common security systems, it is impractical to replace biometric readings with another one from the same person. However, a crime-based situation may occur when a person will cut off the finger of another person to access the security system, laptop, tablet, or vehicle of that person.

4.3 False Scanning by the Sensor

Depending on the performance of scanning sensor, there is a possibility to have false-positive and false-negative readings while comparing current scan data and pre-existing biometric database. Having such a situation will break down the system, as it provides the false reading, which is nowhere required. This situation is very much complicated as a valid individual may be denied access through the system, whereas the access is given to someone who would not be allowed to do so. Hence, privacy issues of an individual with biometric technology are not safe, and important information could be known to others; examples include marital status, religion, age, gender, salary, social security number, or employment situation.

5 Ethical Issues

Biometrics is now progressively more used for the identification and verification of a person in several applications like in insurance sector, visa preparation, border controls, health systems, and attendance system in offices and educational institutions. Biometric technology is very popular among the customers as accessing mechanisms of this technology is very easy and practical. Further, many applications are easily compatible and safe with the involvement of this technique, low maintenance, and the decrement in price of the biometric equipments also attracting the customers.

The biometric system used for distinctive proof of identity of any individual has been available in literature. Some latest examples that evidently emerge are the Frenchman Alphonse Bertillon who had invented “anthropometrics” in 1888 and the Englishman Edward Henry who introduced the concept of fingerprint technology

first time in the world in 1900 in order to trace the fingerprints of criminals. However, due to the increase in terrorism all over the world, biometric technology has been gaining popularity as there is a need for better security systems. There are many benefits in using biometric technologies such as their distinctive and unique features and ability to satisfy the necessity to provide accurate verification and authentication. Some applications where biometric technologies are used include identity cards, e-passports, visa service, e-borders for protection of borders, airport security, and police investigation [24–26]. From commercial point of view, the leading players that use biometric technologies are the tour and travel sector, action parks, transportation systems, banks, and financial institutions.

At the same time, using biometric technologies is leading to many serious ethical implications. Some of the issues are the disclosure of personal identity, the conflict with one's principles and morals, and use of his/her personal biometric data for any other purpose. The civil liberty organizations claimed that the biometric-related technologies reduce the human rights related to privacy. It is unpleasant and has the ability to make serious impact on personal freedom and democratic rights. The technology is always prone to failure and is not false proof as it can be deceived. Nevertheless, many issues and threats around the security world exist, such as risk of terrorism, stealing of personal identity and fraud, security, and entry of illegal immigrants. It has now become important to have the ability to check the person's identity for later identification and verification [27]. After what happened in 9/11, organizations and governments worldwide have increased the use of biometric schemes for identification, verification, and authentication. Nowadays, hardware required for installing biometric technologies has better quality in design and correctness. The prices have also decreased, which moved biometric technology to the mainstream, both by individuals and organizations.

The abovementioned issues cannot really be ignored. There is an urgent convincing need to find practical solutions, which can be deployed easily without any difficulty or hindrance. Academics play an important role through research and development, discussions, seminars, awareness, training, and education.

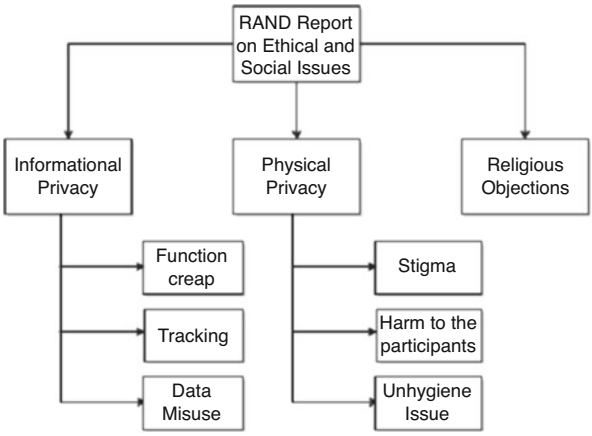
5.1 Ethics and Biometrics

Relevance of the ethics under biometric technology mainly focused around the security, in the very initial phase of this growing technology. Many issues have been related to the rights of an individual. These include safety of the individuals and their dependents, security of personal and official database, privacy, and autonomy. One of the challenging issues is to determine the relationship between the person and his cooperative rights. Biometric technology was initially planned to help out the individuals in terms of their security, but at the same time, this technology has enhanced their roots not only in personal activity, but in social and collective identity as well [28]. Subjects related to sociology are very basic and common at higher school levels and early age of college levels. But these subjects are not having the

Table 21.4 6-year project report issued by official bodies on ethical and social aspects of biometrics

Year	Report	Wide area of application	Remark
2001 [28]	RAND	US defense biometric	Used for sociocultural aspect
2003 [29]	–	European Commission biometric	Working party data protection
2004 [30]	BIOVISION	Integration between client and system	Deployed successfully
2004 [31]	OECD	–	Biometric technology
2005 [32]	IPTS-EC	Joint research	To check the effect on society
2006 [33]	NBC	NSTC	US based

Fig. 21.4 RAND report



significant knowledge of the ethical issues of biometrics at international level, as this technology is very popular at global level. Now, encyclopedia of bioethics has been revised, for example, the word "biometrics" does not feature either as an entry or in the analytical index [31]. In fact, the academic press [32] says it the encyclopedia of human biology and few others encyclopedia of science and technology do the same [33]. Till 2006 few reports have been issued by official bodies on ethical and wider social implications of biometrics; details are given in Table 21.4.

5.2 RAND Report

Detailed structure of RAND report submitted by the RAND institutions on the request of US army is shown in Fig. 21.4. This structure was prepared to explore the legal, ethical, and sociological concerns raised by biometrics.

