Chapter 19
Biometrics Security and Internet of Things (IoT)

Mohammad S. Obaidat
Fellow of IEEE and Fellow of SCS,
Fordham University, USA and University of Jordan, Jordan

Soumya Prakash Rana
Division of Electrical and Electronic Engineering,
London South Bank University, London SE1 0AA, United Kingdom

Tanmoy Maitra
KIIT University, Bhubaneswar, India

Debasis Giri*
Dean, School of Electronics, Computer Science and Informatics,
Haldia Institute of Technology, India

Subrata Dutta
Haldia Institute of Technology, India

*Corresponding Author: Debasis Giri: debasis_giri@hotmail.com

ABSTRACT

The human-to-machine and human-to-human communications are transforming to machine-to-machine communications by which several decision-making systems can be built. When different Internet enabled smart devices interact with each other's to achieve a goal (application depended), then a network is formed in which different sophisticated technologies will integrate to each other to form Internet of Things (IoT). It encompasses the vast amount of diverse smart devices, which collaborate with each other to achieve different smart applications like, smart cities, connected cars, automated agriculture and so on. Though Radio Frequency Identification (RFID), Wireless, mobile and sensor technologies make IoT feasible, but it suffers from many challenges like scalability, security, and heterogeneity problems. Out of many challenges, security is one of the primary concerns in IoT. Without proper security and privacy, the business model of IoT will not succeed. This chapter discusses the secure solutions for IoT using biometric features of users as well as end users. The chapter will demonstrate that biometric security is most feasible, reliable and efficient with respect to other existing security arrangements.

1. Introduction

The Internet of things (IoT) is the inter-connection of different devices of our daily life like cars, refrigerators, mobile phones, smart doors, devices for patient monitoring or any other monitoring devices. These devices are attached with smart sensor RFID tag, actuator and internetwork connectivity, which enable the devices to exchange or collect, and send data to a server. This type of technology is called

Internet of Things. IoT is basically combination of different fundamental types of technology and has different layer of communication level (see Fig. 1). Different level demands require different degrees of security arrangements. For the level where the direct human access is needed biometric security arrangements is highly recommended by researchers. Biometrics security arrangements ensure a scalable solution [1-4] for IoT to work against unauthorized access, ID swapping, and manual badge checks.

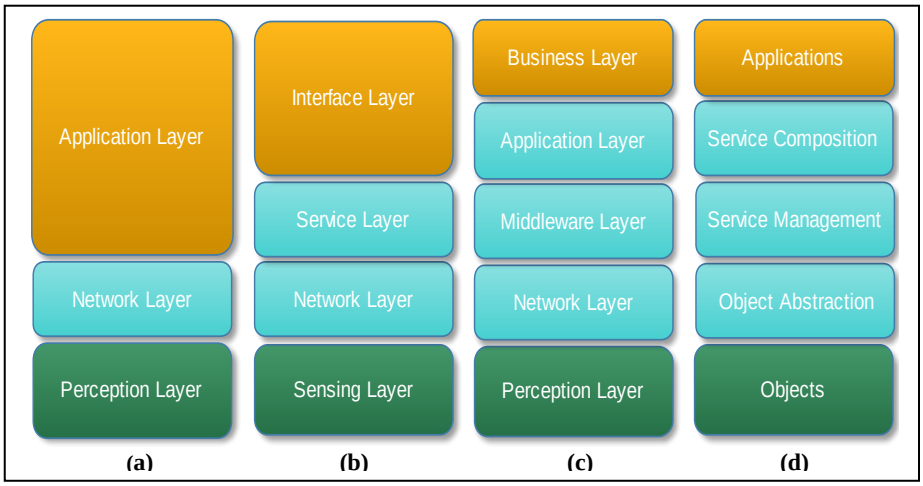


Fig. 1: IoT architecture: (a) 3-layer, (b) 4-layer, (c) 5-layer, and (d) SOA-based [5]

Biometrics deals with recognition of individuals based on their behavioral or biological characteristics. The human organs, which might be considered as biometric means should have the following major desirable properties: universality, permanence, uniqueness, performance, collectability, acceptability, circumvention [1-6].

Applications of IoT

There are several domains where IoT is being successfully implemented. The potentialities of IoT can still be exploited to develop new applications for the benefit of society. It can boost the role of Information and Communication Technology (ICT) so that the quality of our lives can be improved. In the application environments of IoT, smart objects can communicate with each other and represent a context perceived from the environment. The potentiality of IoT can be exploited in many domains like healthcare, transportation systems, environmental monitoring, personal and social, smart city, industrial control, and, any more. In this section, we discuss few promising application domains and pointed out their shortcomings.

***Smart environment* (*homes, buildings, office, and plant*)**: Sensors and actuators deployed or attached with house hold equipment like refrigerator, lighting, and air conditioners can monitor the environment inside a house, plant or office. The lighting system of a house can change according to the time of the day, like in the evening most of the lights will be on while they will be off late at night. Based on the reading of a temperature or a smoke detector sensor, a fire alarm can be set off automatically. Such type of application is very helpful for elderly people staying alone at home. Based on the movement of occupants in home, some appliances like doors in room can be opened, lights can be turned on at current room, and water taps/faucets will be open at kitchen. Air conditioners, refrigerators, and washing machines will now be IoT-enabled and controlled over Internet to save energy. In near future, a smart malfunctioning refrigerator will send a message to a service man automatically without user's intervention. Industrial automation is improved by deploying RFID tags with products. Production

process is controlled to ensure quality of product by getting different parameter values from sensors [1], [2].

IBM has launched Smart Home solution [7], better known as "Stratecast" to provide services to users allowing seamless communication among various smart devices in house, like medical devices, computers, mobiles, TVs, lighting, security and sound system. IBM is collaborating with Verizon as a communication service provider (CSP) and Philips as a device vendor to implement the architecture. Siemens, Cisco, Xerox, Microsoft, MIT and many others are working in this domain. They have set nearly 20 home labs using more than 30 home appliances, five network protocols and three Artificial Intelligence (AI) techniques [8]. The Intel smart home platform supports recognition of family members by voice or face and personalizes the home. Intel provides IoT solutions for smarter building to support personalization by controlling over the office/living environment, mobility by enabling managers to monitor property remotely, and sustainability and efficiency in terms of saving energy, water and other building resources.

Healthcare: Another impact area is healthcare [9], [10], where IoT can be used in tracking of people (i.e., patients and staff) or objects, recognition and verification of people, and automatic data collection [11]. Real-time tracking of person or objects in motion, in the case of patient-flow monitoring helps to manage staffing and improve the workflow in hospitals. Identification and authentication of staff secure the patients and help to avoid mistakes like wrong drug/dose/time. Automatic collection of clinical data must be enabled to enrich medical inventory. Real-time monitoring of patients is possible by attaching different sensors to measure body temperature, blood pressure, and heart response. These IoT-enabled sensors can detect abnormality locally and in no time, send this information to physicist. A community health service [12] has already been proposed with three-layer architecture to monitor the healthcare remotely from hospital. This application can prevent hospitals from overcrowding. Analyzing patient's data doctors can send advice through text/video/voice/email means. The limitation of such application is that there is no security and privacy of patient's data. Timely delivery of accurate response to critical patient is another challenge in this domain. The IoT-based application powered by artificial intelligence, called ambient assisted living (AAL) [13], [14] can assist elderly individual in his or her residence in a convenient and safe manner. In [15], a modular architecture, security, control and communication are included. The m-IoT promotes a mobile computing platform consisting of sensors, and communication technologies. In [16], authors describe eHealth, IoT policies and regulations in accessing healthcare services. The potentiality of m-IoT has been tested in noninvasive sensing of glucose level [17], body temperature monitoring [18], and blood pressure monitoring [13] for ambient assisted living. Pulse oximetry is noninvasive nonstop monitoring of blood oxygen saturation. IoT-based pulse oximetry is an integrated approach used in CoAP-based healthcare services [19], and remote patient monitoring [20]. However, implementing IoT technology in this domain has many challenges [17]. Context-awareness and m-IoT ecosystem are two prominent challenges in this area [17]. IoT is applied in electrocardiogram (ECG) monitoring to provide maximum information in real-time [21]. Research efforts have been done towards full automation of smart wheelchair based on IoT [22] for disabled people. Intel developed connected wheelchair which is connected with data driven machines [23]. Awareness around children's health [24] in monitoring emotional, behavioral, and mental health is exercised by a specialized IoT service called Children Health Information (CHI) where, an interactive totem may be positioned in a pediatric ward offering CHI services for educating, entertaining, and empowering hospital kids. The work in [25] proposes an IoT-based m-health service that can be used to develop a healthy nutritional habit among children. The potentiality of medical semantics and ontologies in providing huge medical information and knowledge influences IoT-based healthcare applications. A medical monitoring service called Semantic Medical Access (SMA) is proposed in [26] that is based on IoT sensors. To analyze large medical data stored in cloud medical rule engines may be employed in healthcare.

Despite its immense benefit to wellness of people, it throws many challenges. As health data is highly sensitive, if misused can deteriorate relation and destroy reputation among individuals. Data centers must be capable of handling of streaming and digitizing large volume health data. Without proper security of such data, there is a risk of cyber-attack. But implementing security measures in healthcare is constrained by the computational, energy, and memory limitation. As healthcare devices are mobile in nature, developing a mobility-compliant security algorithm is a big challenge. Moreover, standard rules and regulations for compatible interfaces and protocols are not followed by devices made by different vendors. It raises the interoperability issue in IoT. Immediate effort is needed for the standardization of IoT-based healthcare services. In [16], authors describe eHealth and IoT policies with regulations in accessing healthcare services. Many countries like Japan, France, China, and India have already announced eHealth policies.

Smart cities: Smart city is a cyber-physical ecosystem emerging by deploying advanced communication facility along with the novel services over a city [1], [27], [28]. Use of IoT in smart city optimizes usage of physical city infrastructure such as power grid, road networks, parking space, etc. and improves the quality of life of its citizens in cities [2], [29], [30] like Glasgow, Barcelona, Masdar, etc. It can be used to monitor the traffic in cities or highways and divert traffic accordingly in order to avoid congestion. Smart parking facility is made available to smart cars through RFID and sensors technology to find out currently available parking space nearby in city [31]. Using IoT sensors can send air pollution data such as amount of carbon-dioxide, etc. to an agency. A Smart City Platform is developed to smart waste management in a European city [32]. Sensor data can be used to detect violator of traffic rules and to analyze the accident scenarios.

Another important application of IoT that can be provided to citizens is water network monitoring and quality assurance of drinking water. To ensure high quality of water, sensors measuring critical water parameters are placed at important locations around the city. This technique eventually detects accidental contamination of drinking water, rain water, and sewage disposal. Smart grid and smart metering are being implemented around the World to ensure efficient energy consumption [33]. Using smart meters energy consumption is monitored at every electricity point in house and the information used to modify the way the electricity is consumed. Similarly, monitoring citywide electricity consumption pattern helps to balance load within the grid thereby ensuring good quality of service.

The sensors used in smart cities are vulnerable to physical as well as cyber-attacks. What will happen if a smart meter is tampered with? Associating authentication to a smart meter to avoid anonymous meter readings is difficult now. The data communication in smart city must be secured against such attacks.