RAND report on ethical and social issues of biometrics use was basically prepared to focus on informational privacy, physical privacy, and the factors related to the religious concern. Citizens of any country are having the fear of insecurity of their personal information that was taken by biometric scanners for the specific application. Function creep, tracking, and data misuse are the important factors in this domain; out of these three, function creep has already been covered in Sect. 4.1. Tracking was similar to the function creep; it can perform the real-time monitoring of the actions performed by an individual. Misuse of data is a major concern as personal information of an individual can be either intentionally or unintentionally used to the situation that was not in the knowledge of that individual. In most of the reported literature, this type of factor has reported as unavoidable risk of the biometric database. The major concern of biometric technology was to enhance the security of any system, but as for appropriate knowledge concern, identification from biometric technique is based on the statistic rather than a full proof mathematic. Meaning is that the probability of mismatching of different templates of biometrics of a primary individual with secondary individual signifies the valid identification of primary. Under physical privacy concerns, report has suggested three kinds of risk: (i) the stigma linked with biometrics, (ii) chance of genuine injury to the person taking part in the process of enrollment either by technology or by surrounding, and lastly (iii) hygienic confirmation of the biometric devices being used for the process may not be available. The last two issues are directly related to the public in terms of direct harm; hence, extra precautions have been recommended in the report for these two issues. The stigma may be an important factor when biometrics is essential for a particular application. Finally, the RAND report addressed some religious objections to the biometric technology.

5.3 Business Ethics and Biometric Security

A list of ethical concerns with biometric identification techniques [34] have been investigated by users:

(a) Retina scans is one of the biometric identification techniques that is fairly invasive.
(b) Number of persons is having a thought that collecting the fingerprints is associated with a record keeping to the criminal behavior of that person.
(c) In general persons may feel the loss of their personal dignity and security while giving their detailed biometric information to a central platform.
(d) Sometimes matching sensor may have scanning problem that may cause the embarrassing feeling among the people if there is a matching error due to malfunctioning of the matching sensor device.
(e) Personal security of an individual may be affected during the automated face recognition taking at public places without prior information to that person.

(f) Most of the time, persons may ask many questions like, how this data will be stored and used? What are the security measures taken while storing the personal information? Who will be responsible for maintaining the safety of electronic biometric information and database?
(g) As we know every individual is worried about his own and his loving one's security. Therefore, the use of biometric scanning techniques in business and government can offer a one-step enhancement on the security of organizations and individuals. However, it may create some issues such as privacy of individual as this is largely affected and any misuse of the same can be harmful. The issues discussed above are some of the major concerns.

6 Case Study

Since the last few decades, biometric technologies are frequently used and very successful in their respective field. In addition to this, the technology is very reliable and provides secure access control. Several successful deployments on medium- to large-scale environments like airports, railway stations, educational institutions, and country borders prove their feasibility. However, applications involving biometric systems for security and privacy concerns, facing lot of challenges to satisfy the customers and end users. In order to find the difficulties for the implementation and possible solutions, a couple of case studies have been considered and discussed in details in the forthcoming sections of this chapter.

6.1 Case Study of Megaproject UIDAI of India

In order to maintain the security of the country, government takes several actions with the help of biometric technologies; this task has rectified several issues of security. Identity of the resident of that country can be taken through biometric scanners and stored to the secure server to maintain the security. One of the Asian countries, India, has started one program for their citizens to provide them with an authorized unique identification (UID) [35]. This program is the part of megaproject Unique Identity Authority of India (UIDAI). The actual purpose of UID is not only to provide the authorized identification but also to provide better services and support to the resident of India (RoI). This program is successfully executing in the all states of the country and is helping the government and RoI. This section is including the development of UID program in details like involvement of different process, execution, and applications. UID is a program of the Indian government that leverages emerging biometric scanning-based technologies to help various government and commercial agencies to identify and maintain the database of RoI. Importantly UID is not an identity card, but a number of 12 digits, which is stored on the cloud server. Cross verification of any UID can be done by comparing the number to

biometrics that are collected and stored on a Central Identities Data Registry (CIDR). This number is unique. The UID program is similar to another program of the government of India, known as know your customer (KYC).

6.1.1 System Architecture of UID

At the organization level, biometric data processing was taken very carefully. CIDR collects three Automated Biometric Identity Subsystems (ABIS) that run simultaneously. Several organizations are using the single biometric scanning mechanism like offices, educational institutes, banks, insurance agencies, and shopping malls. Therefore, keeping in the view of Indian population (1.32 billion as of today, which is the second highest in the world), utilization of three ABIS enhanced the accuracy and minimizes the mismatch rate. The single ABIS enrollment can easily be tracked and misused by multiple systems that ultimately put a question mark against the security of an individual, it also decreased the dependence on single vendor and gave the UIDAI an ability to test and introduce the new solutions. A detailed system architecture of UID is given in Fig. 21.5. The three ABIS are operated by outsourced

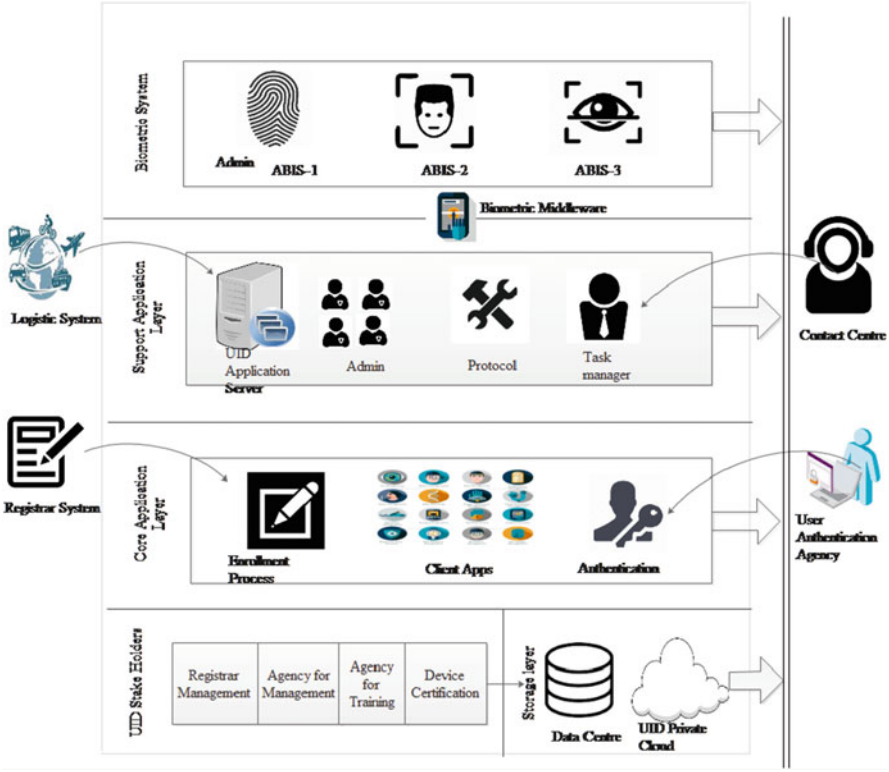


Fig. 21.5 System architecture of UID

biometric service providers (BSPs). They maintain the proprietary fingerprint and iris image templates in their respective database server. Every ABIS autonomously de-duplicates across the complete range of enrolled data and stored all enrollments safely. Quality of every ABIS is that it is independent of the vendor and flexible in terms of modification. The performance of every ABIS is examined over every ten million de-duplications, and as per ABIS's performance, data is reallocated. The collected information from individual vendor is template based and stored centrally at UIDAI level, and ABIS records have been maintained in the form of proprietary templates.

A possible situation may occur when a vendor does not want to continue the services; then a new vendor will take over the same in the form of copy of enrollment records. Further, it convert the same and store for de-duplication in order to help the new vendor demographic de-duplication can be provided to decrease the errors. The continuous accuracy monitoring protocol, the UID Middleware, has been inserted between the three ABIS and main application [36]. As a regular practice, the server cross-examines the entered data with the existing data and provides a scaling count known as fusion count that indicates the similarity of current data with the existing data. Here, lower fusion count represents the lowest similarity, whereas higher fusion count indicates the larger similarity. Main part of the system architecture is CIDR, which includes Tri-ABIS and UID Middleware, enrollment, authentication services, and supporting applications like administration, report preparation, and fraud detection. Supporting applications are interfaced with the logistics provider and the portal to control the internal administrative and information access. An intermediate administrative application is also used for proper user management, access control, status reporting, and business automation purpose.

To improve the data integrity and enhance the data quality, proper execution of algorithm mentioned in Table 21.5 is essential. Symbols used in Table 21.5 are defined as F^r, fingerprint scanning data; I^S, iris scanning data; F^C, facial scanning data; Q^t, biometric data using standard biometrics algorithm; B^d, biometric database;

Table 21.5 Algorithm for UID enrollment process

Input: F^r, I^S, F^C, Q^t, B^d & P^d **Output:** Resident of the Country Enrolled on Aadhar Biometric System	
1.	Q^t of biometric data measured using standard biometric algorithms
2.	If (Q^t = = T^h) **then**
3.	B^d is in its required form
4.	Else
5.	Checks performed by client software to avoid any fraud
6.	B^d checked against the stored data base available with operator
7.	If (User = = P^d) **then**
8.	Additional photograph of hands and face taken
9.	Else
10.	Go to step 2
11.	Operator overrides of the policies set in software
12.	Further investigate the captured process
13.	All captured images sent to the central server

P^d, personal database; and T^h, threshold. It may be possible that a vendor can intentionally introduce the fake identity to the database. But the system has been designed in the beautiful way that the culprit vendor will be identified when the fake identity is identified, because a vendor can submit the respective database by providing his personal biometric as the identity of his database.

6.1.1.1 Enrollment Process

One of the main functions of UIDAI is to set up the standards for enrollment so that the governments of States and the Union Territories can identify the registrars and provide appropriate resources necessary to fulfill the enrollments of UIDs. The State departments, like the Rural Development Department (RDD), Civil Supplies (CSs), and Consumer Affairs Department (CAD), form an association with the UIDAI and sign memorandum of understandings (MOUs) as mentioned in [37] that asserts that the States are committed to "enhance efficiency in delivery of government benefits and services through accurate identification of beneficiaries and to have uniform standards and processes for verification and identification of beneficiaries." As per the agreement, a hierarchy has been formed as shown in Fig. 21.6 in order to collect the biometric data of RoI. Several enrolling agencies, either fixed or dynamic as per the requirement of data collection, have been outsourced to complete the enrollment