Transportation and logistics: IoT is used heavily in intelligent transport systems and autonomous vehicles. Trains, buses, cars can now be equipped with sensors, actuators and processing power and can provide necessary information to passengers, drivers or agencies for better monitoring, and management in order to safely navigate passengers. Transported goods attached with RFID tags can be monitored and the status of delivery could be enquired through IoT. RFID and NFC provide wide market opportunity in the domain of supply chain management, transportation, inventory management, and mobile ticketing. Intel in collaboration with BMW group and computer vision leader, Mobileye, is working towards realizing the next generation platform for automated driving [34]. Cars are embedded with sensors, which can generate 360 degree of data. Intel processors transform the data into actionable insight to assist and/or automated driving. By 2020, self-driving is expected to have traffic signal recognition, emergency braking, pedestrian detection, park assistance, cross traffic alert and many more. Providing security for the connected cars and instant driving assistance is essential for safer, more productive and enjoyable travel. An intelligent monitoring system for refrigerator trucks is proposed in [35] to monitor temperature and humidity inside it using RFID, sensors, and wireless communication technology.

Personal and social: *Social Internet of Things* (SIoT),introduced by Atzori et al. [36] describes a world, where things around the human can intelligently sense and can form a network. SIoT helps individual to interact with other and maintain social relationship [37]. Twitter, Facebook are web portals through which people remain in touch with friends by getting and posting real-time updates [38]. Existing privacy and protection techniques in social networks may be imposed in IoT to improve the security of IoT. Tracking of IoT-enabled objects against losses or thefts is possible by developing applications. For example, smart objects such as laptops, mobiles will send SMS automatically to their owners on reaching a new location or unauthorized access. Many companies have implemented SIoT for their products for collecting data from users. These data are communicated over the Internet to social networks of people and devices who can respond to a problem, deliver a service, or sell a solution [39]. In the current scenario, implementing human-to-thing interactions is a challenge to achieve the complete vision of SIoT. Again, SIoT must be intelligent enough to starting, updating, and terminating the objects' relationships in SIoT. In SIoT, research must address issues like interoperability, device management, security and privacy, fault tolerance, and heterogeneity.

Agriculture: Agriculture is one of the emerging fields for implementing IoT [40-42]. If IoT can be implemented in third world countries like India, Bangladesh, Brazil where agriculture is the main profession then human effort can be used optimally. In [42], authors proposed a framework called AgriTech towards agricultural automation. Deploying sensors like humidity, nutrients and getting data from the field of agriculture farmers can save their time. The excess human effort can be used for the industrialization in these countries. The potential impact of IoT may be exploited in agricultural automation to optimize utilization of water, fertilizers and insecticides.

However, implementing AgriTech in third world countries is challenging due to initial setup cost. Sensors deployed in the field are vulnerable to physical attack. Again, improper deployment of sensors may result in unwanted information from field not belonging to the farmer.

Pharmaceutical industry: Safety and security of pharmaceutical products are of utmost important. In this view, smart labels are attached to drugs for monitoring their status while being transported and stored. Patients are directly benefitted from smart labels on drugs by knowing expiry, authentication, and dosages of medicines. Counterfeiting [43] in this area can be stopped by IoT. Smart medicine cabinet also helps patients to track timely delivery of medicines. In [44], a pharmaceutical intelligent system built on IoT has been employed to inspect drugs in order to perceive drug reaction, injurious effects of excipients, problems associated with liver and renal defect. It helps and assists physicians towards clinical decisions and prescription. Here, Near Field Communication (NFC) and barcode verification techniques are combined in different gadgets. Along with this drug, identity is matched with intelligent information system to detect the suitability of a drug for a patient.

In any IoT system huge amount of data transactions will take place. Some decisions and control signals or suggestions will be sent to the application. For ensuring security of those data, messages of suggestion and control signal, a strong and efficient authentication protocol will be needed.

The organization of this chapter as follows: Section 2 describes the traditional different types of biometric used in IoT applications. Biometric security system and its benefits to use in different IoT applications are discussed in Section 3. Different techniques to extract features from biometrics are given in Section 4. Section 5 provides the brief description of some biometric based security protocols for IoT application. Finally, we conclude this chapter in Section 6.

2. Types of IoT security

IoT security is the domain, which worries researchers and users due to the vulnerable attack on 'things' or connected devices and network. The maximum connection in IoT is derived from the devices, embedded sensor systems (ESS) employed in industrial communication, building computerization system, vehicle communication and wearable gadgets. Therefore, devices, which are connected in this giant network also raise the scope of potential attack for hackers and other cyber criminals. There are five types of attack that occur in IoT inter-networking systems [45-47]:

- Botnet is a network of systems, which take control remotely. Command-and-Control-Servers (C&C Server) is used to regulate the system and used by criminals for stealing private information, exploiting online-banking data, and phishing emails.

- Man-in-the-middle attack is a notion where the invader or hacker interrupts and breaks communication link between two discrete systems. The invader covertly interrupts and sends fake messages, but the sender and receiver believe that they are communicating via authentic message with each other.

- Data and Identity Theft occurs in case of careless handling of Internet connected devices such as, mobile phones, kindles, smart watches, etc. The goal of identity theft is the accumulation of data, which can say a lot about a person. The information accessible on the Internet including social media and smart devices gives an overall clue of personal identity.

- Social engineering is an action of influencing people so they hand over confidential information like device or email passwords or bank details. It also includes the installation of mischievous software that can open the door to access personal data. This type of threat can be done by phishing emails, or redirecting to websites like banking or shopping sites that look genuine but always ask or influence to enter secret information [3].

- Denial of Service (DoS) attack occurs when a service that usually works is unobtainable. A large number of systems maliciously attacks on a particular target in case of Distributed Denial of Service (DDoS) attack. This is done through botnet, where many devices are programmed to demand a service at the same time. This type of attack does not try to steal information or leads to security loss which affects reputation of a company that can cost a lot of time, money and reputation.

- A report by Hewlett Packard shows that 70% of the normally used IoT components are serious vulnerabilities [48]. These components have weaknesses due to absence of transport encryption, insecure website interface, poor software protection, and inadequate authorization. On average, each component contains almost 25 risks of compromising the home network. The properties, such as confidentiality, integrity, authentication, authorization, non-repudiation, availability, and privacy, must be guaranteed [49] [50] to ensure the security of IoT components. There are mainly four types of security requirements like, secure bootstrapping of objects and transmission of data, secure authentication and identification, security on IoT data, secure access to data by authentic users [1], [3].

The probable solution to certify security of things is identification technology (IT), which bids the mapping of unique identifier or UID, to an entity for making it unambiguous. UIDs may be made as sole measure such that the combination of their values is exclusive. In IoT, the 'things' have a digital identity (demonstrated by a unique identifiers), that is identified with a digital name and the relationships among 'things' can be specified in the digital field [51]. There are two categories of IoT security technique to

assign a UID to an entity or things, traditional, and biometric-based techniques. Traditional IoT security is either knowledge based (like, password, PIN or any type of personal information which can be used for Point to Point Protocol (PPP) to authenticate a user) or object based (like smart cards are implemented to deliver user verification by data storage). Smart cards offer a robust security confirmation for single sign-on (SSO) within big establishments, where biometric IoT security states the measurement associated with human characteristics. IoT biometrics validation or real-time verification is employed to recognize entities in groups that are under observation. As this chapter concentrates on biometric security in IoT, therefore it is explained in depth in the rest of the section.

2.1. Biometric Security in IoT

Biometric recognition or biometric security considers two grounds about human body characteristics, distinctiveness and permanence, [3], [52]. Some of the most popular physiological traits, which are used in IoT biometric security are fingerprint, face, iris, hand geometry, gait, DNA (deoxyribonucleic acid) etc. The selection of a biometric generally depends upon the necessities of the authentication application. For an example, voice biometric is suitable in mobile security matters because, the device which senses vocal sound is previously embedded in the mobile phone, and finest part of the IoT biometric authentication is that it can identify the person who is not registered in the system, but still trying to get the access. There are two types of biometrics modalities, physiological and behavioral [3] and brief description is made in the next sections.

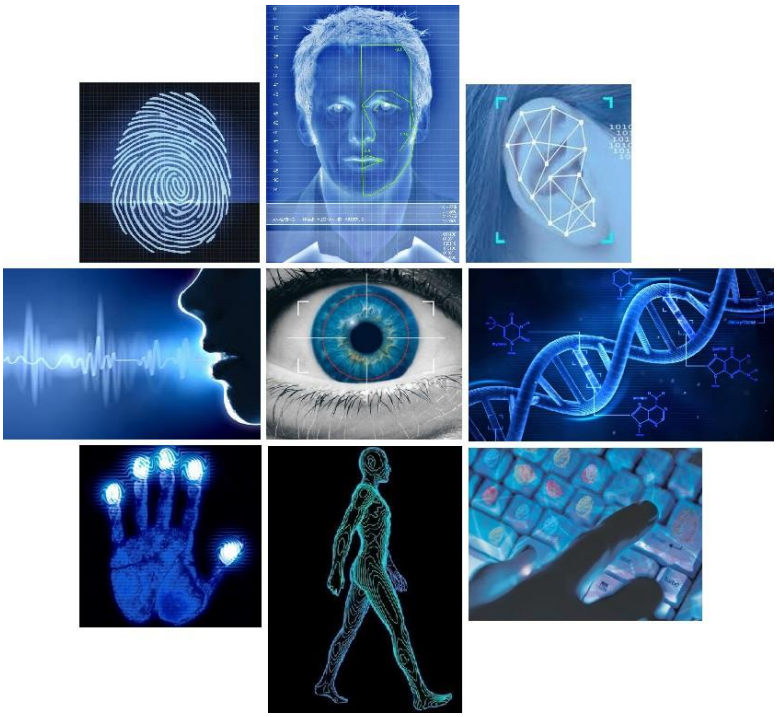


Fig. 2. Set of popular physiological and behavioral IoT biometrics

2.2 Physiological

Physiological features are based on direct measurements of a part of the human body, e.g., face, fingerprint, iris, and hand geometry recognition schemes belong to this category (see Fig. 2).

1. ***Face:*** Face recognition algorithms generally use relationship among the locations of facial features such as eyes, nose, lips, chin, and the global appearance of a face. State of art on face

recognition technology can be found in [53] [54]. There are some significant factors like brightness, motion, makeover, obstruction, and posture disparities, which disturb the execution of a face identification algorithm. Face is a widely accepted biometric and has a good level of accuracy in different environments.

2. ***Fingerprint:*** Fingerprint based recognition is the most successful and widespread method for person authentication in IoT. It contains a unique texture pattern, which is made of ridges and valleys for a person. These ridges are categorized using some points, known as 'minutiae'. Therefore, the spatial distributions are proved to be unique for a person [55]. These 'minutiae' points are used to match two different person's fingerprints. This biometric has received larger consideration since forensic departments of many countries employed Automatic Fingerprint Identification Systems (AFIS) for their purpose. Beside this many civil and commercial application also use fingerprint for authentication.

3. ***Iris:*** Iris is a colored loop around the pupil holds complex pattern in human eye, and it is scientifically proved that it contains unique characteristics for every human being. It has some individual characteristics like, stripes, pits, and furrows, which are being considered for proof of identity. The work of Daugman [56] showed the working principle of iris recognition, matching speed, and accuracy (is very high) of this biometric consideration. The pattern of the texture is steady and idiosyncratic here [56]. Some large-scale systems integrate iris authentication as a part of their identification procedures. It is also noticed that lack of legacy for iris pattern databases may be a challenge for several government applications.

4. ***Palm Print:*** Palm print is another popular and well accepted biometric which is used in IoT security systems. It contains distinct ridges and flexion creases like fingerprint [57] [58]. Mainly, forensics are used this scheme and research shows 30% of palm print samples are being collected from criminal cases (like, knifes, guns, etc.). Minutiae and creases are considered for matching and finding out the required palm print or person. Many palm print samples are available in the databases, which are gathered by forensics. Generally, the resolutions of these samples are low around (75 dpi). From the research point of view, it is a challenge to extract the texture features for feeding into intelligent expert systems.