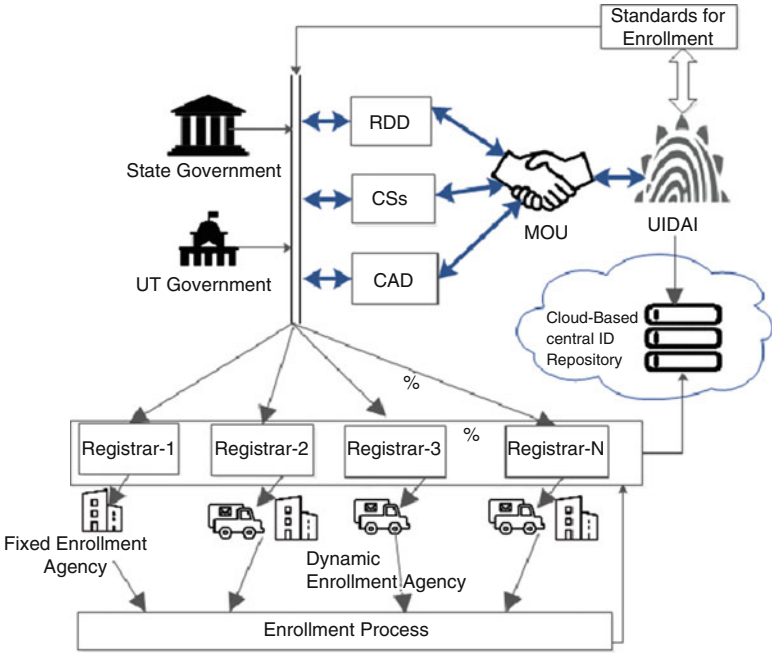


Fig. 21.6 Enrollment process

functions. Enrollments finally should be saving at UIDAI Central ID Repository after passing through registrars. Selection of enrolling agencies is based on meeting the requirements of standards of enrollment functions prepared by UIDAI. After satisfaction, they receive the respective certificates from UIDAI.

6.1.1.2 Updating and Maintenance of Database

Strong and secure cloud is a must at CIDR end because after enrollment process is over, unique identification numbers have to be assigned to the individuals. Further, this process is not fixed as the regular processing and modification on the database is the general practice. Databases stored in the CIDR cloud are of two types, viz., demographic and biometric; data may depend upon the time. RoI can relocate himself/herself as per convenience, but respective RoI has to timely inform the task manager of CIDR cloud. This information can be transferred to the CIDR via multimode which is easily accessible, like mobile phone, to the RoI. Updating process can also be maintained at the registrar end by arranging an online portal for the RoIs. This online portal is managed by the UIDAI and can be easily accessible to the smart RoIs. A systematic execution of updating process is shown in Fig. 21.7. Due to accident if appearance of the face of an RoI is changed, then this high sensitive information could not be processed either online or by mobile phone. In this situation either dynamic enrollment agency has to approach the respective RoI or RoI has to report to the nearest enrollment agency. As this is not the routine process hence, enrollment agency may charge for the updating. As per the current

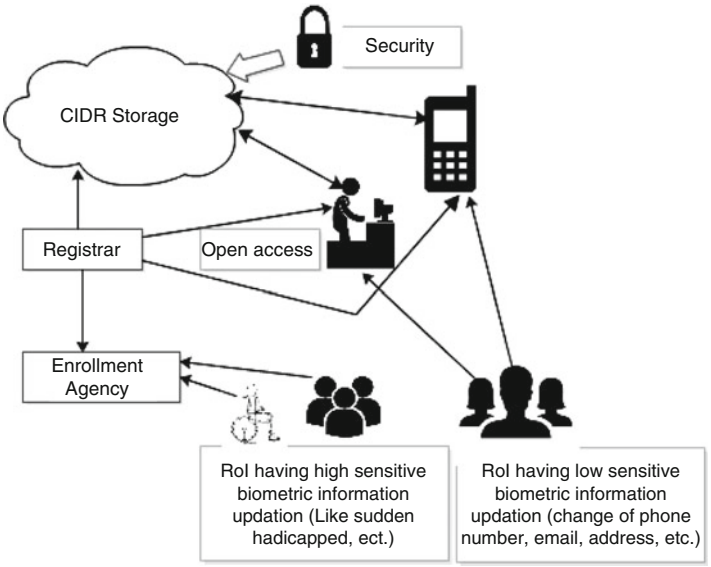


Fig. 21.7 Updating and maintenance process

knowledge, low sensitive information, like change of address, change of mobile phone, change of e-mail address, any correction in the date of birth, etc., are updated through online portal or by mobile phone. CIDR is not charging for the updating of low sensitive information.

6.1.2 Impact on Other Countries

The UIDAI project of India has received massive popularity around the globe. As per media report [37], few nations like, Mexico, Brazil, Indonesia, and Argentina are planning to change their national ID program based on the UIDAI. The India's UIDAI project is popular not only for its size and scope, but it is one of the first national ID projects to have been designed in a way that has the potential to touch every aspect of a society.

6.1.3 Applications of Megaproject UIDAI

The 12-digit UID of an individual along with his personal information in the form of a card, known as *Aadhaar card*, is provided to that individual. This *Aadhaar card* is used in several services; some of them are listed below:

(a) For the opening of a bank account
(b) For registration of new cellular connection
(c) To receive the subsidy directly to the bank account
(d) Passport making
(e) Insurance sector
(f) Health sector
(g) Ladies pension schemes provided by the government of India
(h) Income tax deduction
(i) Liquid petroleum gas (LPG) connection under Ujjwala Yojana provided by the government of India
(j) To verify the identity of an individual in the election by polling party to avoid fake polling

6.1.4 Outcome from the Case Study

We have seen in earlier sections that to increase the level of security, multiple biometrics components have to be added on a single platform. The purpose of UID in India is not only to provide an identity code of 12 digits but also to provide the benefits of government policies that have been designed for the RoIs. Several applications have been covered in Sect. 6.3. Many countries are using fingerprints as the only biometrics for the preparation of identity cards. The purpose of adding facial scanning and iris of the individual is to enhance the security level. A good number of Indian population are also involved in the labor job, so there may be a chance that

quality of their fingerprint will never come to the appropriate level. In order to provide the UID irrespective of the job of an individual, UIDAI has involved tri-biometrics approach in their system. However, the project UIDAI is not fully completed in India but several RoIs are taking the benefits from this project. Hence, this is one of the successful projects of India in terms of the huge database of UID management of their citizens.