5. ***Hand Geometry*****:** It is demanded that identification of persons can be made based on the shape of their hands [59] [60]. Identity verification by hand geometry employs low-resolution hand pattern images to extract geometrical features such as finger length, width, thickness, perimeter, and finger area. The accuracy of person authentication by hand geometry is quite limited. Due to this reason hand geometry is used in 1:1 matching for low safety access mechanism and measurement of attendance like areas. The physical size of the hand geometry measurement systems is large; therefore, it is hard to embed those systems in existing security systems for IoT biometric based security schemes.

6. ***DNA* (*Deoxyribonucleic Acid*)****:** DNA is present in each cell of a human body and composed of genes. This is a hereditary and highly stable material, which is utilized to represent physiological characteristic and identify person [61]. Usually DNA is unique for each person except identical twins. Patterns of DNA are developed from different body parts like, hair, finger nails, saliva and blood. Forensics and law enforcement agencies first make a unique profile of a DNA using some intermediate steps and then the matching process is conducted. This process is very expensive and time consuming. Also, DNA profiles may get contaminated if they are not done in an ideal environment. Therefore, it is challenge to make an automated IoT security using DNA, and not appropriate for outsized biometric implementation for public usage.

7. ***Hand Veins:*** The configuration of blood vessels concealed under the skin is distinct in persons, even among the identical twins and constant over long period of time. The veins present in hands (e.g., palm, finger and palm dorsal surface) are acquired by near infrared illumination and employed for person authentication [62]. The pattern of veins is steady for adult age, but changes after that because of bone and muscle strength; also sometime due to diseases. Till now there is no known large scale vascular biometric system. Therefore, it is challenging to make hand vein recognition based IoT security because of cost of the system and absence of large scale studies on vein uniqueness and steadiness. Beside this, these systems are touchless, which repeatedly pleas to the user.

2.3 Behavioral

Behavioral features are one kind of indirect human characteristics measurement through the feature extraction and machine learning. Some popular behavioral biometrics are signature, key stroke dynamics, gait, and voice [63] which are elaborated later (shown Fig. 2).

1. ***Gait:*** Human walking pattern is considered as the gait, which is almost unique for each person and has the potential to demonstrate a person based on his or her gait biometric. Wearable and non-wearable sensors are used to capture the gait data and later statistical features are extracted to explain the complex gait dynamics for a person [64]. Then a machine-learning model is trained to recognize a person using these features. There are several important parameters like, velocity, linear distance between two successive placements of the same foot, linear distance between the placements of both feet, number of steps per time unit, linear distance between two equivalent points of both feet, and direction of the foot during the step, which are used to describe a gait pattern. Generally, gait biometric is used for medical and health care applications, but these days it is being implemented for IoT biometric applications also.

2. ***Signature:*** This is another behavioral biometric, which is used every day for business transactions. Academics and industry have made several attempts for concrete signature recognition model which is not successful yet. These systems capture the characteristics of signature by measuring the pressure sensitive pen pad. The shape, speed, acceleration, and speed of strokes are captured from the real time signing [65]. These features are learned using machine-learning algorithms to improve the signature recognition and verification performance along with circumvent signature forgeries. However, very few automatic signature verification systems have been deployed.

3. ***Voice:*** Speech or voice recognition schemes find the persons based on their vocalized words [66]. Human voice includes a mixture of behavioral and physiological characteristics. The physiological factor of voice relies on the shape and size of vocal tracts, nasal cavities, lips, and mouth. The behavioral elements are established by the movements of jaws, lips, tongue, larynx, and velum, and can change with the person's age. Another side, duration, intensity, pitch information and quality are the spectral information to train a machine learning system, which would be able to verify a person's identity by the vocal sound. Voice biometric is mainly used for verification purpose.

4. ***Keystroke:*** It states the skills are established for automatic person authentication based on the learning of typing patterns. These technologies present numerous problems related to demonstrating and matching dynamic orders with high intra class variability (e.g. samples from the same user show huge differences) and variable performance (e.g. human behavior is strongly user-dependent and varies significantly between subjects) [1], [2], [63],[67].

3. Biometrics Security and Internet of Things (IoT)

This section discusses the biometric security system and its benefits in different IoT applications.

3.1 Biometrics Security System

Matching problem of the identity can be classified into two different types of problems with different complexity: (a) authentication, and (b) recognition or identification. Verification proves or disproves a claim of a person whereas identification process identifies. Fig. 3 depicts the scenario of biometric used in the security system.

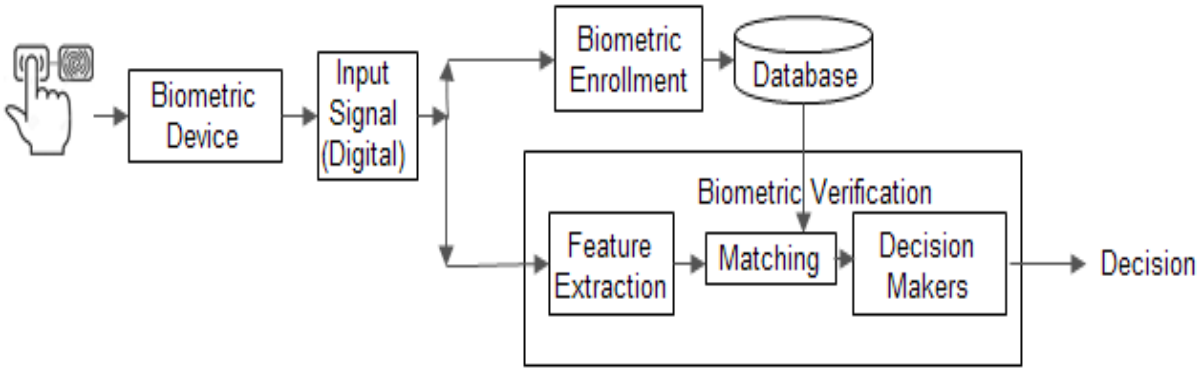


Fig 3: Working procedure of biometric security system: a part of IoT system

Table 1 shows the performance comparison of different biometric organ of human being. Table 1 is given to compare different type of biometrics like, finger print, hand geometry, voice, retina, iris, signature, face etc. However, though the accuracy, ease of implementation for fingerprint is higher than the signature of people, still signature (biometric type) is more popular than fingerprint.

Biometric type	Accuracy	Ease of use	Acceptability of users	Implementation viewpoint	Cost
Fingerprint	⇑	⇳	⇓	⇑	⇳
Hand geometry	⇳	⇑	⇳	⇳	⇑
Voice	⇳	⇑	⇑	⇑	⇓
Retina	⇑	⇓	⇓	⇓	⇳
Iris	⇳	⇳	⇳	⇳	⇑
Hand writing	⇳	⇳	⇑	⇓	⇳
Face	⇓	⇑	⇑	⇳	⇓

⇑ : High, ⇓ : Low, and ⇳ : Medium

Table 1: Comparison of the popular biometric technologies [68]

3.2 Comparison of biometric security over other conventional security system

Biometric-based security is far better than password based/PIN based security. Biometric-based security has many advantages over conventional password based security system which are discussed below:

1. *Accurate information*: Biometric-based security can get accurate more secure information than PIN/password based security systems. No need to remember the password/PIN by the user or no evil person can break the security by duplicating, guessing or hacking the password from the server of the system.

2. *Easy and safe for use*: Biometrics is very easy and safe to use. Hackers cannot posses the biometric information of the legitimate users.

3. *Accountability*: A person who is using a system using biometric cannot deny the activity, which has been done by him in future. Therefore, it can be said that the accountability of a system will also increase from the user end for any kinds of malfunction, misuse of the system.

4. *Security of biometric information*: Biometrics cannot be guessed or stolen. Therefore, it may provide a long-term security solution. However, in the password systems, a sequence of numbers, symbols and letters are used to build a password, which is very tough to remember. Furthermore, in the token-based system, token can be stolen easily or lost. Therefore, both the password and token-based systems have a high risk to use as the secret information is being shared or disclosed. In such case, verifier may not be sure about the legal user. But, these would not be the case with biometric characteristics, and thus biometric-based systems are free from the problem of fraud, sharing, and duplication.

5. *Scalability*: Biometrics-based systems provide flexibility and scalability from the users' viewpoints. Users can use higher versions of sensors and security systems based on their needs. User can use their characteristics, which are not very discriminative. However, to get the higher level of security in a large-scale database of a user with higher identification accuracy, this kind of systems can be used with more discriminable features. This is because chances of collision of hash value of biometric are lower than the in conventional security systems.

6. *Time saving*: Biometric identification is very fast to execute, which is another advantage over other traditional security techniques. A person can be verified (i.e., rejected or accepted) in a fraction of seconds. Moreover, the use of this technology can only be beneficial to the office revenue by increasing productivity and reducing costs by removing fraud and wastage of time in the verification process.

7. *User-friendly systems*: Users can install the biometrics systems easily into their e-devices and then, they can do their job uniformly, quickly, and reliably. To understand the operational functionality of the biometric system, minimum amount of training is needed for the users, and there is no need for expensive password administrators. New problems are arising with the aging of the population due to increased life expectancy and declining birth rate. Now a days, there are 600 million aged people in the world. The number will be doubled in 2025 and will reach $\approx$ 2000 million in 2050. Therefore, user friendly system is very much mandatory for the aged people who will use IoT system as end user.

8. *Convenience*: It is a convenient security mechanism because people do not need to remember passwords, as well as do not need to carry secret documents or identity cards for verification.

9. *Versatility*: Nowadays, different types of biometrics scanners are available in the market and they are suitable to use in various applications. Many organizations and companies use the biometric devices at the security check points like, doorways, entrances, and exits. Beside this, users can build the most out of the biometric mechanism to obtain the knowledge about accessibility on the systems. Companies also use such biometric scanners to monitor the entry or exit time of an employee and their attendance. In case of the remote patient monitoring systems, the biometric identity can be used to send an emergency message to a rescue team of remote patient monitoring system. A soldier can ask help to get rescue from danger situation by pressing a button, which is basically a transmitter along with biometric identification system. Thus, it can be said that the biometric security systems have versatile applications in different IoT environments.

10. *Return on investment*: This is definitely high, because human can avoid fraud including "buddy punching", besides lowering payroll costs, accurate computation of work hours, and reduced management time. While the security is enhanced, users can also easily apply consistent policies and procedures at the same time. More thinking is required about the initial cost of the biometric system. Industries can benefit from biometrics systems to a great extent. Rather than remembering the password, biometric systems offer unique biometrics information for individual so that users can get their accessibility to obtain services after verification. Therefore, from business point of view biometric technology is very much profitable.

Authentication Procedure	Advantages	Drawbacks
Handheld tokens (Card, ID, and passport)	• A new one can be generated • People can get same facility to the different country by accessing the tokens as it seems to be standard.	• It can be stolen. • A fake or duplicate can be generated. • It can be shared. • A user can register him/herself with several identities.
Knowledge based (Password and PIN)	• It is a manageable and has low cost to fabricate. • For any problem, it can be replaced with new one easily.	• It can be guessed or cracked. • Long or complicated password is hard to remember. • It can be distributed. • A user can be registered with different identities.
Biometrics	• It cannot be guessed, lost, forgotten, stolen, and shared. • One person with multiple identities can be verified easily. • It provides a greater degree of security than others	• For any problem (Oily skin for fingerprint), replacement is not possible. • It is impossible to replace if biometric data of a person is stolen.

Table 2: Comparison of three main authentication approaches [69]

3.3 Benefits in Using Biometric-based Security Schemes for IoT applications

Biometric-based security can be used in every application area of IoT. Biometric used in the application level where man and machine interaction is required. Fig. 4 describes the security system needed in

different application areas. Security systems can be usable in smart home systems. A person can use smart lock system in the door using biometric locking system. An old person can report his/her health condition by login to the IoT health care system using biometric identification/verification system. In the IoT of transportation systems, the system can verify the identity of an end user while parking a car or paying a traffic fine etc. Traffic police can verify whether a car belongs to a driver or not using a biometric verification means. Before using the IoT applications, which are related to national project or application area like smart grid [68] or defense applications, an end user needs to verify his/her identity using biometric security to increase the reliability of the system. Biometric security can be useful in case of IoT health care systems [69]. All the medical persons need to pass biometric verification before prescribing or accessing the data of a patient. If any person faces any accident then biometric information is able to help identity and get his medical history. Presently, researchers are trying to introduce the IoT in agricultural systems [70]. Third world countries like India, Indonesia, Bangladesh etc. are the largest producers of food grain, but farmers in these countries have very low literacy rate. Therefore, it is mandatory that the IoT in agricultural systems should be easy to use. Here, biometric security systems are very much easier to use. Therefore, biometric-based systems are very useful in agricultural IoT systems.

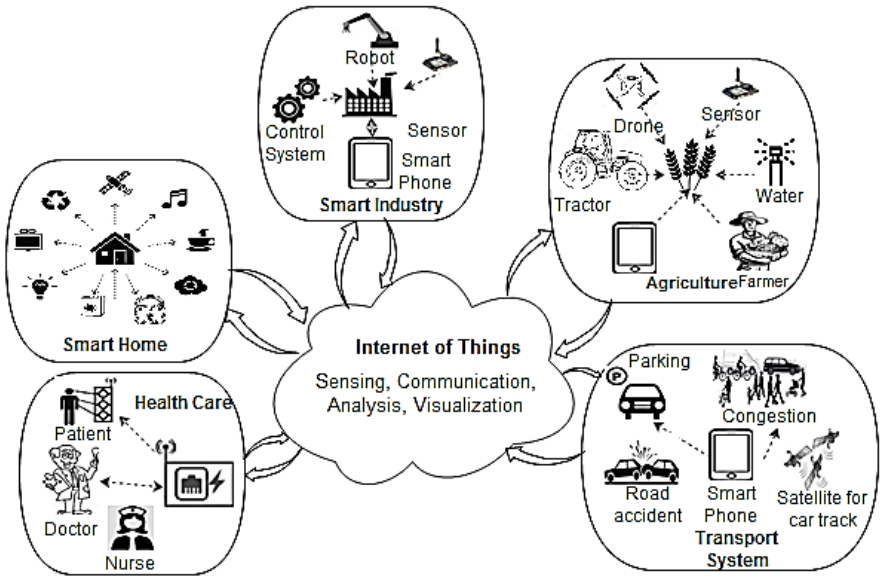


Fig. 4: End users and application areas based on data in IoT

The IoT enables the objects so that they can participate in daily activities. However, in complex system, controlling such objects along with their security is a very challenging task. Generally, IoT is a scope where persons relate to the technology built on smart devices. Relations of four IoT components i.e., individual, intelligent devices, high-tech ecosystem, and method, provide a complete and perceptive characteristic for IoT security. In this regard, secrecy on human information is required when they interact with the smart technological ecosystem. Similarly, during the communication with the control processes, safety on data should be guaranteed. Methods should safeguard their dependability and preserve the aims. Beside this, due to the increasing autonomy of objects, IoT security based on cognitive and systemic techniques is going towards a greater autonomy so that the different security threats can be protected. Here, we will discuss the role of each actors i.e., i.e., person, intelligent and smart devices, technological ecosystem, and process in IoT security to highlight the research issues.

According to [71], the major component of IoT can be categorized in four different nodes. There are four numbers of fundamental node and they are *process*, *person*, *technological eco system*, and *intelligent object*. In the imaginary, those nodes form a tetra hadron shape due to the nonlinear relationship amongst

them. Four planes of that tetra hadron represent different scenarios of security management system of IoT like safety, security, access and cyber security (see Fig 5).

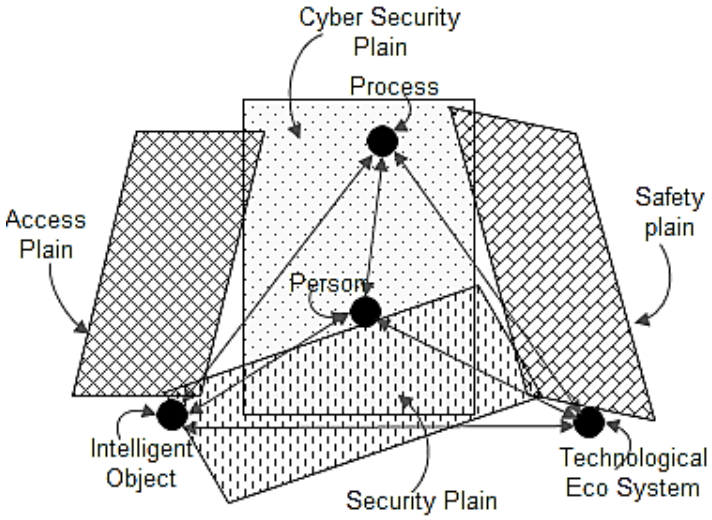


Fig. 5: Tetrahedron shape of security system in IoT [72]

Fig. 6 is the representation of each plane of Fig. 5 in two-dimensional area. From Fig. 5, it can be said that safety, security and access plane consists of a node named as person. According to [72], the edge of each side is named as tension.

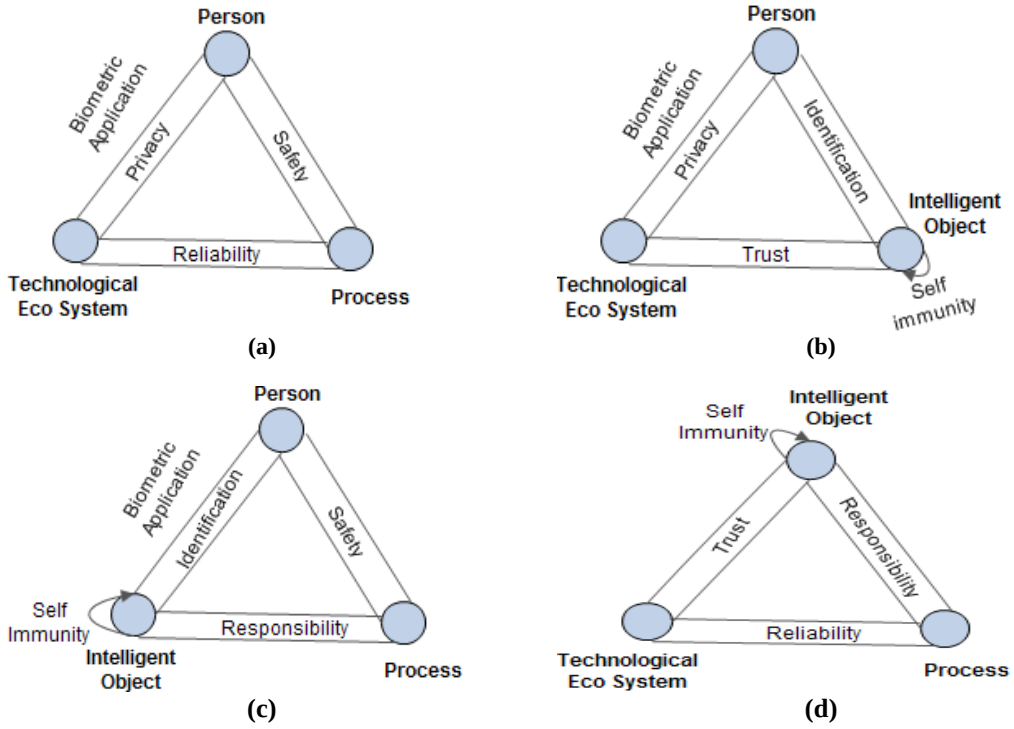


Fig. 6: Projections of the 3D-pyramid on each of the planes: (a) safety plane, (b) security, (c) access, and (d) cyber security [72]

4. Feature Extraction and Biometrics

Several applications are employed to ensure the identity of a 'thing' in the IoT paradigm. Examples of such applications include secure and reliable access to smart buildings, mobile phones, cloud databases, ATMs, etc. Therefore, these systems are vulnerable without a robust verification algorithm. The emergence of biometric-based identification or verification systems has pointed out to the problem that affects traditional verification methods by using physiological or behavioral features related to the person under consideration. IoT biometric systems use hand geometry, fingerprints, retina, iris, face, signature, voice, among others, to validate a person's uniqueness. A simple IoT biometric system contains four components: (a) sensing or acquisition, (b) feature extraction, (c) pattern matching, and (c) decision making [73]. A typical biometric authentication enabled IoT architecture is shown in Fig. 7, where fingerprint biometric based verification is considered to get access control over the 'things'.

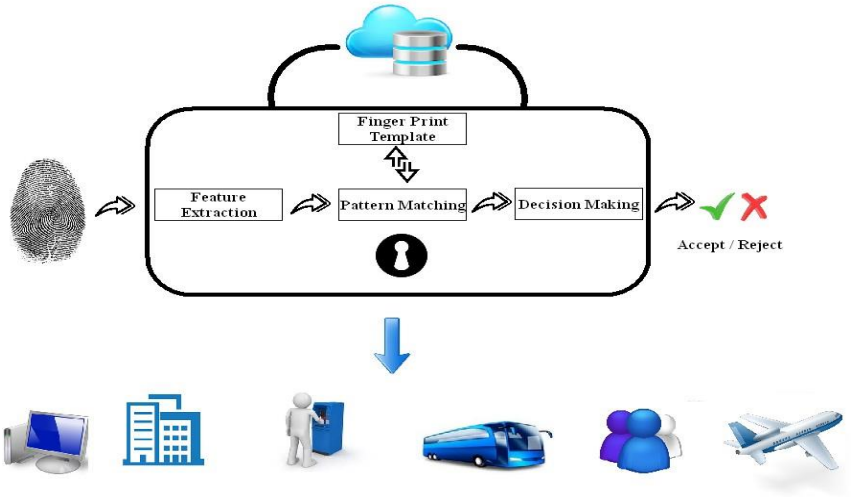


Fig. 7: Framework of IoT biometric-based security system

According to Fig. 3, a brief description on the components is included here, and feature extraction unit is described later.

- *Sensor or acquisition module*: It obtains the biometric of an individual. As an example, fingerprint sensor captures the fingerprint impressions of a user (see Fig. 3).
- *Feature extraction module*: The assimilated data is managed to extract feature values. As an example, the positional and orientation related features are extracted from a fingerprint image in the feature extraction module of a fingerprint recognition system.
- *Matching module*: The feature values are compared and calculated against the template by making matching. An example, here the matching score is calculated between query and template in this module, which helps in the next section.
- *Decision-making module*: The requested identity is either rejected or accepted here based on the similarity score.

The effectiveness of a biometric scheme is assessed by taking account the True Positive Rate (TPR) and False Positive Rate (FPR). These two measurements are graphed together in Receiver Operating

Characteristic (ROC) curve, which plots TPR against FPR. As per the interest of this chapter next sections are focused on feature extraction module.