6.2 *Case Study on Biometric-Based Security in Banking Sector*

This case study includes identification and discussion on various issues and factors related to implementing biometrics in banking sector, specifically for the user authentication and control [38].

6.2.1 Objectives

The main objectives of this case study are shown below:

- To perform the analysis of security issues in the banking sector in New Zealand
- To check the biometric solutions as a key for security in banking sector
- To track different security strategies for banking sector

6.2.2 Background

This case study includes the survey of current banking system in New Zealand. In this study, analysis on different security models has been performed. This study also includes the involvement of biometric technology in New Zealand banking sector. We have taken this case study from [39]; the database has been collected from research journals, Internet, textbooks, and social websites. Authors in [39] have prepared the questionnaire that includes qualitative and quantitative questions for collection of information related to the New Zealand banking sectors. The questionnaire was intentionally prepared in such a fashion that gathers maximum-security issues in banking sector. Key areas of the investigation [39] for banking sector are given below:

- To know the current IT security processes
- To know the current IT security policies
- To know the current IT security infrastructure
- To know how to control the IT security
- To know how biometric technology affects the current banking sector

- To know how much knowledge of biometric-enabled security is known to the staff
- To classify the challenging issues and concerns

6.2.3 Analysis of Information Security Models Used in Banking Systems

Nowadays, computer-based secure environment is a major requirement of any banking system. As a policy of security in banking sectors, the following issues are essential along with proper auditing, confidentiality, accountability, availability, integrity, and non-repudiation [40, 41]. A systematic comparison of different models has been given in [39]. This task is executed on the physical layer of the protocol. Accessing of the banking account can be provided after cross-checking of several parameters. Several security models have been compared with those that are promptly used in the banking sectors.

6.2.4 A Detailed Discussion on the Case Study

In this study authors of [39] collected the information in the banking sector of New Zealand and performed the analysis to check the security issues in the subject. Here, the integration of biometric-based security technology with current system should not ignore the client privacy fears and account holder's tolerance levels, changing to the banking system and legal issues. A new paradigm in the case study was investigated that will support biometric-based security systems in banking sectors. This paradigm was known as critical success factor (CSFs). The CSFs have been broadly classified into four categories, viz., technology factors, monetary factors, management factors, and legal and ethical factors. Figure 21.8 represents a summary of CSFs along with related factors and respective solutions. CSFs have been analyzed by the authors of [39] according to the questioner's database. A detailed classification of individual factor of CSFs has been presented in Fig. 21.8. The next section includes the detailed discussion on every factor.

6.2.4.1 Technology Factors

(a) *Accuracy*: Accuracy is one of the measuring parameters of a biometric system; usually this parameter is used to check the involvement of technology, which is used in the current system. A number of measuring terms have been covered in the literature to check the accuracy of biometric system on banking sectors; some of them are rejection of false measurement, reduction in false matching rate, failure to false enrollment, and ability to verify (ATV) the correct measurement [28]. In the banking environment, the ATV has given the most priority in the biometric security-based banking system because it can maintain better accountability and also can give the attractive performance in terms of the fraud

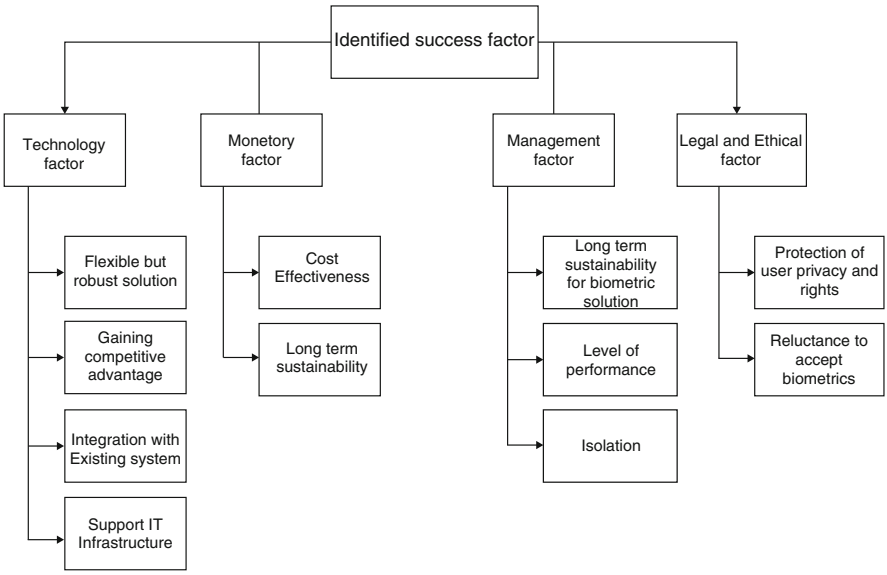


Fig. 21.8 Four main categories of success factors

detection and rejection. Therefore, on the basis of technology factor, CSF of the banking sector could be increased.

(b) *Flexibility*: Biometric systems stored the sensed database to a secure server or to the cloud. During the scanning process, some threshold value of the parameter is required. As time increases, the nature of the body of a human will also change, like wrinkles on the face and palm and rubbing of fingerprint due to hard work. Therefore biometric system must be fault-tolerant considering the abovementioned issues. During the cross verification of a person's biometrics for a low-level security system, hundred percent matching of his biometrics may not be required; hence, considering the abovementioned issues, the threshold should be decided accordingly. In banking sectors usually two levels of security are preferred. First could be biometric-based fingerprint, iris, or facial scanning and secondly either swiping of cards or password based. This mechanism involves some sort of flexibility to the client side, as user can change/update the password on regular basis. This parameter enhances the belief of client to the banking sector as security can be changed partially by himself. Hence, flexibility in the technology along with appropriate tolerance levels in biometric-based security system for the banking sector may increase the success of adoption of this system.

(c) *Privacy and confidentiality issues*: Security and privacy are always the prime issues to be considered in the system, especially for financial transaction-based system. Any system could collapse if biometric database is either stolen or intentionally misused by the service provider. Therefore, level of security must be defined earlier while enrolling the database for biometric system. Three levels

of security, low, average, and high [42], can be planned for banking sectors. Different services have been offered by the bank; administrative authority of the bank, usually bank manager, can choose application-based security level. Decision for the selection of level of security is crucial as selection of the appropriate biometrics totally depends on this decision. In general low to average security could be verified from behavioral biometrics. On the other hand, physical biometrics is required for high-level security [43].

6.2.4.2 Monetary Factors

Biometric-based security systems are considerably more costly than ordinary security systems [44]. The following are the significant costs that play a major role for the success factors of case study. Integration to the existing system along with the testing costs and, secondly, high-level skilled trainers and maintenance costs are required to manage the updating in existing system.

(a) *Intangibles*: The authors of [39] survey have investigated that some of the intangible remuneration in banks can have competitive advantage and improve productivity and prosperity. By doing this, there will be a reduction in security risks which increases the confidence level of account holders of the banking system.
(b) *Long-term stability and sustainability issues*: In order to maintain the internal security system of bank, few banking systems have provided the facility of smart card to their clients. Smart clients are also in a habit to use these smart cards in their regular routine. Therefore, to maintain the long-term stability and sustainability, banking sectors have to arrange proper counseling and training modules to the existing clients to communicate the additional benefits of biometric system. To maintain the long-term relationship to existing clients, these training programs should be provided free of cost. However, a significant charge can be taken from the new clients, or it may depend upon the bank or respective government.

6.2.4.3 Management Factors

Database of employee segment collected by authors of [39] indicates that management also maintains a clear impact on the success of a biometric-enabled security in the banks. Support to the biometric innovation should be enthusiastically taken by the branch manager. Enthusiasm of the upper management staff of bank plays a very significant role on the adoption of biometric-based security to their bank. Branch manager is responsible and should arrange the minimum amount to be used in this security system. Sudden change in the working culture and the new policy may create the cause among the staff members of the bank. Hence, appreciation to the staff should be given on existing environment, and at the same time, staff should be

motivated to the change in policy. By doing this activity of staff can be managed by themselves without any dispute to the possible change.

(a) *Availability of resources*: Availability of appropriate resources plays a vital role for making the biometric-based security system a great success. Some of the resources are as follows: training and orientation programs need to be arranged in a timely manner for the banking staff, especially those who are directly involved in this program. Selection of skilled and trained staff member for program is essential, infrastructure can't be tolerable for the program, sufficient capital should be arranged prior to start the program, and additional staff members and infrastructure will improve the stability of the program in case of any emergency situation.

6.2.4.4 Legal and Ethical Factors

New Zealand banking sectors are required to fulfill the government programs for the banking security like the Credit Contracts and Consumer Finance Act (2003) (3CFA), Consumer Guarantee Act (CGA), Privacy Act (PA), Fair Trading Act (FTA), and Contract Enforcement and Contractual Mistakes Act (CECMA) [39]. These factors are essential and will play a very important role for the biometric-based security system implementation process for the banking sectors.

(a) *Social and psychological issues*: The impact of biometric technology on social and psychological concern is divulging the bodies of an individual to the biometric scanning system [45, 46]. Few vendors supplying biometric equipments have been claimed that their products are of good quality and have less effect on the human biological system. However, in relation to the biometric system, this type of claims is simply myths and must be rejected.

After combining the factors as discussed above, altogether, it has been observed that in biometric-based security systems for banking sectors, legal and ethical factors could not be ignored to achieve CSF. Even timely orientation and training programs must be arranged to the banking staffs and the account holders so that they should know about the ethical and legal issues of biometrics.

6.2.5 Bio-Sec Project Development

A biometric-enabled security project known as Bio-Sec was specially developed for the banking sectors. This mechanism has Bio-Sec access controls. Authors of [39] have investigated and discussed this project. In this project, highest priority is given to the security against illegal admission, which could be internal or external. At initial level, Bio-Sec project has included the integration of biometrics with access card in order to secure the identification of internal members of the bank. Figure 21.9 shows the every segment of Bio-Sec project in details.