4.1Different Techniques to Extract Biometric Features

The framework of IoT biometric security shows the fingerprint template is fed into a feature extractor module, which transforms the template image into a set of features or feature vector. These features contain distinct properties of the input patterns that assist in discriminating between the classes of input patterns. The idea of feature extraction and the selection of features in a computer vision problem are highly reliant on the specific problem at hand. There are two types of feature extraction methods in computer vision: low-level and high-level feature extractors. Low-level feature extractor transforms the visual content of a biometric template by associating features such as color, gradient orientation, texture, and shape with the content of the input template. For example, link an extracted color such as blue with the sea or sky, white with a car or dress, red with an apple, and so on, whereas high-level algorithms are typically associated with the machine learning field. These procedures are concerned with the transformation or classification of a scene. Multiple methodologies are presented for each of these visual features and each of them symbolizes the feature from a different perception. Some popular feature extraction techniques are described in the next section.

Fourier Transform (FT)

Fourier Transform is a concept, which states that any function can be expressed as the integral of sines and/or cosines multiplied by a weighting function. The function, stated in a FT, can be reconstructed completely via an inverse procedure. These significant properties of FT allow working in the 'frequency domain' and then reappearance to the original form without missing any information. The Fourier transform, *FT*(*s*) for a single variable, and *f*(*a*) continuous function, is defined below:

$$FT(s) = \int_{\infty}^{\infty} f(a) e^{-j2\pi sa} da$$

Where$j = \sqrt{-1}, and$ the Inverse Fourier transform (IFT) is given by:

$$f(a) = \int_{\infty}^{\infty} FT(s) e^{j2\pi sa} ds$$

These two forms indicate no loss of information in forward and inverse FT. These mathematical expressions are easily mapped for two variables, *s* and t:

$$F(s,t) = \int_{\infty}^{\infty} \int_{\infty}^{\infty} f(a,b) e^{-j2\pi(sa+tb)} dadb$$

Also, inverse transform is,

$$f(a,b) = \int_{\infty}^{\infty} \int_{\infty}^{\infty} F(s,t) e^{j2\pi(sa+tb)} dsdt$$

FT is complex valued function of frequency, where absolute part indicates that the frequency exists in the original function, and complex part indicates phase offset of the frequency. These frequency components are used as feature value for further classification or learning algorithms. FT is a useful feature extraction and filtering means for face, gait, voice, speech, and heart beat recognition [74], [75].

Local Binary Pattern (LBP)

LBP is an efficient texture operator. It labels the pixels of an image by thresholding the neighborhood of each pixel and contemplates the consequences as binary numbers or patterns. This was first proposed in 1990 [76]. LBP is popular for biometric applications [77], [78] in machine learning domain because of its high discriminative power and computational simplicity. This is usually a divergent statistical and structural model of texture feature extraction and robust to monotonic gray-scale changes caused by illumination variations. LBP divides the input window template into cells (e.g. 16×16 pixels for each cell). The objective patterns are usually extracted in a circularly symmetric neighborhood by comparing each image pixel with its neighborhood, which is expressed by:

$$LBP(P,R) = \sum_{i=0}^{P-1} u(g_i - g_c)2^i$$

Where, P is the number of neighboring samples and R is the radius of neighborhood, g_i denotes the intensity value of neighboring pixel $I(i = 0, \dots, P-1)$, g_c is the intensity value of the center pixel, and $u(x)$ is a step function with:

$$u(x) = \begin{cases} 1, \text{for } \ x \geq 0 \\ 0, \text{otherwise,} \end{cases}$$

The intensities of neighboring pixel values, which do not fall exactly on the image grid are obtained by bilinear interpolation. Then, after getting the interpolated template from the function $LBP(P, R)$, we find: a histogram h_i which is the total number of observations, the total number of bins (b), and the histogram m_i that counts the number of observations that fall into the specified bins defined as:

$$h_i = \sum_{i=1}^{b} m_i$$

This histogram is used as a feature vector later on for the input of a machine learning algorithm. An example to generate local binary pattern is included in Fig. 8, where a center pixel value 70 is surrounded by 8 neighboring pixel intensity values. It shows the differentiation among the pixels and thresholding to make a binary pattern. After differentiation and thresholding, the binary pattern will be: 11110000. Then the final decimal value 15 is substituted instead of 70.

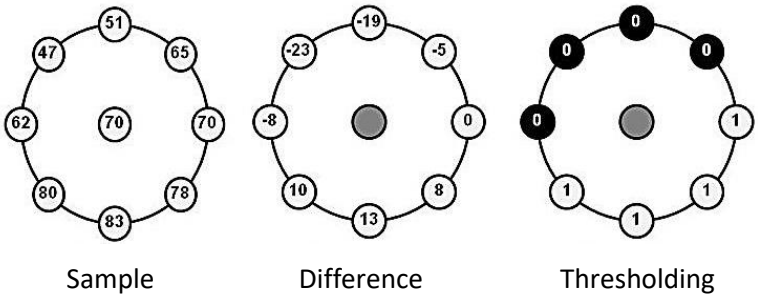


Fig. 8: An example of Local Binary Pattern generation

Gabor filtering (GF)

Gabor filtering is popular feature extraction technique in computer vision domain. It is widely used for biometric authentication also. GF is an efficient texture feature descriptor for palm print, face, fingerprint, and iris image template [79], [80]. Gabor elementary functions are Gaussians modulated by sinusoidal functions. It is shown that the functional form of GFs conforms closely to the receptive profiles of simple cortical cells, and GF is an effective scheme for image representation A two-dimensional (2D) even Gabor filter can be represented by the following equation in the spatial domain:

$$G(x, y; \theta, f) = e^{-\frac{1}{2}\left[\frac{x'^2}{\delta_{x'}^2}+\frac{y'^2}{\delta_{y'}^2}\right]}\cos(2\pi f x')$$

$$x' = x\cos\theta + y\sin\theta$$

$$y' = y\cos\theta - x\sin\theta$$

where f is the frequency of the sinusoidal plane wave along the direction θ from the x-axis; $\delta_{x'}$ and $\delta_{y'}$ are the space constants of the Gaussian envelope along x' and y' axes, respectively. Therefore, GF over different frequency and directions are considered as feature values for a biometric pattern. Fig. 9 shows an input template of finger print and its enhanced version using the GF, where the enhanced version Fig. 9(b) contains smooth edges than the input Fig. 9(a).

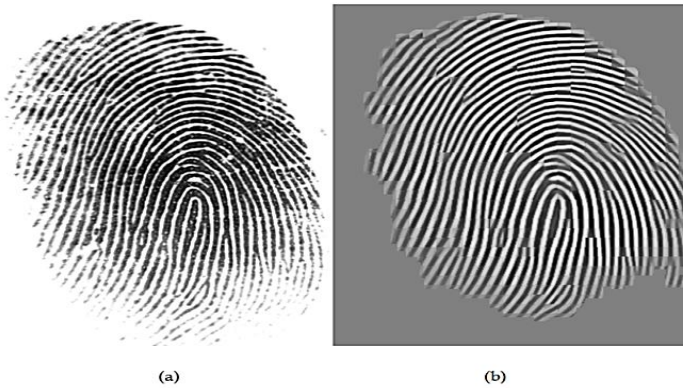


Fig. 9: Finger print enhancement using GF

Radial Zernike Polynomials (RZP)

RZP is first proposed by Fritz Zernike in 1934 [81]. It is useful in describing the wave front data since these are of the same form as the categories Zernike Polynomials of aberrations often experimented in optical tests. This is a well-known shape feature descriptor in computer vision domain. The complex Zernike moments of order *n* with repetition l are defined as,

$$A_{nl} = \frac{n+1}{\pi}\int_0^{2\pi}\int_0^{\infty}[V_{nl}(r,\theta)]^{*} f(rCos\theta, rSin\theta) r dr d\theta$$

Where, $n = 0, 1, 2, \ldots, \infty$ and *l* take on positive and negative integer values subject to the conditions:

$$n - |l| = even, |l| \leq n$$

The symbol '*' denotes complex conjugate. The Zernike polynomials:

$$V_{nl}(x,y) = V_{nl}(rCos\theta, rSin\theta) = R_{nl}(r)e^{il\theta}$$

are a complete set of complex-valued functions orthogonal on the unit disk $x^2 + y^2 \leq 1$,

$$\int_0^{2\pi}\int_0^{\infty}[V_{nl}(r,\theta)] * V_{mk}(r,\theta) r dr d\theta = \frac{\pi}{n+1}\delta_{mn}\delta_{kl}$$

The real-valued radial polynomials $\{R_{nl}(r)\}$ satisfy the relation:

$$\int_0^1 R_{nl}(r)R_{ml}(r) r dr = \frac{1}{2(n+1)}\delta_{mn}$$

and are defined as:

$$R_{nl}(r) = \sum_{s=0}^{(n-|l|)/2}(-1)^s \frac{(n-s)!}{s!\left(\frac{n+|l|}{2}-s\right)!\left(\frac{n-|l|}{2}-s\right)!} = \sum_{k=|l|, n-k=even}^{n} B_{n|l|k} r^k$$

The function *f*(*x*, *y*) can be expanded in terms of the Zernike polynomials over the unit disk as:

$$f(x,y) = \sum_{n=0}^{\infty}\sum_{\substack{l=-\infty \\ n-|l|=even \\ |l|\leq n}}^{\infty} A_{nl}V_{nl}(x,y)$$

Where, the Zernike moments A_{nl} are calculated over the unit disk. If the series expansion is truncated at a finite order *N*, then the truncated expansion is the optimum approximation to *f* (*x*,*y*):

$$f(x,y) \approx \sum_{n=0}^{N}\sum_{\substack{n-|l|=even \\ |l|\leq n}} A_{nl}V_{nl}(x,y)$$

Therefore, if maximum value of radial degree n = 5, and azimuthal degree m = 5 are considered then, 21 radial Zernike polynomials are generated from unit disk for each gait pattern; this means 21 features can be generated or the feature vector length is 21. Zernike polynomials are very popular in iris, and face recognition research [82], [83].

Scale-Invariant Feature Transform (SIFT)

SIFT is a procedure in computer vision to identify and define local features in a template. This is a high-level feature extraction algorithm in machine learning domain. The method is patented in the United States by the University of British Columbia and first published by David Lowe [84]. It takes the original input template, produces gradually blurred images and converts original image to its half of size. Mathematically, 'blurring' is known as the convolution of the gaussian operator and the image template. It has an operator that is applied to each intensity value and that results a blurred image.

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y)$$

Where the symbols, L is a blurred image, G is the Gaussian Blur operator, I is an image, x and y are the location co-ordinates, σ is the scale parameter; this means that the greater the value is, the greater the amount of blur, * is the convolution operator in x and y, which uses Gaussian blur G over the image I. The mathematical expression of Gaussian blur operator is given by:

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-\frac{(x^2+y^2)}{2\sigma^2}}$$

Now these blurred images are used with another set of images, which is the *Difference of Gaussians* (DoG). Those are then used to calculate *Laplacian of Gaussian* (LoG) approximations that are scale invariant. There are two parts to find out key points: (a) locate maxima/minima in DoG images, and (b) find out sub pixel maxima/minima. This is done by the Taylor expansion of the image around the approximate key point. Mathematical expression can be written as:

$$D(x) = D + \frac{\partial D^T}{\partial x} x + \frac{1}{2} x^T \frac{\partial^2 D}{\partial x^2} x$$

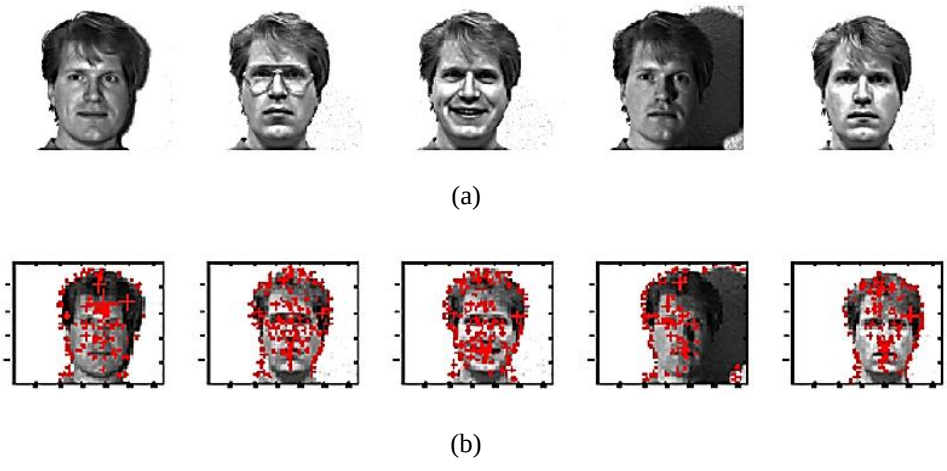
It is easy to find out the extreme points of this equation which increase the chances of matching and stability of the algorithm. After that, the extreme points are needed to be free from low contrast key points. If the magnitude of the intensity at the current pixel in the DoG image (i.e., being checked for minima/maxima) is less than a certain value, it is rejected. Now gradient directions and magnitudes around each key point are collected and we can figure out the most prominent orientation(s) in that region. Then these orientations are assigned to the key points. Gradient magnitudes and orientations are computed using these formulae:

$$m(x, y) = \sqrt{\big(L(x+1, y) - L(x-1, y)\big)^2 + \big(L(x, y+1) - L(x, y-1)\big)^2}$$

$$\theta(x, y) = \tan^{-1}\left((L(x, y+1) - L(x, y-1))/(L(x+1, y) - L(x-1, y))\right)$$

Finally, a histogram is created for 360^0 of orientation and are broken depending upon the problem statement. A typical example of the outcome of SIFT algorithm is included in Fig. 10 where (a) are the input images of face and then LoG is used to find out the key points on each face image and resultant

images are shown in (b). There are many researchers who used SIFT as a high-level feature extractor [85], [86].



(a)

(b)

Fig. 10: (a) Input set of facial expression image, (b) detection of scale invariant key points from the input template

As per the focus of the chapter, some famous, efficient, and robust biometric feature extraction techniques are discussed here for IoT. But, the evolution of Deep Learning and its high capacity for learning the different categories are slightly changing the choice of the people. This giant Deep Learning algorithm itself is a perfect package for pre-processing, feature extraction, and classification steps, and it is going to change the way researchers think today. It will open huge research scopes for IoT, Big Data, and Machine Learning.

5. Secure Biometric based IoT Systems: A Review

Section 5.1 demonstrates several applications of IoT like e-health systems. Based on the applications viewpoint, in this section, we discuss some application based biometric security protocol in details.

5.1 Biometric based e-Health System: An Authentication and Key Agreement Approach

Maitra and Giri [87] proposed a biometric based authentication and key agreement scheme for secure communication in medical systems. In such systems, a patient can get his/her treatment from home by accessing his/her biometric smart card using a mobile device through the Internet. For this purpose, patients do their registration to an authentication server (*AS*) to get their biometric smart card, and then they can get several medical services from medical servers (*MS*) by punching their smart card. Fig. 11 shows the network structure of the scheme of Maitra and Giri [87].

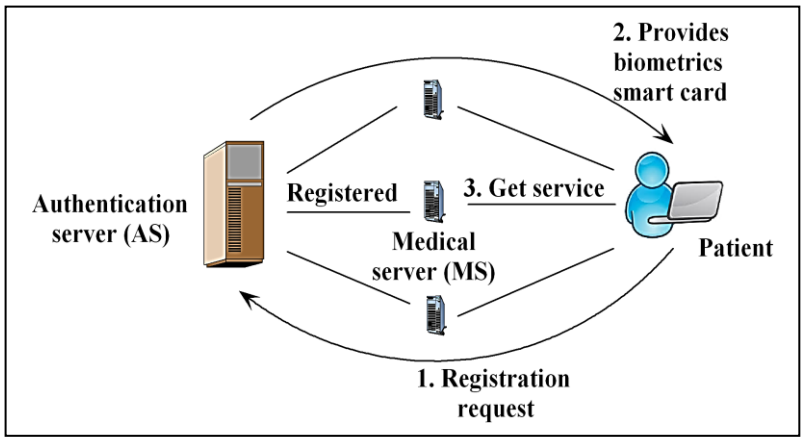


Fig. 11: Network structure of Maitra and Giri's scheme [87]

5.1.1 Description of Maitra and Giri's Scheme

There are four phases of Maitra and Giri's scheme [87]: (a) setup phase, (b) registration phase, (c) login phase, and (d) authentication and session key agreement phase.

Setup Phase

The authentication server (*AS*) makes two large prime numbers x and y such that $x = 2y+1$. *AS* picks a secret key $d \in_R Z_y^*$, where Z_y^* is the set of integer numbers (except 0) over modulo y. *AS* also selects a cryptographic one-way hash function $f(.)$: $\{0,1\}^* \rightarrow Z_y^*$. Finally, *AS* declares y and $f(.)$ publicly and keeps d as secret. Note that, cryptographic one-way hash function is collision resistant as defined in [2], [88].

Registration Phase

All the medical servers (*MS*) and the patients do their registration under the authentication server (*AS*) in this phase.

- ***Registration phase of medical server***

By performing the following steps, a medical server MS_i performs its registration under *AS* by executing the following steps:

Step1: MS_i picks its identity MID_i and transmits it to *AS* using secure channel. As the registration is performed only one time in offline mode, thus the communication pattern can be termed as secure channel.

Step2: After getting MID_i from MS_i, *AS* picks a number a_i randomly from Z_y^* and calculates the unique secret key S_{key}^i of MS_i as $f(a_i \| d)$. Then, *AS* supplies S_{key}^i to MS_i secretly.

- ***Registration phase of patient***

A patient P_i does his/her registration under *AS* by executing the following steps:

Step1: Sensor of mobile device scans the biometric of patient P_i and extracts the biometric feature b_i, by following a suitable technique as discussed in Section 4. P_i selects a unique identity

PID_i and password pw_i through mobile application. Then the mobile device of P_i computes $bpw_i = f(pw_i \| b_i)$ and sends $\{PID_i, bpw_i\}$ to *AS* via secure channel.

Step2: Upon getting $\{PID_i, bpw_i\}$, *AS* calculates $A_i = f(PID_i \| d)$, $C_i = bpw_i \oplus A_i$ and $D_i = f(A_i \| PID_i \| bpw_i)$. AS further computes p number of key-plus-id combinations $\{key_p, MID_p \mid 1 \le p \le i+n\}$, where key_p is calculated as $ENC_{A_i}[f(\underbrace{f(a_p \| d)}_{S_{key}^p} \| PID_i)]$, ENC_{Ai} is the symmetric key encryption (i.e., ASE-128 [89]) using a key A_i and p is the number of medical servers present in the e-medical system to provide medical services.

Step3: *AS* finally burns $\{PID_i, C_i, D_i, \{key_p, MID_p \mid 1 \le p \le i+n\}, f(\cdot), y\}$ into the memory of biometric smart card and issues the card for patient P_i.

Login Phase

To reach several medical facilities by accessing the medical servers (*MS*), the patient P_i punches the biometric smart card into his/her mobile device and also the sensor of the mobile device scans the biometric of P_i and extracts the feature $b_i^{'}$ of P_i. Then the patient P_i supplies his/her password pw_i to the mobile device. After that the mobile device of P_i executes the following operations:

Step1: Mobile device calculates $bpw_i^{'} = f(pw_i \| b_i^{'})$, $A_i^{'} = C_i \oplus bpw_i^{'}$ and $D_i^{'} = f(A_i^{'} \| PID_i \| bpw_i^{'})$ Then, it checks $D_i = ? D_i^{'}$. For the correct value, the device executes the next step; otherwise, it stops the current session.

Step2: Mobile device provides the permission to select an identity of medical server from which P_i wants to get service. P_i submits an identity MID_i of MS_i.

Step3: The mobile device retrieves key_i corresponding to MID_i. It then extracts $f(f(a_i \| d) \| PID_i)$ by decrypting key_i using the key $A_i^{'}$ as $f(f(a_i \| d) \| PID_i) = DEC_{A_i}[key_i]$.

Step4: The device picks a number r_i randomly from Z_y^* and calculates $L_i = ENC_{f(f(a_i \| d) \| PID_i)}[r_i \| f(b_i \| r_i \| T_1)]$ and $R_i = f(r_i \| T_1 \| MID_i \| PID_i \| f(b_i \| r_i \| T_1))$, where T_1 is the current timestamp. Then the mobile device transmits a login message $\{PID_i, L_i, R_i, MID_i, T_1\}$ to the medical server MS_i via the Internet.

Authentication and Session Key Agreement Phase

Upon getting the login message $\{PID_i, L_i, R_i, MID_i, T_1\}$ at timestamp T_2, the medical server MS_i checks the validity of timestamp as $(T_2 - T_1) \le \Delta T$, where ΔT is the threshold value of time span. For the correct result, MS_i executes the following steps:

Step1: MS_i calculates $f(S_{key}^i \| PID_i)$, retrieves $[r_i^* \| (f(b_i \| r_i \| T_1))^*]$ by decrypting L_i as $DEC_{f(S_{key}^i \| PID_i)}[L_i]$ and calculates $R_i^* = f(r_i^* \| T_1 \| MID_i \| PID_i \| (f(b_i \| r_i \| T_1))^*)$. Then MS_i checks $R_i = ? R_i^*$. For the false result, and MS_i rejects the current session; otherwise, it executes the next step.

Step2: MS_i picks a number e_i randomly from Z_y^*, and calculates $re_i = r_i^* \oplus e_i$, $SK_i = f(r_i^* \| e_i \| T_1 \| T_2 \| (f(b_i \| r_i \| T_1))^*)$ and $K_i = f(SK_i \| e_i)$. Then, MS_i transmits a reply message $\{re_i, K_i, T_2\}$ to the mobile device of P_i.

Step3: After getting $\{re_i, K_i, T_2\}$ at timestamp T_3, the mobile device verifies the validity of sent timestamp. For the correct result, it computes $e_i^{'} = r_i \oplus re_i$, $SK_i^{'} = f(r_i \| e_i^{'} \| T_1 \| T_2 \| f(b_i \| r_i \| T_1))$ and $K_i^{'} = f(SK_i^{'} \| e_i^{'})$. Then the device checks $K_i = ? K_i^{'}$.For the correct equality, both the patient P_i and medical server MS_i agree upon a session key SK_i for secure data communication into the same session.

6. Conclusion and Future Scope

Biometric technology has been around for decades but it is mainly popular for identity authentication or verification in highly secure environment. Biometric-based security systems are becoming popular day by day. Fig.12 discussed the changes of revenue of total biometric revenue market with respect to year. The change is monotonically and exponentially increasing in nature. Therefore, it can be said that day by day, biometric-based security is becoming more and more popular. Still there are some challenges being faced by biometric technology. The first challenge is the cost of biometric technology. There are some reasons for increasing cost of biometric technology like: hardware maintenance, processing power for databases, experimental infrastructure, real-time implementation, salary for employees, training for the employees, marketing cost, exception handling, productivity loss, and system maintenance, among others.