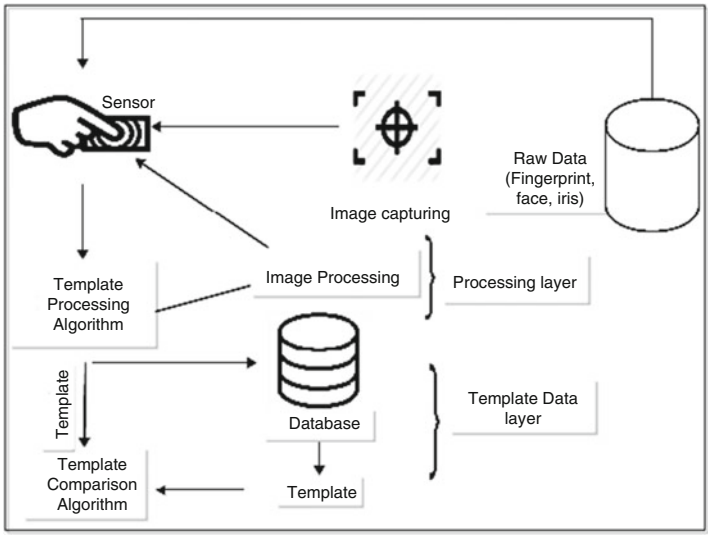


Fig. 21.9 Detailed biometric system in banking sector

Bio-Sec project has deeply classified the roles and responsibilities of individual component. In addition to this access, provisions and authentication processes are also defined properly and assigned the respective duties. The template data layer was used to store the database by using the template comparison algorithm, whereas processing layer was used to perform the image processing; template processing algorithm was used in this layer. This composite segment is known as Bio-Sec project for the security of banking sector.

6.2.6 Outcome from the Case Study

This case study was focused on the biometric-based secure technology implementation on banking sectors.

Several challenges have been identified in this work, and CSF was discussed that really enhances the adaptation rate of biometric technology in banking sectors. Benefit of this case study is that possible challenges in the banking sectors can be estimated before the implementation of biometric technology to the banking sector as there is always a significant amount of risk in the banking domain due to financial transaction involvement. Hence, this case study supports very well especially for technology factors, monetary factors, management factors, and legal and ethical factors. The success rate of the banking system will depend on the successful execution and regular monitoring of the abovementioned factors. CSF helps the banking administration to prepare their business plan, make the system flexible in terms the rectification of problems of clients, and arrange the proper healthy

environment to their account holders for a successful biometric security implementation. The architecture of Bio-Sec was given so that it can be used to implement the biometric-based security to the banks.

7 Conclusion

Nowadays the adoption rate of biometric technology is rapidly increasing in all applications. Biometric technology is to be considered as an effective measure for the protection against crime. However, there is always the concern that it violates the privacy and rights of the individuals. These factors may include the possibility of fraud, identity theft, civil liberty violations, and inaccuracy of data. As a result factors may create the conflicts between service provider and public as they may be accused of a crime or may become a victim of discrimination. In these situations, persons may put up the question mark on the storage of biometric database. They can further point out the issue that their personal information may be shared with entities that are not supposed to know them. We must plan for short-term security and long-term security of biometric database separately. This process will reduce the probability of biometric data tracking. A couple of case studies has been covered in this chapter: UID developed by the government of India to provide several facilities to the RoI and inclusion of biometric-based secure technology to existing banking systems. Considering the facts discussed in the second case study, we can conclude that by proper planning, inclusion of relevant blueprint with an appropriate, flexible, and stable biometric scheme that should be focused on ethical, legal, social, and technological issues of the system can build a helpful and secure biometric-based banking system. Further, perfect planning of administration, sufficient homework on fault-tolerant schemes, policy making to sustain the security, and excellent database management will ensure the flawless biometric-based security systems that meet the future's requirements.

References

1. D. Wright et al., Ethical dilemma scenarios and emerging technologies. Technol. Forecast. Soc. Chang. **87**, 325–336 (2014)
2. E. Maria, M. Gameiro, Security, privacy and freedom and the EU legal and policy framework for biometrics. Comput. Law Secur. Rev. **28**, 320–327 (2012)
3. V. Diaz, Legal challenges of biometric immigration control systems. Mexican Law Rev. **7**(1), 1–28 (2015)
4. J. Catherine, Biometric standards–an overview. Inf. Secur. Tech. Rep. **7**(4), 36–48 (2002)
5. M. Baca, J. Cosic, Z. Cosic, Forensic analysis of social networks (Case Study), Proc. of the ITI 2013 35th Int. Conf. on Information Technology Interfaces, 219–224 (2013)
6. M. A. Kowtko, "Biometric authentication for older adults," IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014, Farmingdale, NY, 2014, pp. 1-6.