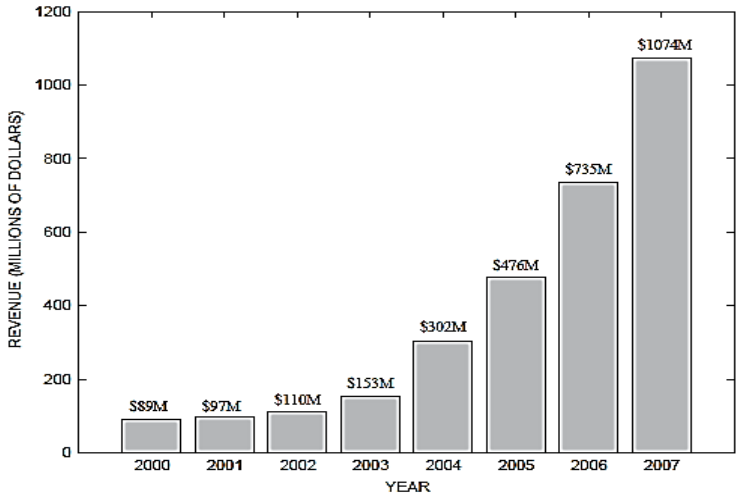


Fig. 12: Total biometrics revenue market: 2000-2007 [68]

Fig. 13shows the possible threat of biometric security system. At the sensor level where end user puts his/her biometric information, there are different attacks that can occur like collective attack, spoofing attacks, and mimicry attacks. However, at the time of biometric features extraction, different attacks might take place like, eavesdropping, man-in-the middle attack, replay attack, and brute force attack. The storage data can be attacked by reading template, replacing template attack, and change-binding attack (ID-biometric).Those attacks influence the error of matching during the matching process of biometric information inserted by the end user with the stored but tempered biometric information. If we can

consider that stored biometric information is correct then also attacks can occur at the time of matching phase. The type of attack occurred at matching phase is insertion of imposter data, component replacement, hill climbing, and manipulation of score guessing attack. Eavesdropping attack, reply attack and man-in-the-middle attack can occur during the transmission of biometric data from Data Storage to the Matching block. After matching process is done, the message regarding percentage of matching information is to transfer to the Decision block. During transfer process, the message might be tempered with by hill climbing, and manipulation of match score process. Even hackers can change the data at the decision level. Moreover, attacks can occur after transmitting the decision and such attacks are component replacement, hill climbing, and manipulation of decision, among others.

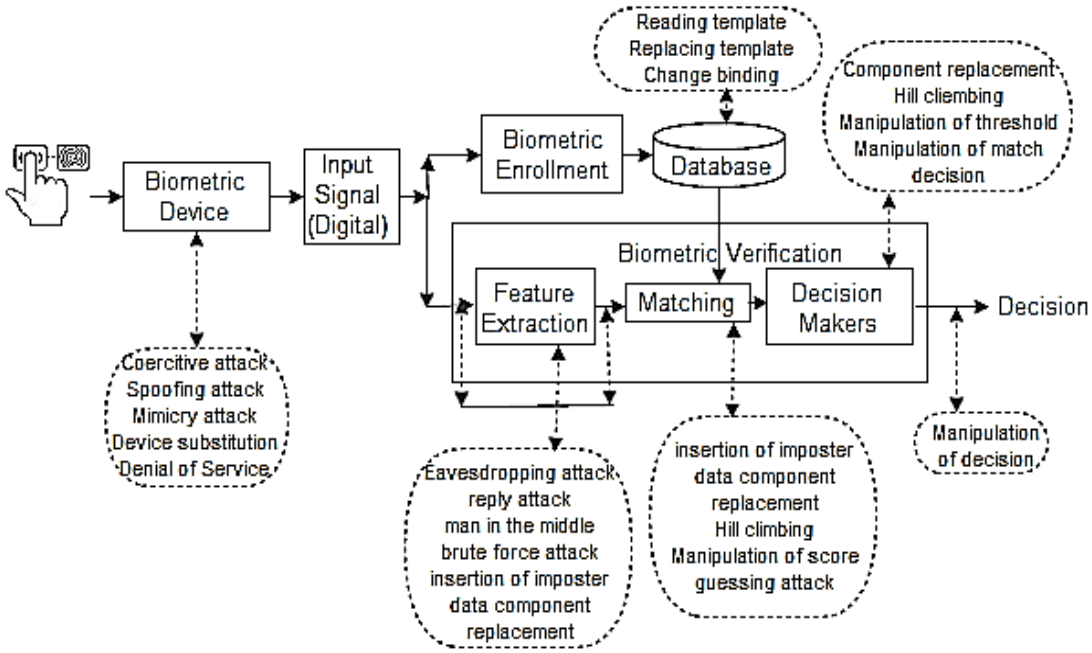


Fig. 13: List of security threat in different steps of biometric security system

References

[1] M. S. Obaidat, and P. Nicopolitidis, "Smart Cites and Homes: Key Enabling Technologies," Elsevier, 2016

[2] M. S. Obaidat and S. Misra, "Principles of Wireless Sensor Networks," Cambridge University Press, 2014.

[3] M. S. Obaidat and N. Boudriga, "Security of e-Systems and Computer Networks, Cambridge University Press, 2007.

[4] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in *Proceedings. IEEE Symposium on Security and Privacy (Cat. No.98CB36186)*. pp. 148–157, 1998.

[5] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys*

& Tutorials, vol. 17, no. 4. pp. 2347–2376, 2015.

[6] M. Hansen, P. Berlich, J. Camenisch, S. Clauß, A. Pfitzmann, and M. Waidner, "Privacy-enhancing identity management," *Inf. Secur. Tech. Rep.*, vol. 9, no. 1, pp. 35–44, 2004.

[7] M. Jude, "IBM: Working Towards a Smarter Connected Home. Internet: http://docs.caba.org/documents/IBM-Smart-Cloud-Home-SPIE2012.pdf," 2014.

[8] L. Jiang, D.-Y. Liu, and B. Yang, "Smart home research," *Proceedings of 2004 International Conference on Machine Learning and Cybernetics (IEEE Cat. No.04EX826)*, vol. 2. pp. 659–663 vol.2, 2004.

[9] N. Bui and M. Zorzi, "Health Care Applications: A Solution Based on the Internet of Things," in *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*, 2011, p. 131:1--131:5.

[10] A.-M. Rahmani, N. K. Thanigaivelan, T. N. Gia, J. Granados, B. Negash, P. Liljeberg, and H. Tenhunen, "Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems," in *Consumer Communications and Networking Conference (CCNC), 2015 12th Annual IEEE*, 2015, pp. 826–834.

[11] A. M. Vilamovska, E. Hattziandreu, R. Schindler, C. Van Oranje, H. De Vries, and J. Krapelse, "Rfid application in healthcare–scoping and identifying areas for rfid deployment in healthcare delivery," *RAND Eur. Febr.*, 2009.

[12] L. Lei-hong, H. Yue-shan, and W. Xiao-ming, "A Community Health Service Architecture Based on the Internet of Things on Health-Care," in *World Congress on Medical Physics and Biomedical Engineering May 26-31, 2012, Beijing, China*, 2013, pp. 1317–1320.

[13] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," in *Information technology: new generations (ITNG), 2010 seventh international conference on*, 2010, pp. 804–809.

[14] G. Acampora, D. J. Cook, P. Rashidi, and A. V Vasilakos, "A survey on ambient intelligence in healthcare," *Proc. IEEE*, vol. 101, no. 12, pp. 2470–2494, 2013.

[15] M. S. Shahamabadi, B. B. M. Ali, P. Varahram, and A. J. Jara, "A network mobility solution based on 6LoWPAN hospital wireless sensor network (NEMO-HWSN)," in *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on*, 2013, pp. 433–438.

[16] S. M. R. Islam, D. Kwak, M. D. H. Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: a comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[17] R. S. H. Istepanian, S. Hu, N. Y. Philip, and A. Sungoor, "The potential of Internet of m-health Things 'm-IoT' for non-invasive glucose level sensing," in *Engineering in Medicine and Biology Society, EMBC, 2011 Annual International Conference of the IEEE*, 2011, pp. 5264–5266.

[18] Z. L. In, "Patient body temperature monitoring system and device based on Internet of Things," *Chinese Pat.*, vol. 103, pp. 577–688, 2014.

[19] H. A. Khattak, M. Ruta, and E. Di Sciascio, "CoAP-based healthcare sensor networks: A survey," in *Applied Sciences and Technology (IBCAST), 2014 11th International Bhurban Conference on*, 2014, pp. 499–503.

[20] E. C. Larson, M. Goel, G. Boriello, S. Heltshe, M. Rosenfeld, and S. N. Patel, "SpiroSmart: using a microphone to measure lung function on a mobile phone," in *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, 2012, pp. 280–289.

[21] P. K. Dash, "Electrocardiogram monitoring," *Indian J. Anaesth*, vol. 46, no. 4, pp. 251–260, 2002.

[22] L. Yang, Y. Ge, W. Li, W. Rao, and W. Shen, "A home mobile healthcare system for wheelchair users," in *Computer Supported Cooperative Work in Design (CSCWD), Proceedings of the 2014 IEEE 18th International Conference on*, 2014, pp. 609–614.

[23] Dr. Hawking's Connected Wheelchair Project, http://smartcitiescouncil.com/resources/stephen-hawking-and-intel-connected-wheelchair-project.

[24] Awareness Day 2014 Activities by Program Type, National Children's Mental Health Awareness Day, May 2014. https://www.samhsa.gov/sites/default/files/children-awareness-day-activities-by-program-2014.pdf

[25] M. Vazquez-Briseno, C. Navarro-Cota, J. I. Nieto-Hipolito, E. Jimenez-Garcia, and J. D. Sanchez-Lopez, "A proposal for using the internet of things concept to increase children's health awareness," in *Electrical Communications and Computers (CONIELECOMP), 2012 22nd International Conference on*, 2012, pp. 168–172.

[26] G. Zhang, C. Li, Y. Zhang, C. Xing, and J. Yang, "SemanMedical: a kind of semantic medical monitoring system model based on the IoT sensors," in *e-Health Networking, Applications and Services (Healthcom), 2012 IEEE 14th International Conference on*, 2012, pp. 238–243.

[27] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[28] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, 2014.

[29] T. Nam and T. A. Pardo, "Conceptualizing smart city with dimensions of technology, people, and institutions," in *Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times*, 2011, pp. 282–291.

[30] T. Bakıcı, E. Almirall, and J. Wareham, "A smart city initiative: the case of Barcelona," *J. Knowl. Econ.*, vol. 4, no. 2, pp. 135–148, 2013.

[31] H. Wang and W. He, "A reservation-based smart parking system," in *Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on*, 2011, pp. 690–695.

[32] D. Bonino, M. T. D. Alizo, A. Alapetite, T. Gilbert, M. Axling, H. Udsen, J. A. C. Soto, and M. Spirito, "Almanac: Internet of things for smart cities," in *Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on*, 2015, pp. 309–316.

[33] M. Yun and B. Yuxin, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," in *Advances in Energy Engineering (ICAEE), 2010 International Conference on*, 2010, pp. 69–72.

[34] E. Qin, Y. Long, C. Zhang, and L. Huang, "Cloud computing and the internet of things: Technology innovation in automobile service," in *International Conference on Human Interface and the Management of Information*, 2013, pp. 173–180.

[35] Y. Zhang, B. Chen, and X. Lu, “Intelligent monitoring system on refrigerator trucks based on the internet of things,” in *International Conference on Wireless Communications and Applications*, 2011, pp. 201–206.