7. G. Paul, J. Irvine, IEDs on the road to fingerprint authentication. IEEE Consum. Electron. Mag. **5**, 79–86 (2016)
8. M. Krlic, "Social costs of surveillance and the case of biometrics," 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2014, pp. 1278-1282.
9. S. Thavalengal, P. Corcoran, Iris recognition on consumer devices-challenges and progress. IEEE Int. Symp. on Technology in Society (ISTAS) Proc., 1–4 (2015)
10. K. Michael, The legal, social and ethical controversy of the collection and storage of fingerprint profiles and DNA samples in forensic science. IEEE Int. Symp. on Technology and Society, 48–60 (2010)
11. A. Krupp, C. Rathgeb and C. Busch, "Social acceptance of biometric technologies in Germany: A survey," 2013 International Conference of the BIOSIG Special Interest Group (BIOSIG), Darmstadt, 2013, pp. 1-5.
12. G. Hornung, M. Desoi, M. Pocs, Biometric systems in future preventive scenarios – legal issues and challenges, 83–94 (2009)
13. C. Sullivan, Digital citizenship and the right to digital identity under Int. law. Comput. Law Secur. Rev. **32**, 474–481 (2016)
14. R. Clarke, Privacy impact assessments as a control mechanism for Australian counter-terrorism initiatives. Comput. Law Secur. Rev., Volume 32, Issue 3, 1–16 (2016)
15. K. Stoychev, T. Georgiev, An alternative approach and attempt to come up with a standard for biometric user authentication in a network based environment. Procedia. Soc. Behav. Sci. **47**, 74–78 (2012)
16. P. Li et al., An effective biometric cryptosystem combining fingerprints with error correction codes. Expert Syst. Appl. **39**, 6562–6574 (2012)
17. C. Tal, M.H. Shiang, An efficient biometrics-based remote user authentication scheme using smart cards. J. Netw. Comput. Appl. **33**, 1–5 (2010)
18. T. Caldwell, Web service-based standards for biometrics interoperability. Biom. Technol. Today **2013**, 9–11 (2013)
19. T. Caldwell, Market report: border biometrics. Biom. Technol. Today **2015**, 5–11 (2015)
20. K.L. Fors, Monitoring migrants or making migrants 'misfit'? Data protection and human rights perspectives on Dutch identity management practices regarding migrants. Comput. Law Secur. Rev. **32**, 443–449, 2016
21. Y. Liu, Scenario study of biometric systems at borders. Comput. Law Secur. Rev. **27**, 36–44 (2011). 2016
22. S.M. Matyas, J. Stapleton, A biometric standard for information management and security. Comput. Secur. **19**, 428–441 (2000)
23. C. Roberts, Biometric attack vectors and defenses. Comput. Law Secur. Rev. **26**, 14–25 (2007)
24. V. Smejkal, J. Kodl and J. Kodl, "Implementing trustworthy dynamic biometric signature according to the electronic signature regulations," 2013 47th International Carnahan Conference on Security Technology (ICCST), Medellin, 2013, pp. 1-6.
25. Y. Sun, M. Zhang, Z. Sun, T. Tan, Demographic analysis from biometric data: achievements, challenges, and New Frontiers. IEEE Trans. Pattern Anal. Mach. Intell., 1–20 (2017). https://doi.org/10.1109/TPAMI.2017.2669035
26. A. S. Munalih, L. Mat Nen, A. Goh, L. K. Win, K. S. Ng and L. Ching Ow Tiong, "Challenge response interaction for biometric liveness establishment and template protection," 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, 2016, pp. 698-701.
27. M. Cehic, M Quigley, Ethical issues associated with biometric technologies, Proceedings of the 2005 Information e-sources Management Association Int. Conf., 1–5 (2005)
28. J.D. Woodward et al., *Army Biometric Applications: Identifying and Addressing Socio Cultural Concerns* (RAND, Santa Monica, 2003). [Online]. Available: http://www.rand.org/pubs/monograph_reports/MR1237
29. BIOVISION, Roadmap for biometrics in Europe to 2010. [Online]. Available: http://www.eubiometricsforum.com/dmdocuments/BIOVISION_Roadmap.pdf

30. Data Protection Working Party of the European commission, *Biometrics* (EC, Brussels, 2003). [Online]. Available: http://www.europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf; Last visited 27 Mar 2007
31. Organization for Economic Co-operation and Development (OECD), *Committee for Information, Computer and communication Policy – Working Party on Information Security and Privacy*, Biometric-based technologies, OECD (2004). [Online]. Available: http://www.oecd.org/sti/security-privacy
32. European Commission Joint Research Center, *Biometrics at the Frontiers: Assessing the Impact on Society* (2005). [Online]. Available: http://www.jrc.cec.eu
33. National Science and Technology Council, *The National Biometrics Challenge*. [Online]. Available: http://www.biometrics.gov/NSTC/pubs/biochallengedoc.pdf
34. K. Yang, E.D. Yingzi, Z. Zhou, Consent biometrics. Neurocomputing **100**, 153–162 (2013)
35. F.Zelazny, The evolution of India's UID program, Center for Global Development, 1–44 (2012)
36. Unique Identification Authority of India, *Ensuring Uniqueness: Collecting Iris Biometrics for the Unique ID Mission* (2006). [Online]. Available: http://uidai.gov.in/UID_PDF/Working_Papers/UID_and_iris_paper_final.pdf
37. Unique Identification Authority of India, *Envisioning a Role for Aadhaar in the Public Distribution System* (2006). [Online]. Available: http://uidai.gov.in/UID_PDF/Working_Papers/Circulated_Aadhaar_PDS_Note.pdf
38. T.S. Siang et al., Ethical implications of digested medical and biometric data. IIMC Int. Conf. Mgt. Corp., 1–9 (2010)
39. S. Venkatraman, I. Delpachitra, Biometrics in banking security: A case study. Inf. Manag. Comput. Secur. **16**(4), 415–430 (2008)
40. Int. Telecommunication Union, ICT Facts and Figures (2011). [Online]. Available: http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf
41. A. Rebera, B. Guihen, Biometrics for an Ageing Society Societal and Ethical Factors in Biometrics and Ageing. Int. Conf. of the Biometrics Special Interest Group (BIOSIG), 1–4 (2012)
42. S. Prabhakar, S. Pankanti, A.K. Jain, Biometric recognition: Security and privacy concerns. IEEE Secur. Priv. **2**, 33–42 (2003)
43. E. Mordini, C. Petrini, Ethical and social implications of biometric identification technology. Ann Ist Super Sanità **43**(1), 5–11 (2007)
44. S.C. Dass, Y. Zhu, A.K. Jain, Validating a biometric authentication system: Sample size requirements. IEEE Trans. Pattern Anal. Mach. Intell. **28**(12), 1902–1913 (2006)
45. C. Costanzo, Suddenly, biometric ID doesn't seem like science fiction. Am. Bank. **171**(107), 6–11 (2006)
46. L. Hunter, A. Orr, B. White, Towards a framework for promoting financial stability. Reserve Bank N. Z. Res. Bull. **69**(1), 5–17 (2006)
47. M.S. Obaidat, N. Boudriga, *Security of E-Systems and Computer Networks* (Cambridge University Press, Cambridge, 2007)