[36] L. Atzori, A. Iera, and G. Morabito, “SIoT: Giving a Social Structure to the Internet of Things,” *IEEE Communications Letters*, vol. 15, no. 11. pp. 1193–1195, 2011.

[37] L. Atzori, A. Iera, G. Morabito, and M. Nitti, “The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization,” *Comput. networks*, vol. 56, no. 16, pp. 3594–3608, 2012.

[38] J. Kleinberg, “The convergence of social and technological networks,” *Commun. ACM*, vol. 51, no. 11, pp. 66–72, 2008.

[39] P. Semmelhack, *Social machines: how to develop connected products that change customers’ lives*. John Wiley & Sons, 2013.

[40] Y. Bo and H. Wang, “The Application of Cloud Computing and the Internet of Things in Agriculture and Forestry,” *Service Sciences (IJCSS), 2011 International Joint Conference on*. pp. 168–172, 2011.

[41] J. Zhao, J. Zhang, Y. Feng, and J. Guo, “The study and application of the IOT technology in agriculture,” *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*, vol. 2. pp. 462–465, 2010.

[42] A. Giri, S. Dutta, and S. Neogy, “Enabling agricultural automation to optimize utilization of water, fertilizer and insecticides by implementing Internet of Things (IoT),” *2016 International Conference on Information Technology (InCITe) - The Next Generation IT Summit on the Theme - Internet of Things: Connect your Worlds*. pp. 125–131, 2016.

[43] T. Kelesidis, I. Kelesidis, P. I. Rafailidis, and M. E. Falagas, “Counterfeit or substandard antimicrobial drugs: a review of the scientific evidence,” *J. Antimicrob. Chemother.*, vol. 60, no. 2, pp. 214–236, 2007.

[44] A. J. Jara, A. F. Alcolea, M. A. Zamora, A. F. G. Skarmeta, and M. Alsaedy, “Drugs interaction checker based on IoT,” in *Internet of Things (IOT), 2010*, 2010, pp. 1–8.

[45] L. Toms, “5 Common Cyber Attacks in the IoT-Threat Alert on a Grand Scale”, *Global Sign, GMO Internet Group*.

[46] N. K. Ratha, J. H. Connell and R. M. Bolle, “Enhancing Security and Privacy in Biometrics-Based Authentication Systems,” *IBM Systems Journal*, vol. 40, no. 3, pp. 614-634, 2001.

[47] M. Abomhara, “Cyber Security and The Internet of Things: Vulnerabilities, Threats, Intruders and Attacks”, Journal of Cyber Security and Mobility, vol. 4, no. 1, pp. 65-88, 2015.

[48] Hewlett Packard, “HP study reveals 70 percent of Internet of Things devices vulnerable to attack”, July 2014.

[49] T. Heer, O. Garcia-Morchon, R. Hummen, S.L. Keoh, S. S. Kumar, K. Wehrle, "Security Challenges in the IP-based Internet of Things", *Wireless Personal Communications, vol.* 61, no. 3, pp. 527-542, 2011.

[50] S. Cirani, G. Ferrari, and L. Veltri. "Enforcing Security Mechanisms in the IP-Based Internet Of Things: An Algorithmic Overview," *Algorithms, vol.* 6, no. 2, pp. 197-226, 2013.

[51] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, "Vision and Challenges for Realizing the Internet of Things", *Cluster of European Research Projects on the Internet of Things, European Commission*, vol. 3, no. 3, pp. 34-36, 2010.

[52] A. K. Jain, and S. Z. Li, "Handbook of Face Recognition", *Springer, New York*, 2011.

[53] C. Ding, C. Xu, and D. Tao, "Multi-Task Pose-Invariant Face Recognition", *IEEE Transactions on Image Processing, vol.* 24, vol. 3, pp. 980-993, 2015.

[54] L. B. Rowden, and A. K. Jain, "Longitudinal Study of Automatic Face Recognition", *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 2017.

[55] R. Teixeira,and N. Leite, "A New Framework for Quality Assessment of High-Resolution Fingerprint Images", *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 2016.

[56] J. Daugman, "How Iris Recognition Works", *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21-30, 2004.

[57] L. Zhang, Y. Shen, H. Li, and J. Lu, "3D Palm print Identification using Block-Wise Features and Collaborative Representation", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 37, no. 8, pp. 1730-1736, 2015.

[58] L. Zhang, L. Li, A. Yang, Y. Shen, and M. Yang, "Towards Contactless Palm print Recognition: A Novel Device, A New Benchmark, and A Collaborative Representation Based Identification Approach", *Pattern Recognition*, vol. 69, pp. 199-212, 2017.

[59] A. Tkach, M. Pauly, and A. Tagliasacchi, "Sphere-Meshes for Real-Time Hand Modeling and Tracking", *ACM Transactions on Graphics (TOG)*, vol. 35, no. 6. pp. 222-2016.

[60] S. Sharma, S. R. Dubey, S. K. Singh, R. Saxena, and R. K. Singh, "Identity Verification using Shape and Geometry of Human Hands", *Expert Systems with Applications*, vol. 42, no. 2, pp. 821-832, 2015.

[61] J. G. Rodriguez, P. Rose, D. Ramos, D. T. Toledano, and J. O. Garcia, "Emulating DNA: Rigorous Quantification of Evidential Weight in Transparent and Testable Forensic Speaker Recognition", *IEEE Transactions on Audio, Speech, and Language Processing*, vol. 15, no. 7, pp. 2104-2115, 2007.

[62] A. Kumar, and K. V. Prathyusha, "Personal Authentication using Hand Vein Triangulation and Knuckle Shape", *IEEE Transactions on Image Processing*, vol. 18, no.9, pp. 2127-2136, 2009.

[63] M. S. Obaidat and B. Sadoun, "Verification of Computer Users Using Keystroke Dynamics," IEEE Trans. on Systems, Man, and Cybernetics, Part B, Vol. 27, No. 2, pp. 261-269, 1997.

[64] A. M. D. L. Herran, B. G. Zapirain, and A. M. Zorrilla, "Gait Analysis Methods: An Overview of Wearable and Non-Wearable Systems, Highlighting Clinical Applications", *Sensors*, vol. 14, pp. 3362-3394, 2014.

[65] A. Fischer, and R. Plamondon, "Signature Verification Based on the Kinematic Theory of Rapid Human Movements", *IEEE Transactions on Human-Machine Systems*, vol. 47, no. 2, pp. 169-180, 2017.

[66] D. P. Jarrett,E. A. P.Habets, and P. A. Naylor, "Theory and Applications of Spherical Microphone Array Processing", *Springer*, pp. 1-10, 2017.

[67] K. Ali, A. X. Liu, W. Wang, and M. Shahzad, "Recognizing Keystrokes Using Wi-Fi Devices", *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 5, pp. 1175-1190, 2017.

[68] R. de Luis-García, C. Alberola-López, O. Aghzout, and J. Ruiz-Alzola, "Biometric identification systems," *Signal Processing*, vol. 83, no. 12, pp. 2539–2557, 2003.

[69] M. Faundez-Zanuy, "Biometric security technology," in *Encyclopedia of Artificial Intelligence*, IGI Global, 2009, pp. 262–269.

[70] Y. Zhen, X. Li, Q. Ou, and L. Zeng, "Internet of things and smart grid," *Digit. Commun.*, vol. 39, no. 5, 2012.

[71] A. Kulkarni and S. Sathe, "Healthcare applications of the Internet of Things: A Review," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 5, pp. 6229–6232, 2014.

[72] A. Riahi, E. Natalizio, Y. Challal, N. Mitton, and A. Iera, "A systemic and cognitive approach for IoT security," in *Computing, Networking and Communications (ICNC), 2014 International Conference on*, 2014, pp. 183–188.

[73] A. K. Jain, A. Ross, and S.Prabhakar, "An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology*,vol. 14, no. 1, pp. 4-20, 2004.

[74] W. Hwang, H. Wang, H. Kim, S. C.Kee, and J. Kim, "Face Recognition System Using Multiple Face Model of Hybrid Fourier Feature under Uncontrolled Illumination Variation", *IEEE Transactions on Image Processing*, vol. 20, no. 4, pp. 1152-1165, 2011.

[75] S. D. Choudhury, and T.Tjahjadi, "Silhouette-Based Gait Recognition using Procrustes Shape Analysis and Elliptic Fourier Descriptors", *Pattern Recognition*, vol. 45, no. 9, pp. 3414-3426, 2012.

[76] D. C.He, and L. Wang, "Texture Unit, Texture Spectrum, and Texture Analysis", *IEEE Transactions on Geoscience and Remote Sensing*, vol. 28, pp. 509 – 512, 1990.

[77] U. Park, R. R. Jillela, A. Ross, and A. K. Jain, "Periocular Biometrics in the Visible Spectrum", *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 96-106, 2011.

[78] Z. Guo, L. Zhang, D. Zhang, and X.Mou, "Hierarchical Multi scale LBP for Face and Palmprint Recognition", *In Proceedings of 17th IEEE International Conference on Image Processing (ICIP)*, pp. 4521-4524, September 2010.

[79] C. Gottschlich, "Curved-Region-Based Ridge Frequency Estimation and Curved Gabor Filters for Fingerprint Image Enhancement", *IEEE Transactions on Image Processing*, vol. 21, no. 4, pp. 2220-2227, 2012.

[80] S. Xie, S. Shan, X. Chen, and J. Chen, "Fusing Local Patterns of Gabor Magnitude and Phase for Face Recognition", *IEEE Transactions on Image Processing*, vol. 19, no. 5, pp. 1349-1361, 2010.

[81] V. F, Zernike, "Diffraction Theory of the Cutting Process and its Improved Form, the Phase Contrast Method", *Physica*, vol. 1, no. 7-12,pp. 689-704, 1934.

[82] C. W. Tan, and A. Kumar, "Unified Framework for Automated Iris Segmentation using Distantly Acquired Face Images", *IEEE Transactions on Image Processing*, vol. 21, no.9, pp. 4068-4079, 2012.

[83] C. W. Tan, and A. Kumar, "Accurate Iris Recognition at a Distance using Stabilized Iris Encoding and Zernike Moments Phase Features", *IEEE Transactions on Image Processing*, vol. 23, no.9, pp. 3962-3974, 2014.

[84] D. G. Lowe, "Object Recognition from Local Scale-Invariant Features", *In Proceedings of the IEEE International Conference on Computer Vision*, vol. 2, pp. 1150–1157, Washington, DC, USA,1999.

[85] X. Wu, Y. Tang, and W. Bu, "Offline Text-Independent Writer Identification Based on Scale Invariant Feature Transform", *IEEE Transactions on Information Forensics and Security*, vol. 9, no.3, pp. 526-536, 2014.

[86] D. Smeets, J. Keustermans, D. Vandermeulen, and P. Suetens, "meshSIFT: Local Surface Features for 3D Face Recognition under Expression Variations and Partial Data", *Computer Vision and Image Understanding*, vol. 117, no.2, pp. 158-169, 2013.

[87] T. Maitra, and D. Giri, "An Efficient Biometric and Password-Based Remote User Authentication using Smart Card for Telecare Medical Information Systems in Multi-Server Environment", *Journal of Medical Systems*, vol. 38, no. 12, Article Id. 142, 2014.

[88] T. Maitra, M. S. Obaidat, R. Amin, SK H. Islam, S. A. Chaudhry, and D. Giri, "A Robust Elgamal-Based Password-Authentication Protocol using Smart Card for Client-Server Communication," *International Journal of Communication System*, vol. 30, no. 11, 2017.

[89] Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, 2001.https://www.nist.gov/publications/advanced-encryption-standard-aes, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf