Journal of Computers Vol. 29 No. 1, 2018, pp. 189-208
doi:10.3966/199115992018012901017

# Security, Comfort, Healthcare, and Energy Saving: A Review on Biometric Factors for Smart Home Environment

Taqiyah-Khadijah Ghazali, Nur-Haryani Zakaria*

School of Computing, Awang Had Salleh College of Arts and Sciences, Universiti Utara Malaysia, Sintok, Kedah, Malaysia
taqiyah_khadijah@ahsgs.uum.edu.my, haryani@uum.edu.my

Received 15 October 2016; Revised 6 March 2017; Accepted 30 March 2017

Abstract. The Internet of Things (IoT) have become significantly important in authentication mechanisms in which traditional authentication have shift to the biometric factors whereby biometric is said to offer more security and convenience to the users. The purpose of this paper is to provide an extensive review on biometric factors for smart home environments that are intended for security, comfort, healthcare, and energy saving. This paper also discusses the security authentication mechanisms, which are knowledge factor (password, PIN), ownership factor (ID card, passport), and inherent factor (fingerprint, iris, facial), known as biometric factors. Biometric factors can be used as authentications for smart home environments, which are more robust and reliable in terms of accuracy, convenience, and speed.

Keywords: authentication, biometrics, IoT, smart home environment

## 1 Introduction

The advancement of technology has transformed our lives tremendously from various perspectives, ranging from sports, health, education, and lifestyle. Mobile devices are incorporated with computational capabilities that enables us to control and monitor many things at our fingertips. One such application that has gained attention lately is the smart homes [1-4]. Smart homes enable users to control and monitor our home features from lighting, heating, ventilation, and air conditioning (HVAC) to entertainment, shades, doors, alarms system, security, and various other home appliances [5-6]. One of the main characteristics that make a house becomes a smart home is the automation. With automation, the features in the home are integrated and interconnected so that they can communicate automatically with each other by means of home controller through the Internet [7-8]. Another criterion of the smart home is intelligence, whereby it can learn from the daily activities, and then control and manage the activities by itself without the involvement of the users [9-12]. It also comprises a large number of network sensors and actuators with different functionalities that provide users with easy and comfortable access [13-15].

As a matter of fact, migration from the traditional home to a smart home is worthy because the smart home itself has the possibility to give a better quality of life for human beings, such as convenience, comfort, security, and energy conservation [16-19]. Apart from that, smart homes can also provide a safe and secure environment for older and disabled people by giving them an opportunity to control many complicated functions based on their capabilities, which previously can only be done with others' help [10, 20-24]. Therefore, it is very crucial for smart home users to strengthen the access control mechanisms, so that the security and privacy aspects are well protected [25-26].

The access control in a smart home basically enables authorized home owners to access the house and to prevent the unauthorized people from gaining access into the house [25]. Access controls in a smart home are not only limited to the entrance door, but also applied to other features in the house, which

* Corresponding Author

include home appliances, services, and applications [26-28]. Hence, it needs authentication and authorization [29]. Authentication will identify and verify the owner through several security mechanisms such as passwords or smart cards, and if the person is the owner of the house, the system will authorize the owner to gain access. Meanwhile, authorization determines what appliances or applications that the owners have rights to access. For example, dangerous appliances like the stove could be authorized for parents only and not for young children [30].

In general, authentication factors can be classified into three factors: (1) Knowledge factor (e.g.: passwords or PINs); (2) Ownership factor (e.g.: a token or smart cards); and (3) Biometric factor that relies on two factors (e.g.: psychological factor: finger print or iris, and behavioral factors: signature, voice, handwriting). These factors can either be used alone or in combination with one another [31]. Every authentication mechanism has its advantages and drawbacks. There is no perfect authentication, but rather its efficiency and convenience for the home owners to use.

The significant in using biometric for smart home is that biometric sensors can be used to collect data that can be applied by other interconnecting systems [20]. In terms of security and customizable of smart home environment, biometric recognitions are able to identify physiological and behavioral characteristic of human activities thus making the systems automate and intelligent. For example home lighting automation, windows opening, and closing automation. Besides, the automation of smart home can prevent electrical appliances from malfunctioning and provide human safety from disaster like gas leakage or fire. Apart from that, the advantage of using biometric in smart home is that the appliances 'knows' who is using it. This allows automatic adaptation to the needs of people and also tracking of their actions in the case of misuse. By employing biometrics in smart home system, a profile for each resident will be characterized by his or her unique biometric characteristic. This profile consists of authorisation and permissions specific to the profile owner [32].

Based on the highlights discussed above, this paper intends to provide a review on biometric factors used in smart homes. To present the review, recent and past related work have been gathered and summarized, (as far as the author's knowledge) analyzed, and discussed accordingly. By providing the information related to the biometric factors used in smart home, this review aims to motivate further research in exploring new field or enhancing potential studies in the field of biometrics' contributions in smart home. The paper is organized as follows: Section 2 will provide conceptual model of smart homes, related work and key research problems. Section 3 will further elaborate the biometric factors applied for the smart home, followed by Section 4, which will present the existing security authentications. The last section concludes with some discussion and conclusion.

## 2 Conceptual Model of Smart Homes

The smart home system consists of several components that can be divided into three layers: the front end, the middle end and the back end. The users sit at the front end, whereby they use mobile devices such as mobile phones, tablets or television remote controls to control the functions available. Those mobile devices are usually equipped with the smart home application. Through these applications, users communicate via interfaces that provide commands to various functions.

The middle layer is considered the heart of the system, whereby the smart home gateway and the modem are connected to the Internet. This connectivity enables the smart home devices to be controlled anywhere by the authorized users via the mobile devices relying upon standard protocols such as IEEE 802.11x [33].

The back end layer is where all the smart home devices reside. The devices range from home lightings, heating ventilation and air conditioning (HVAC), shades and blinds, refrigerator, stove, and many other home appliances. These devices are controlled by the users via the smart home application, relying on senses and standard protocols such as the IEEE 802.15.4. These senses rely on biometric factors (e.g.: facial, voice, body temperature) to enable the control of the automation process. For example, for the air-conditioning system, smart home users are able to adjust the temperature based on human body heat or via voice command. This scenario provides security, comfort, and energy conservation to the users, and also becomes an assistive mechanism for the elderly and disabled people [34-35]. The following Fig. 1 illustrates a conceptual design of the smart home system [36].

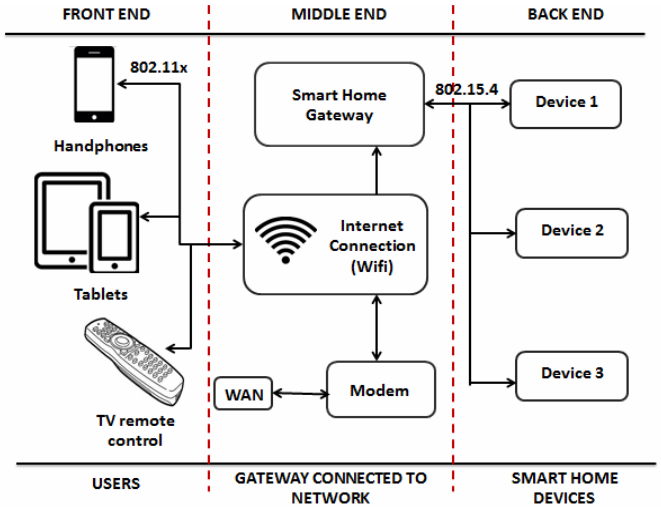


**Fig. 1.** Conceptual design of smart home system

### 2.1 Issues Associated with Smart Home

Several review studies have been done on smart home apparently [24, 34, 35, 37-40] to name a few. Among the issue stated by the previous researchers is from [3] which conducted a risk analysis on a smart home automation. They concluded that "the highest ranked risk related to the information processed is derived from inadequate access control configuration in the in-house gateway, within network communication whereby the main risks come from inadequate authentication and confidentiality settings" (p. 190). Study by [14] also acknowledged, achieving security have been identified as one of the top barriers in smart home environment.

Therefore, to ensure security in the smart home environment, authentication, access control and user privacy need to be established to prevent such attacks [3]. Besides that, they also added that the software risk authentication mechanism is susceptible to attack; providing attackers to bypass such as password authentication schemes and thus obtain access to the system without proper authorizations. To lessen this risk, the use of standardized mechanisms for managing authentication and session control should be employed over such components applied within smart home environment. With constant searches for the illusive ideal security identifier, biometric smart home systems have become more widespread and have gained the public interest [20]. Apart from security issue, others challenges in smart home system are related to hardware, software, design and domestication [38]. Public reviews have been gathered in a workshop organized by [41] also highlighted that, loss of control, reliability, privacy, security, trust, cost, and irrelevance are among the social barriers in adopting smart home. Therefore, to open the minds of readers and the public, the advantages of applying biometric sensors in smart home environment may help to improve the issues and challenges stated above where lots of benefits can be gained from adopting smart home.

## 3 Biometric Factors Applied in the Smart Home Environment

Various biometric factors have been applied for smart homes. According to [35], security problems can occur to smart homes if no protection has been made. Smart homes can also become vulnerable to weak authentications, whereby smart devices can be intercepted by intruders or hackers and controlled remotely from other places to capture the information, accidently or purposely in order to steal or modify them. Therefore, it is very important to protect and keep the house safe from the undesired incident. Nevertheless, a home is where a family lives together to achieve comfort, convenience, and security.

In order to achieve that, sophisticated security can be applied for the smart home for the purpose of authentication and access control those of appliances. Thus, biometric factors can be implemented for smart home to protect, monitor and control the house [42]. For example, studies by [43-46] used footsteps and gait recognition for surveillance in order to track intruders or any persons in the house. Besides, based on the footsteps and gait recognition, it can identify the users whether they are the owner of the house or not. In addition, fingerprint, iris, palm vein, face, ear, and height can be applied to

authenticate various devices and appliances in the house as well as access control. For biometric factors, a study by [47] found that facial recognition can be applied at the entrance door to capture the face of unrecognized individuals and monitor the surrounding of the smart home environment to identify users and intruders.

Not only can the biometric factors be applied for security base, but they can also be used to collect data of certain applications and process them to become information for the benefits of the family. That is to say, smart homes can implement health monitoring for the elders and disabled people, and even for anybody in the house who wants to maintain a healthy lifestyle [34-35]. For example, electrocardiogram (ECG) can measure vital signs and heart rates in the body as well as blood pressure, blood sugar, blood flow, temperature, and weight. These can be done by embedding smart sensors on the body (Body Area Network) and integrating it with the home network to capture the data. Apart from that, footsteps and gait recognition can also recognize human behaviors for medical purposes.

Furthermore, biometric factors can carry out command features. For example, speech recognition has the ability to perform voice command control to the smart home appliances and devices, whereby users can give commands to remote control to open certain television channels or radio music, open curtains or blinds at the windows, lock the door, switch on and off lights and air conditioners, as well as kitchen appliances like coffee maker, microwave, and many more. In addition, speech recognition is also suitable to the impaired vision and disabled people to ease their tasks, whereby they only need to give commands without burdening themselves to move around frequently.

However, despite numerous benefits and advantages, biometric authentications may also have issues and drawbacks as well. The significant factor for this issue is that natural behavior may affect the effectiveness of the biometric. For example, in footsteps recognition, there may occur confusions when walking, differences in lighting conditions and backgrounds to capture the gait movements, or unobtrusive movements when a person walking quietly or unnoticeably. The following Table 1 summarizes several main perspectives of biometric factors applied in smart homes.

**Table 1.** Biometric factors applied in smart homes

| Biometric Factors | Technology Used | Advantages | Drawbacks | Specific Applications for Smart Homes | Ref. |
|---|---|---|---|---|---|
| Footsteps and gait | Enhanced Gait Energy Image (EGEI) and Multilinear Principal Component Analysis (MPCA), fusion of spatio-temporal, semi-automatic system, support vector machine (SVM) and equal error rate (EER), K- Means, K-NN | Recognition at a distance or at low resolution, can be collected covertly | Confusion, differences in lighting conditions and background movements, unobtrusive movements | Surveillance, tracking person, recognizing human behavior, identification | [43], [44], [45], [46] |
| Fingerprint and iris | ARM7TDMI-S Microcontroller, Hamming distance | Accuracy, reliable, speed | Injured, wear contact lens, glasses | Authentication, access control | [7], [48] |
| Speech/ Voice | Multiple Sensor-Based Perception System Integrated with Mobile and Voice Technology, Single Board Computer (SBC), Cloud-based API, Wolfram Alpha, Natural Language, Dynamic Time Wrapping (DTW) | Reduce time consumption, convenience, mobile | Background noise, slow in recognizing | Controlling smart home features and appliances (voice command control), impaired vision | [49], [50], [51], [52], [53], [54], [55] |

**Table 1.** Biometric factors applied in smart homes (contine)

| Biometric Factors | Technology Used | Advantages | Drawbacks | Specific Applications for Smart Homes | Ref. |
|---|---|---|---|---|---|
| Face | Detecting human emotions, Principle Component Analysis (PCA), feature extraction techniques and Support Vector Machines (SVM), face detection by stepwise pruning, coarse-to-fine facial feature extraction for face normalization, face identification by cascaded discriminant analysis. | Reducing stress-related health problems | Angel image, complexity | Automate smart home appliances, surveillance (face detection at entrance home) | [56], [57], [47] |
| Height | Mounting ultrasonic distance sensors | Effective among small Populations, cheap, convenient and minimally invasive | Ageing factor might change, adult women usually are the same height (if more than one woman in the house) | Authentication / Access control | [58] |
| Ear | Using smartphone camera to capture the ear image with location-based service (LBS) support, local invariant patterns | Low cost since it uses a smartphone camera | Difficult to see the ear, and inconvenience for women wearing scarves. | Authentication / Access control | [59] |
| Palm vein | Wireless Sensor Networks (WSNs) | Ease of feature extraction, spoofing resistant, high accuracy | Only can applied at the front door | Authentication / Access control | [32] |
| ECG (electro-encephalogram) | Hamming distance, DES algorithm, threshold | Stability and distinctiveness | ECG is not strong as other biometric factors in terms of identification | Health monitoring | [60], [61] |
| EEG (electro-cardiogram) | Autoregressive(AR) Model, Back-propagation Neural Network | Confidential, difficult to mimic and almost impossible to steal | Difficult in setting up the subject for the signal acquisition, obstacle in acquisition protocol, EEG cannot be acquired at a distance, brain waves are weak signals and sensitive to the contamination from many artefact signals. | Authentication | [62] |
| Blood pressure, blood glucose, blood flow, temperature | BioSensor, Wireless Network | Prevents the need for expensive computations | Low power, limited memory, low computational memory | Health monitoring | [20], [63], [64] |

Based on Table 1 above, many researches have been done on speech and voice biometric for smart home. Voice biometric can rely on voice command control to control smart home features and appliances. Impaired or blind users can have the advantage of using voice command control. By using voice or speech, it can limit the users' movement which is why becomes one of the favorite biometric factors that

can be adopted in smart home. However, using voice biometric has one major disadvantage which the speed recognition is slow especially when there are background noises. Besides, sore throat may change the voice into hoarse or husky that will affect the systems to recognize the command appropriately. Nevertheless, voice and speech biometric are fast and convenience way of command to control the smart home features. Health monitoring has also shown a significant contribution in smart home environment. By analyzing ECG, blood pressure, blood glucose, blood flow, and temperature the system can monitor and detect early abnormalities or symptoms in users' bodies especially on ill and elder users, thus the information will alert the users to meet doctors. Footsteps and gait can be used to increase surveillance aspect by alert the security alarm system if intruders were found within the house compound.

Besides providing comfort and assistance to the smart home users, it is shown that the security aspect is no longer similar to traditional homes using keys and padlocks, but it has extended beyond physical security such as authentication mechanisms, which has deemed important. This is due to the fact that smart home applications are now controlled via the Internet, and with the advancements of technology, potential intruders can use sophisticated attacks to penetrate the smart home system and easily obtain access to the entire system. Therefore, the next section will further discuss the existing authentication mechanisms in the domain of security.

## 4 Authentication Mechanism

Authentication mechanism refers to a process whereby users provide some form of credentials, which are then compared to those on the file in a database of authorized users' information on a local operating system or within an authentication server. If the credential matches, the process is completed and the user is granted authorization for access. There also exist two or multi-factor authentications that are combined with different factors. Both authentications must be successfully carried out; if one is not successful, the other one is not carried out [65]. Other examples are from the studies by [66, 67]. Authentication mechanism can be classified into four categories. The following sub-sections will elaborate further on each category.

### 4.1 Authentication Based on Knowledge and Ownership Factor

Authentication based on knowledge factor relies on something that a user knows, for example, passwords or PINs. This type of mechanism is highly dependent on the strength of a particular password. Therefore, standard guidelines for constructing a password are necessary, so that users are protected at least to a certain extent. For instance, the password must be of a certain length and a mixture of several characteristics, so that it is hard to be guessed by a third party. The main challenges of using passwords as an authentication mechanism is that users are likely to choose weak passwords due to memorability limitation. Therefore, passwords are often the weakest factor in authentication mechanisms.

Similarly, PINs are also considered as a weak option, as normally PINs constitute of several characters only. Besides human factor limitations, this type of authentication mechanism is also prone to many attacks. There are several ways attackers can obtain the password. First, attackers can attempt to gain access to the database profile in the system, through spying or eavesdropping the secret information or perhaps the passwords itself is self-exposed accidently by a user who has written down their passwords (or PINs) on post-it notes [68].

Despite the drawbacks mentioned, passwords are still found to be a highly relevant and commonly used authentication among users [69]. This is due to its robustness in nature, which is easily compatible across many platforms as it can be seen applied in critical domains such as online banking. Security researchers and academicians are putting a huge effort in studying and proposing countermeasures to increase the protections provided by this authentication mechanism. It can also be applied as two factors as well, for example, a combination of a password and ID card, or fingerprint and password, to make the authentication stronger and reliable. The following Table 2 summarizes the knowledge factor-based authentications.

The second type of authentication mechanism is based on ownership factor. This factor is associated with something that users bring anywhere and anytime. For example, smart cards, ID, token, and passport. Usually, this type of authentication relies on small items that are easy to carry, as without it, users cannot gain access and authorization will not be successful. It also becomes more complicated if the factor is lost,

misplaced or damaged. This type of authentication is prone to counterfeit attacks, whereby attackers attempt to reproduce fake items to substitute the original. Nevertheless, this type of authentication is normally preferable in less critical domains, such as to record daily work attendance at the college or used in online voting. The following Table 3 summarizes the ownership factor-based authentication.

**Table 2.** Knowledge and ownership factor-based authentications

| Knowledge | Mechanisms | Domain | Advantages | Drawbacks | Counter-measures | Ref. |
|---|---|---|---|---|---|---|
| factor-based authentication mechanisms | Password | Online banking, Smart home | Convenience, easier and inexpensive, accurate, cost-effective | Time-consuming, user interaction, forgotten due to frequent changes or too long to remember, shared, observed or hacked | Negative Authentication (anti-password), One-time password (OTP) | [68], [69], [70], [71], [72], [73], [74], [75], [76], [77], [78] |
| | PIN | ATM | | | | |
| | Security question answer | Online banking | | | | |
| | Graphical/pattern password | Smart phone | | | | |
| Ownership factor-based authentication mechanisms | ID card | E-Government, Online Voting, E-Banking | Standard throughout the state and country | Damage, one person can be registered different identity, have to carry everywhere, stolen, shared, fake can be issued. | One-time password authentication scheme for smart card, Password-based authentication scheme using Elliptic Curve Cryptography (ECC) for smart card. | [79], [80] |
| | Passport | Airport Security | | | | |
| | Smart card | University, college, school, Office | | | | |
| | Token | Smartphone, subway and light railway transit | Convenience, easier and inexpensive | Damage, have to carry everywhere, stolen, | | [67], [70], [81], |

Despite the drawbacks based on knowledge and ownership factors in Table 2, most fields and organizations are still using them because they are cheap and the system is not difficult to develop, whereas many man powers have these knowledge and skill to develop the systems. In the other hand, to develop biometric systems, special skills and expertise in that field are needed and are expensive too.

### 4.2 Authentication Based on Biometric Factors

Biometric factors rely on two factors. First is the psychological factor, which is something a person is. These biometric authentications use part of the features in the human body, which include fingerprints, iris, and face. Second is the behavioral factor, which is something a person does. This biometric factor is where a user produces some of the characteristics that come from an action, for example signature, voice, and handwriting recognition. Biometric is a unique element in every human being [82-84]. Besides, biometric is more convenient than traditional methods such as password because the users always have it to themselves. The biometric factor can be used as biometric authentication, whereby it is more reliable to be used in providing access control to many applications because of its robustness, accuracy, and convenience [85-88].

Therefore, researchers and organizations tend to shift from traditional authentication like passwords to biometric authentication. For example, fingerprint, iris, face, and speech recognition are among the established biometric authentications that have been applied in many areas such as online banking, online voting, e-passport, e-health, as well as smart homes. This is because biometric authentication is significantly convenient, and efficient, which is not easily forgotten or lost from the users, given that fingerprint, iris, face, and speech are always together with them. In addition, the benefits of biometric authentication can also reduce fraud among employees since it is unique to every person, whereby they

cannot exchange the part of their body to that of another person. Unlike the traditional authentication mechanisms such as ID card or smart card, the card can be shared, duplicated, and stolen between them [7, 89].

However, biometric authentication has its issues as well, particularly when a part of the body is injured due cuts, burns, and callouses. External substances on a scanner or finger such as dust, oil or lotion may affect the scanner to read the biometric features. Besides, some people may have peculiar characteristics such as being too tall or too short, thus it affects the distance between the scanner device to capture the face or eyes. From the criminal point of view, the intruders can create artificial biometrics such as a picture of a fingerprint, an image of contact lenses with fake irises, sticky fingerprints made form gelatin, voice, and signature imitation [31, 90]. For this reason, to prevent the drawbacks, many researches have been done to counter these problems. Among the preventions of these problems are to implement cancellable biometrics, fuzzy vault, and anti-spoofing, in order to protect the secret biometric templates from intruders capturing them [91-95].

Numerous areas have now implemented strong authentications for access control, thus biometric authentication can be said to be more reliable than other available authentication mechanisms, where traditional passwords can prompt to hackers [95-96]. Hence, to make authentications more powerful, a combination of two factors is a good way for the authentication mechanisms, such as the combination of fingerprint authentication and passwords or PIN number [65-67]. The following Table 3 summarizes the types of biometric authentication mechanisms along with their advantages, drawbacks, and countermeasures.

**Table 3.** Biometric-based authentication mechanisms

| Biometric Factors | Functions | Area/Domain | Benefits | Drawbacks | Ref. |
|---|---|---|---|---|---|
| Fingerprint | Compares the characteristic templates of a fingertip to a stored template | E-banking, Online voting, Smart home, E-passport, Forensic | Convenient, efficient, not easily lost or forgotten, non-repudiation, accuracy, reliable, speed, always with users, reduces fraud | Injured, peculiar, artificial fingerprints/templates, foreign substances on the scanner<br>*Counter-measures:* Anti-spoofing, biometric cryptosystems, cancellable biometrics, fuzzy vault, reversible watermarking | [31],[32], [48], [81], [93], [70], [97], [98], [99], [100], [101], [102], [103] |
| Hand geometry/ grip-pattern | Unique features of a hand such as the length of the fingers, and the width of the hand | Smart gun | | | |
| Vein | Unique pattern of palm and finger veins | Smart home, E-banking | | | |
| Handwriting/ Signature | Uses a pen and a specialised writing tablet to capture a shape, a speed, a stroke, a pen pressure, and timing information | E-banking | | Forgery | [104][105] |
| Typing | Capturing the time intervals between the keystrokes and the amount of time a key is depressed | Students typing pattern behavior | Prevent identity theft | Less accuracy (typing changing), not suitable for authentication | [106] |
| Footsteps | Signals extracted from floor sensors. | Smart home/ smart building | Recognition at a distance or at low resolution | Occlusions, differences in lighting conditions, and background movements, unobtrusive movements | [43], [44], [45], [46], [107] |
| Gait | Video sequences of people walking | | | | |
| Iris | Measures a coloured ring around the pupil of an eye. | E-Passport, Smart home, Wireless Sensor Networks, E-Banking | Accuracy, reliable, speed | Wear contact lens, glasses, eye surgery, lighting, fake biometric, distance between devices | [7], [108] |

**Table 3.** Biometric-based authentication mechanisms (continue)

| Biometric Factors | Functions | Area/Domain | Benefits | Drawbacks | Ref. |
|---|---|---|---|---|---|
| Retina | Identified by the distinctive pattern of blood vessels on the retina, at the back of the eye. | | | | |
| Face | Uses different algorithms to create a biometric signature of the face and matches it through an automated or semi-automated process. | Smart homes, E-Health, E-passport, Steganography | Low cost if it use in Smartphone camera | Fake biometric, angle image, facial changing (age, medication, and weight), and distance between devices *Counter-measures:* Fuzzy Vault | [57], [92] |
| Ear | The identification of an individual using the shape of the ear | Smart home | | Difficult to see the ear, and inconvenient for women wearing scarves. | [59] |
| Height | Measure the height of Individuals | Smart home | Effective among small populations, cheap, convenient and minimally invasive | Ageing factor might change, adult women usually are the same height (if more than one woman in the house) | [58] |
| Speech/voice | Identifies people by unique characteristics of their voice as rhythm of the vocal cords and the concavity of the mouth to create a "voice print" | Smart home, forensic, telephone banking | Hygiene benefit, remote authentication | Variable nature of human voice, background noise, cold, cough, surgery | [51], [52], [53], [54], [55], [109], [110] |
| Body Odor | The use of an individual's odor to determine identity | Authentication/ detect disease by using e-nose / health screening | Lowest error rate, fool-prove, impossible to replicate human odor, deodorant and perfumes cannot mask the basic human odor | Lack of knowledge in information processing, difficult to develop | [111], [112], [113], [114], [115], [116] |
| EEG (electro-encephalogram) | Electrical recording of brain activity | Authentication/ Identification | Confidential, difficult to mimic and almost impossible to steal | Difficult in setting up the subject for signal acquisition, obstacle in acquisition protocol, EEG cannot be developed at a distance, brain waves are weak signals and sensitive to the contamination from many artefact signals. | [117], [118], [119], [120] |
| ECG (electro-cardiogram) | Records the electrical activity of the heart for a person at a given time | Authentication/ Identification | Stability and distinctiveness | ECG is not strong as other biometric factors in terms of identification | [121], [122] |
| Blood pressure, blood glucose, blood flow, temperature | Vital signs of body | Health monitoring | Prevents the need for expensive omputations | Low power, limited memory, low computational memory | [123], [124], [125] |

**Table 3.** Biometric-based authentication mechanisms (continue)

| Biometric Factors | Functions | Area/Domain | Benefits | Drawbacks | Ref. |
|---|---|---|---|---|---|
| DNA (deoxyribonucleic acid) | The identification of an individual using the analysis of segments from DNA | Forensic, ATM security, person identification | Assist in investigation, support evidence presented in a court of law | Privacy issues associated with DNA-based biometric systems because the DNA samples may contain a wealth of personal information | [126], [127], [128] |

Based on the Table 3 above, visual biometric like fingerprint, hand geometry, and vein recognition are among the highest adopted in many fields and domain areas. This is because it is convenient, efficient, not easily lost or forgotten, non-repudiation, accuracy, reliable, speed, and always with users. Although fingerprint may be victim by the snooping attack or artificial fingerprint, nevertheless it is among the cheaper and affordable biometric factors to be applied in smart application whereas to identify someone and to authenticate users. Besides, among other biometric factors that gain attraction for research is body odor. Study have shown that, body odor have the lowest error rate which is 15% compare with other biometric factors [111]. The advantages are unique and impossible to duplicate and fool-prove, which means it does not have to get permission by the user to use it. The technology lies in electronic nose (E-Nose). By using E-Nose, health screening can be done by smell certain chemical in our body that detects disease like gastroenterology relating disorder. Despite of it advantages, it is still in research and lack of knowledge in term of information processing and difficult to develop. But it is of interest to further research into this biometric factor as it have low error rate compare to other biometric factors.

## 5 Discussion

Given these points, biometric factors are a sophisticated way to control the smart home environment technology that could assist and contribute to human beings in various aspects and conditions. As described in Section 2, biometric factors can provide smart home users with security, comfort, healthcare, and energy conservation.

Security plays a big role for the smart home environment, whereby a house is a shelter for people to protect themselves from danger. One element in the security for smart home environment is access control and authentication. Biometric factors can provide user with biometric authentication to protect the house. For example, the access control of smart homes can be implemented using fingerprint, iris or face recognition at the entrance door. This will ease the users and save time as the users do not have to bring any physical key and smart card or to key-in the passwords. It is also very secure as biometrics are hard for intruders to break the system. However, if an unrecognized user enters the house, the fingerprint or biometric scanner can capture the picture of the unrecognized user to activate the alarm system.

Besides, biometric authentication can be used in smart appliances to identify and verify the users if they want to use that function. Although all smart home users have the privilege to use all the appliances and services in the smart home, there are certain appliances that are available only for certain users. For example, dangerous appliances like stove, oven, microwave, and washing machine can only be used by adult users and are not authorized for children, whereby the users have to scan their fingerprint at the appliances to activate them. Therefore, only the users' fingerprint templates are saved in the smart appliances' memory. Other biometric factors are also applicable to be implemented, such as voice recognition, whereby the smart appliances recognize the authorized users' voice only.

In addition, footsteps recognition can be implemented to track users in the house, in which the signal from the smart floor can sense the footsteps and sounds of the users and can act as surveillance if intruders gain access inside the house; hence, the smart floor will trigger the alarm system to activate. Readers can refer to these articles for further reading about security and safety topic [48, 129-136].

With the help of biometric factors such as human body heat, face, iris, and voice recognition, various tasks can be implemented, such as lighting and heating, ventilation, and air conditioning (HVAC) will be activated by detecting the presence of the users, in which they can sense the human body heat. Apart from that, the users also can use speech recognition to do voice command control to the smart appliances to activate them. Besides, biometric factors can ease and minimize the workload of the housewife, for example, using voice or facial recognition to control the appliances, such as cooking, laundry, dish

washing, cleaning the house, and many more. Furthermore, biometric factors can ease the smart home users with remote monitoring from their smart phone, for example using voice command control that is integrated between the smart phone and smart home. Some related articles about comfort and luxury topic can be read here [137-139].

Biometric factors such blood pressure, blood sugar, body temperature, heart and pulse rate, and electrocardiogram (ECG) can be used to measure the health problem of the users. Nowadays, there are devices that can be implanted inside the human body and are connected through wireless network to capture the health information, in order to maintain the health of certain people. This service can be applied in the smart home environment for the elderly, sick, and disabled people, as well as people living alone with health problems. In addition, vision-impaired people are suitable users to benefit from the smart home environment. With the help of voice recognition, many tasks can be done by command voice control, whereby it is likely to talk to the home. More articles on healthcare services in smart home can be found here [20, 40, 61, 64, 140-144].

Smart home features have the ability to sense the humans in the house as mentioned above by detecting human body heat. Power consumption in the house such as electricity, water, and gas can be reduced, whereby lighting and air-conditioner will automatically switch off if no one is at a certain room or area. Smart appliances like television will switch on if authorize users control it. Furthermore, it can implement face detection to detect the users while watching television. The device can also detect if users are watching television or not; if they accidently slept or are away from that area, the device will automatically switch off if there is no detection of users' face after a few minutes. Related articles about energy conservation topic can be read here [10, 17, 30, 145-148].

The following Fig. 2 shows the overview of biometric factors intended for smart home environment which is enhanced from [34-35, 39-40].

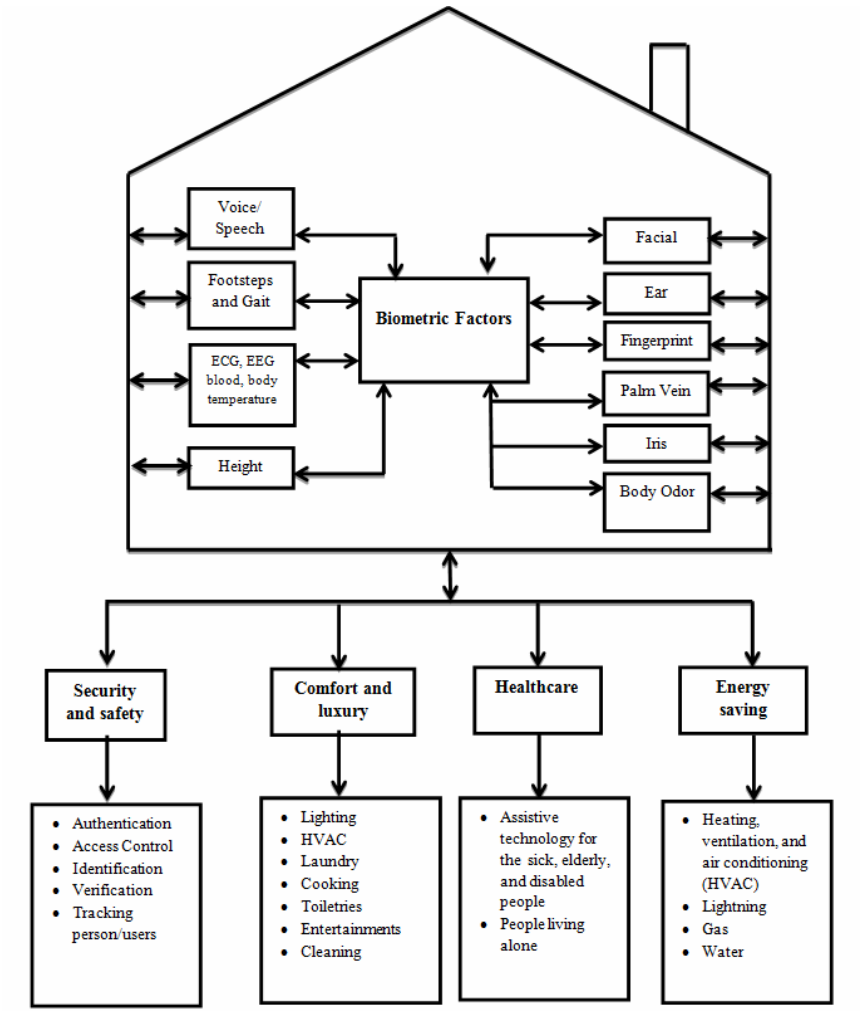


**Fig. 2.** The overview of biometric factors intended for smart home environment

## 6 Conclusion and Future Work

This paper has provide a review on the general smart home concept and system, security authentication mechanism and its related issues, the benefits of biometrics that have been applied in many areas, as well as smart homes. Given this point, there are many biometric factors that can be implemented for the intended services in smart home environment, which are security and safety, conform and luxury, healthcare, and energy conservation.

This paper emphasized its focus on reviewing relevant existing work and making further critical analysis towards them, thus this should be claimed as its main contribution. Interested researchers in this domain may be able to extend this work further especially those looking into specific issues related to smart home environment. Instead of relying on empirical data produced through experiments this paper highlighted analysis and comparison done on various aspects of smart home environment particularly focusing on aspects such as security, comfort and energy saving. The comparison was done based on peer to peer approach. For example, when comparing a particular biometric mechanism, comparison was done with other similar biometric mechanism within the domain of smart home application. This provides a holistic review on that perspective for future researcher to embark on.

In the long run, biometric factors are vital to be applied for the smart home environment, especially in the security and safety features. For future work, more research should be conducted to study further on the technological advances of biometric authentication for smart home environment. This include things like lightweight technology that can be applied to the biometric authentication for power saving, security, and reliability. This is because a smart home is where a family lives and stays for a long time. Therefore, it is wise to consider a robust biometric factor to protect the house and also the family.

## Acknowledgments

The authors wish to thanks the Ministry of Higher Education (Malaysia) for funding this study under the Trans Disciplinary Research Grant Scheme (TRGS), S/O code: 13164 and RIMC Universiti Utara Malaysia for administration of this study.

## References

[1] S.H. Seo, T. Cho, An access control mechanism for remote control of home security system, in: Proc. 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2012, 2012.

[2] D. Sunehra, A. Bano, An intelligent surveillance with cloud storage for home security, in: Proc. 11th IEEE India Conference: Emerging Trends and Innovation in Technology, INDICON 2014, 2015.

[3] A. Jacobsson, M. Boldt, B. Carlsson, On the risk exposure of smart home automation systems, in: Proc. Future Internet of Things and Cloud (FiCloud), 2014 International Conference, 2014.

[4] R. Piyare, R.L. Seong, Smart home-control and monitoring system using smart phone, in: Proc. The 1st International Conference on Convergence and It's Application, 2013.

[5] T. Mendes, R. Godina, E. Rodrigues, J. Matias, J. Catalão, Smart home communication technologies and applications: wireless protocol assessment for home area network resources, Energies 8(7)(2015) 7279-7311.

[6] K. Lee, R.D. Caytiles, S. Lee, A study of the architectural design of smart homes based on hierarchical wireless multimedia management systems, International Journal of Control and Automation 6(6)(2013) 261-266.

[7] F. Ishengoma, Authentication system for smart homes based on ARM7TDMI-S and IRIS-Fingerprint recognition technologies, CiiT International Journal of Programmable Device Circuits and Systems 6(6)(2014) 64-69.

[8] S. Ventylees Raj, Implementation of pervasive computing based high-secure smart home system, in: Proc. 2012 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2012, 2012.

[9] Y. Dahl, Redefining smartness: the smart home as an interactional problem, in: Proc. 4th International Conference on Intelligent Environments (IE 08), 2008.

[10] R. Kadam, P. Mahamuni, Y. Parikh, Smart home system, International Journal of Innovative Research in Advanced Engineering 2(1)(2015) 81-86.

[11] S. Bagaveyev, D.J. Cook, Designing and evaluating active learning methods for activity, in: Proc. 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing Adjunct Publication, 2014.

[12] A.N. Gowda, D.L. Girijamba, G.N. Rishika, S.D. Shruthi, S. Niveditha, Smart home control using lab VIEW, International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) 2(5)(2013) 485-490.

[13] B. Ivanov, H. Ruser, M. Kellner, Presence detection and person identification in smart homes, in: Proc. International Conference on Sensors and Systems, 2002.

[14] A.J.B. Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, C. Dixon, Home automation in the wild: challenges and opportunities, in: Proc. CHI Conference on Human Factors in Computing Systems, 2011.

[15] K. Bouchard, S. Giroux, Smart homes and the challenges of data, in: Proc. the 8th ACM International Conference on PErvasive Technologies Related to Assistive Environments (PETRA ’15), 2015.

[16] S. Nakamura, S. Shigaki, A. Hiromori, H. Yamaguchi, T. Higashino, A model-based approach to support smart and social home living, in: Proc. the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp 2015), 2015.

[17] C. Felicetti, R. De Rose, C. Raso, A.M. Felicetti, S. Ammirato, Collaborative smart environments for energy-efficiency and quality of life, International Journal of Engineering and Technology 7(2)(2015) 543-552.

[18] L. Liu, Y. Liu, A. Zomaya, L. Wang, S. Hu, Economical and balanced energy usage in the smart home infrastructure: a tutorial and new results, IEEE Transactions on Emerging Topics in Computing 3(4)(2015) 556-570.

[19] S. Mennicken, J. Vermeulen, E.M. Huang, From today â€TMs augmented houses to tomorrow â€TMs smart homes: new directions for home automation research, in: Proc. UbiComp ’14 Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, 2014.

[20] P.W. Matthew, Biometric implementation in autonomous systems with an emphasis on smart home applicability, in: Proc. International Conference on Information Society (I-Society 2011), 2011.

[21] K. Doelling, J. Shin, D.O. Popa, Service robotics for the home, in: Proc. the 7th International Conference on PErvasive Technologies Related to Assistive Environments - PETRA ’14, 2014.

[22] V.K. Ravishankar, B. Winslow, D. Mahoney, Smart home strategies for user-centered functional assessment of older adults, International Journal of Automation and Smart Technology 5(4)(2015) 233-242.

[23] J. Lapointe, B. Bouchard, J. Bouchard, A. Potvin, A. Bouzouane, Smart homes for people with Alzheimer’s disease: adapting prompting strategies to the patient’s cognitive profile, in: Proce. the 8th ACM International Conference on PErvasive Technologies Related to Assistive Environments (PETRA ’12), 2012.

[24] S. Solaimani, W. Keijzer-Broers, H. Bouwman, What we do - and don’t - know about the smart home: an analysis of the Smart Home literature, Indoor and Built Environment 24(3)(2013) 370-383.

[25] W. Stallings, Access control, in: Proc. Computer Security, 2012.

[26] J.R. Rosslin, K. Tai-hoon, Applications, systems and methods in smart home technology: a review, International Journal of Advanced Science and Technology 15(2010) 37-48.

[27] Y. Wardhana, B. Hardian, G. Guarddin, H. Rasyidi, Context aware door access control on private room using fuzzy logic:

case study of smart home, in: Proc. 2013 International Conference on Advanced Computer Science and Information Systems, ICACSIS 2013, 2013.

[28] Y.T. Park, P. Sthapit, J.Y. Pyun, Smart digital door lock for the home automation, in: Proc. IEEE Region 10 Annual International Conference, Proceedings/TENCON, 2009.

[29] M. Covington, M. Moyer, M. Ahamad, Generalized role-based access control for securing future applications, in: Proc. 23rd National Information Systems Security Conference, (NISSC 2000), 2000.

[30] F. Allerding, H. Schmeck, Organic smart home - architecture for energy management in intelligent buildings, in: Proc. the 2011 Workshop on Organic Computing - OC '11, 2011.

[31] I. Vorobyeva, D. Guriel, M. Ferguson, H. Oladapo, Benefits and issues of biometric technologies, in: Proc. IEEE SOUTHEASTCON 2014, 2014.

[32] B. El-Basioni, S. El-kader, M. Abdelmonim, Smart home design using wireless sensor network and biometric technologies, International Journal of Application or Innovation in Engineering & Management (IJAIEM) 2(3)(2013) 413-429.

[33] D. Bregman, A. Korman, A universal implementation model for the smart home, International Journal of Smart Home 3(3)(2009) 15-30.

[34] L.C. De Silva, C. Morikawa, I.M. Petra, State of the art of smart homes, Engineering Applications of Artificial Intelligence 25(7)(2012) 1313-1321.

[35] M.R. Alam, M.B.I. Reaz, M.A. Mohd-Ali, A review of smart homes — past, present, and future, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews 42(6)(2012) 1190-1203.

[36] J. Israelsohn, LED lighting in home automation: Ready, Aim. <http://www.mouser.com/applications/LED-lighting-home-automation/>, n.d.

[37] A. Bejarano, B. Fernandez, M. Jimeno, A. Salazar, P. Wightman, Towards the evolution of smart home environments: a survey, International Journal of Automation and Smart Technology 6(3)(2016) 105-136.

[38] C. Wilson, T. Hargreaves, R. Hauxwell-Baldwin, Smart homes and their users: a systematic analysis and key challenges, Personal and Ubiquitous Computing 19(2)(2015) 463-476.

[39] C. Badica, M. Brezovan, A. Badica, An overview of smart home environments: Architectures, technologies and applications, CEUR Workshop Proceedings 1036(i)(2013) 78-85.

[40] M. Chan, E. Campo, D. Esteve, J.Y. Fourniols, Smart homes - Current features and future perspectives, Maturitas 64(2)(2009) 90-97.

[41] N. Balta-Ozkan, R. Davidson, M. Bicket, L. Whitmarsh, Social barriers to the adoption of smart homes, Energy Policy 63(2013) 363-374.

[42] M. TOLENTINO, Biometric trends for the smart homeSiliconANGLE. <http://siliconangle.com/blog/2015/02/13/biometric-trends-for-the-smart-home/>, 2015.

[43] R. Vera-Rodriguez, J. Fierrez, J.S.D. Mason, J. Orteua-Garcia, A novel approach of gait recognition through fusion with footstep information, in: Proc. 2013 International Conference on Biometrics, ICB 2013, 2013.

[44] R. Vera-Rodriguez, R. Lewis, J.S.D. Mason, Footstep recognition for a smart home environment, International Journal of Smart Home 2(2)(2008) 95-110.

[45] R.L. Carvalho, P.F.F. Rosa, Identification system for smart homes using footstep sounds, in: Proc. IEEE International Symposium on Industrial Electronics, 2010.

[46] R.J. Orr, G.D. Abowd, The smart floor: a mechanism for natural user identification and tracking, in: Proc. Conference on

Human Factors in Computing Systems, 2000.

[47] M. Sahani, C. Nanda, A.K. Sahu, B. Pattnaik, Web-based online embedded door access control and home security system based on face recognition, in: Proc. the 2015 International Conference on Circuits, Power and Computing Technologies, 2015.

[48] N.S. Prakash, N. Venkatram, Establishing efficient security scheme in home IOT devices through biometric finger print technique, Indian Journal of Science and Technology 9(17)(2016) 1-8.

[49] A. Ahmed, T. Ahmed, S. Ullah, M. Islam, Controlling and securing a digital home using multiple sensor based perception system Integrated with mobile and voice technology, International Journal of Information and Communication Technology Research 1(5)(2011) 189-196.

[50] D.G. Shin, M.S. Jun, Home IoT device certification through speaker recognition, in: Proc. International Conference on Advanced Communication Technology, ICACT. 2015, 2015.

[51] K.A. Lee, A. Larcher, H. Thai, B. Ma, H. Li, Joint application of speech and speaker recognition for automation and security in smart home, in: Proc. the Annual Conference of the International Speech Communication Association, INTERSPEECH, 2011.

[52] S. Hidayat, S.F. Firmanda, Scheduler and voice recognition on home automation control system, in: Proc. 3rd International Conference on Information and Communication Technology (ICoICT), 2015.

[53] E. Fytrakis, I. Georgoulas, J. Part, Y. Zhu, Speech-based home automation system, in: Proc. British HCI 2015, 2015.

[54] B. Yuksekkaya, A.A. Kayalar, M.B. Tosun, M.K. Ozcan, A.Z. Alkar, A GSM, internet and speech controlled wireless interactive home automation system, IEEE Transactions on Consumer Electronics 52(3)(2006) 837-843.

[55] O. Joymala, N. Khare, Securing a smart home network using voice biometric, International Journal of Application or Innovation in Engineering & Management 5(2)(2016) 113-118.

[56] S.A. Khowaja, K. Dahri, M.A. Kumbhar, A.M. Soomro, Facial Expression Recognition using two-tier classification and its Application to Smart Home Automation System, in: Proc. Emerging Technologies (ICET), 2015 International Conference, 2015.

[57] F. Zuo, P. De With, Real-time embedded face recognition for smart home, 184 IEEE Transactions on Consumer Electronics 51(1)(2005) 183-190.

[58] V. Srinivasan, J. Stankovic, K. Whitehouse, Using height sensors for biometric identification in multi-resident homes, Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 6030 LNCS (1)(2010) 337-354.

[59] P.N. Ali Fahmi, E. Kodirov, Ardiansyah, D. Choi, G. Lee, Hey home, open your door, I'm back! authentication system using ear biometrics for smart home, International Journal of Smart Home 7(1)(2013) 173-182.

[60] R. Khokher, R.C. Singh, Generation of security key using ECG signal, in: Proc. International Conference on Computing, Communication and Automation (ICCCA2015), 2015.

[61] F. Adib, H. Mao, Z. Kabelac, D. Katabi, R.C. Miller, Smart homes that monitor breathing and heart rate, in: Proc. the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15, 2015.

[62] J.F. Hu, Z.D. Mu, Authentication system using EEG biometric for smart home, Applied Mechanics and Materials 457-458(2013) 1228-1231.

[63] S. Cherukuri, K.K. Venkatasubramanian, S.K.S. Gupta, Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body, in: Proc. the International Conference on Parallel Processing

Workshops, 2003.

[64] E.D. Muse, P.M. Barrett, S.R. Steinhubl, E.J. Topol, Towards a smart medical home, The Lancet 389(10067)(2017) 358.

[65] M. Vipin, A.V. Sarad, K. Sankar, A Multi way tree for token based authentication, in: Proc. International Conference on Computer Science and Software Engineering, CSSE 2008. 3, 2008.

[66] D. Giri, R.S. Sherratt, T. Maitra, R. Amin, Efficient biometric and password based mutual authentication for consumer USB mass storage devices, IEEE Transactions on Consumer Electronics 61(4)(2015) 491-499.

[67] A.P. Muniyandi, R. Ramasamy, Indrani, Password Based Remote Authentication Scheme using ECC for Smart Card, in: Proc. of the 2011 International Conference on Communication, Computing & Security (ICCCS '11), 2011.

[68] D. Dasgupta, S. Saha, A biologically inspired password authentication system, in: S. Frederick, P. Greg, A. Krings, A. Robert, M. Ali (Eds.), Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies (CSIIRW '09), ACM, New York, NY, USA, 2009, pp. 1-4.

[69] A. Conklin, G. Dietrich, D. Walz, Password-based authentication: a system perspective, system sciences, in: Proc. the 37th Annual Hawaii International Conference, 2004.

[70] M. Koschuch, M. Hudler, H. Eigner, Z. Saffer, Token-based authentication for smartphones, in: Proc. ICETE 2013- 10th Int. Joint Conf. on E-Business and Telecommunications, 2013.

[71] A. Badlani, S. Bhanot, Smart home system design based on artificial neural networks, in: Proc. the World Congress on Engineering and Computer Science, 2011.

[72] A. Joseph, D.B.L. Bong, D.A.A. Mat, Application of neural network in user authentication for smart home system, International Journal of Electrical and Computer Engineering 4(5)(2009) 1146-1153.

[73] J. Al-Muhtadi, M. Anand, M.D. Mickunas, R. Campbell, Secure smart homes using Jini and UIUC SESAME, in: Proc. Annual Computer Security Applications Conference, 2000.

[74] T. Li, J. Ren, X. Tang, Secure wireless monitoring and control systems for smart grid and smart home, IEEE Wireless Communications 19(3)(2012) 66-73.

[75] S. Kumar, S.R. Lee, Android based smart home system with control via Bluetooth and internet connectivity, in: Proc. the International Symposium on Consumer Electronics, 2014.

[76] S. Kumar, Ubiquitous smart home system using Android application, International Journal of Computer Networks & Communications 6(1)(2014) 33-43.

[77] I. Kaur, Microcontroller based home automation system with security, IJACSA International Journal of Advanced Computer Science and Applications 1(6)(2010) 60-65.

[78] S.Z. Reyhani, M. Mahdavi, User authentication using neural network in smart home networks, International Journal of Smart Home 1(2)(2007) 147-154.

[79] M. Faúndez-Zanuy, On the vulnerability of biometric security systems, IEEE Aerospace and Electronic Systems Magazine 19(6)(2004) 3-8.

[80] B. Vaidya, J.H. Park, S.-S. Yeo, J.. Rodrigues, Robust one-time password authentication scheme using smart card for home network environment, Computer Communications 34(3)(2011) 326-336.

[81] C.T. Li, M.S. Hwang, An efficient biometrics-based remote user authentication scheme using smart cards, Journal of Network and Computer Applications 33(1)(2010) 1-5.

[82] G. Lawton, A new era in security, Computer 31(8)(1998) 16-18.

[83] A. Dasso, A. Funes, Verification, Validation, and Testing in Software Engineering, Idea Group Publishing, London, 2007.

[84] H. Van De Haar, D. Van Greunen, D. Pottas, The characteristics of a biometric, in: Proc. 2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference, 2013.

[85] S. Prabhakar, S. Pankanti, A.K. Jain, Biometric recognition: Security and privacy concerns, IEEE Security & Privacy 1(2)(2003) 33-42.

[86] M. Barni, G. Droandi, R. Lazzeretti, Privacy protection in biometric-based recognition systems, IEEE Signal Processing Magazine 32(5)(2015) 66-76.

[87] S. Bakshi, T. Tuglular, Security through human-factors and biometrics, in: Proc. the 6th International Conference on Security of Information and Networks - SIN ’13, 2013.

[88] SANS Institute Infosec Reading Room, Biometrics: A Double Edged Sword - Security and Privacy, SANS Institute InfoSec Reading Room, Atlanta, GA, 2002.

[89] A. Rabie, U. Handmann, Biometric for home environment challenges, modalities and applications, Information Technology and Computer Applications Congress (WCITCA), 2015.

[90] A.K. Jain, A. Kumar, Biometrics of next generation: an overview, in: E. Mordini, D. Tzovaras (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context, Spring, Dordrecht, 2012, pp. 49-79.

[91] K.M.S. Soyjaudah, G. Ramsawock, M.Y. Khodabacchus, Cloud computing authentication using cancellable biometrics, IEEE AFRICON, 2013.

[92] T. Frassen, X. Zhou, C. Busch, Fuzzy vault for 3D face recognition systems, in: Proc. 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008.

[93] S. Hidano, T. Ohki, N. Komatsu, M. Kasahara, On biometric encryption using fingerprint and it’s security evaluation, in: Proc. 2008 10th International Conference on Control, Automation, Robotics and Vision, ICARCV 2008, 2008.

[94] E. Marasco, A. Ross, A survey on antispoofing schemes for fingerprint recognition systems, ACM Computing Surveys 47(2)(2014) 1-36.

[95] M. Belkhede, V. Gulhane, P. Bajaj, Biometric mechanism for enhanced security of online transaction on Android system: a design approach, in: Proc. 2012 14th International Conference on Advanced Communication Technology (ICACT), 2012.

[96] J.E. Thurman, Biometric security now and in the future, [dissertation] Greenvile, NC: East Carolina University, 2016.

[97] O. Ouda, N. Tsumura, T. Nakaguchi, Tokenless cancelable biometrics scheme for protecting iriscodes, in: Proc. International Conference on Pattern Recognition, 2010.

[98] C. Rathgeb, A. Uhl, A survey on biometric cryptosystems and cancelable biometrics, EURASIP Journal on Information Security 2011(1)(2011) 3.

[99] N.K. Ratha, S. Chikkerur, J.H. Connell, R.M. Bolle, Generating cancelable fingerprint templates, IEEE Transactions on Pattern Analysis and Machine Intelligence 29(4)(2007) 561-572.

[100] V.B. Joshi, M.S. Raval, S. Mitra, P.P. Rege, S.K. Parulkar, Reversible watermarking technique to enhance security of a biometric authentication system, in: Proc. 2013 Fourth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG), 2013.

[101] K. Nandakumar, A.K. Jain, A. Nagar, Biometric template security, Eurasip Journal on Advances in Signal Processing 2008 (2008).

[102] M. Boatwright, L. Xin, What do we know about biometrics authentication?, in: Proc. the 4th Annual Conference on Information Security Curriculum Development (InfoSecCD ’07).

[103] R.N.J. Veldhuis, A.M. Bazen, J. Kauffman, P.H. Hartel, Biometric verification based on grip-pattern recognition, in: Proc. IS\&T/SPIE 16th Annual Symp. on Electronic Imaging – Security, 2004.

[104] L. Ballard, D. Lopresti, F. Monrose, Forgery quality and its implications for behavioral biometric security, IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics 37(5)(2007) 1107-1118.

[105] S. Mohammadi, S. Abedi, ECC-based biometric signature: a new approach in electronic banking security, in: Proc. the International Symposium on Electronic Commerce and Security, ISECS 2008, 2008.

[106] B. Ngugi, B.K. Kahn, M. Tremaine, Typing Biometrics, Journal of Data and Information Quality 2(2)(2011) 1-21.

[107] R. Ma, Cognitive heterogeneous sensor platform for human biometric and activity pattern analysis, [dissertation] Tuscaloosa: The University of Alabama, 2016.

[108] M. Abid, S. Kanade, D. Petrovska-Delacrétaz, B. Dorizzi, H. Afifi, Iris based authentication mechanism for e-Passports, in: Proc. 2010 2nd International Workshop on Security and Communication Networks, IWSCN 2010, 2010.

[109] M. Adamski, B. Von Solms, An open speaker recognition enabled identification and authentication system, 2014 IST-Africa Conference and Exhibition, IST-Africa 2014, 2014.

[110] R.A. Rashid, N.H. Mahalin, M.A. Sarijari, A.A. Abdul Aziz, Security system using biometric technology: design and implementation of voice recognition system (VRS), in: Proc. the International Conference on Computer and Communication Engineering 2008, ICCCE08: Global Links for Human Development, 2008.

[111] P. Inbavalli, G. Nandhini, Body Odor as a Biometric Authentication, International Journal of Computer Science and Information Technologies 5(5)(2014) 6270-6274.

[112] U.P. de Madrid, Identity verification: Body odor as a biometric identifierScienceDaily. <www.sciencedaily.com/releases/2014/02/140204073823.htm>, 2014.

[113] M. Gibbs, Biometrics: body odor authentication perception and acceptance, ACM SIGCAS Computers and Society 40(4)(2010) 16-24.

[114] A. Rashed, H. Santos, Odour user interface for authentication: possibility and acceptance: case study, in: Proc. the International MultiConference of Engineers and Computer Scientists (IMECS'10), 2010.

[115] C. Wongchoosuk, M. Lutz, T. Kerdcharoen, Detection and classification of human body odor using an electronic nose, Sensors 9(9)(2009) 7234-7249.

[116] D.J. Penn, E. Oberzaucher, K. Grammer, G. Fischer, H.A. Soini, D. Wiesler, M. V Novotny, S.J. Dixon, Y. Xu, R.G. Brereton, Individual and gender fingerprints in human body odour, Journal of the Royal Society, Interface/the Royal Society 4(13)(2007) 331-40.

[117] M. DelPozo-Banos, C.M. Travieso, C.T. Weidemann, J.B. Alonso, EEG biometric identification: a thorough exploration of the time-frequency domain., Journal of Neural Engineering 12(5)(2015) 56019.

[118] C.R. Hema, Biometric Identification using Electroencephalography, International Journal of Computer Applications 106(15)(2014) 17-22.

[119] A.S. Danko, G.C. Fernandez, My brain is my passport. Verify me, in: Proc. 2016 IEEE International Conference on Consumer Electronics, ICCE 2016, 2016.

[120] E. Maiorana, D. La Rocca, P. Campisi, On the permanence of EEG signals for biometric recognition, IEEE Transactions on Information Forensics and Security 11(1)(2016) 163-175.

[121] S. Peter, B.P. Reddy, F. Momtaz, T. Givargis, Design of secure ECG-based biometric authentication in body area sensor networks, Sensors (Switzerland) 16(4)(2016).

[122] M. Bassiouni, W. Khalefa, E.A. EL-Dahsan, A.M. Salem, A machine learning technique for person identification using ECG signals, International Journal of Applied Physics. 1(2016) 37-41.

[123] K. Lai, S. Samoil, S.N. Yanushkevich, G. Collaud, Application of biometric technologies in biomedical systems, in: Proc. DT 2014 - 10th International Conference on Digital Technologies 2014, 2014.

[124] K. Okereafor, O. Osuagwu, C. Onime, Multi-biometric liveness detection - a new perspective, West African Journal of Industrial and Academic Research 16(1)(2016) 26-37.

[125] M. Das, S. Sarker, S.L. Ahad, A novel health support system with biometric data acquisition device, in: Proc. 19th International Conference on Computer and Information Technology, 2016.

[126] A.K. Jain, A. Ross, Bridging the gap: from biometrics to forensics, Phil. Trans. R. Soc. B. 370(1674)(2015) 20140254.

[127] A. Felix, Improving Atm Security Check Using DNA Biometrics, American Journal of Engineering Research 4(6)(2015) 152-159.

[128] O. Lloanusi, I. Okeke, Automating DNA biometric recognition for real-time person identification, in: Proc. the 1st African International Conference/Workshop on Applications of Nanotechnology to Energy, Health and Environment, 2014.

[129] R.J. Robles, T. Kim, A review on security in smart home development, International Journal of Advanced Science and Technology 15(2010) 13-22.

[130] M.R. Alam, M.B.I. Reaz, M.A.M. Ali, A review of smart homes - past, present, and future, IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews 42(6)(2012) 1190-1203.

[131] C. Levy-Bencheton, E. Darra, G. Tetu, G. Dufay, M. Alattar, Security and resilience of smart home environments good practices and recommendations, in: Proc. The European Union Agency for Network and Information Security (ENISA), 2015.

[132] I. Kapoor, P. Sharma, Home security using biometric sensor technology, International Journal of Control Theory and Applications 9(17)(2016) 8407-8413.

[133] A. Braeken, P. Porambage, M. Stojmenovic, L. Lambrinos, eDAAAS: efficient distributed anonymous authentication and access in smart homes, International Journal of Distributed Sensor Networks 12(12)(2016) 155014771668203.

[134] J. Dahmen, D.J. Cook, X. Wang, W. Honglei, Smart secure homes: a survey of smart home technologies that sense, assess, and respond to security threats, Journal of Reliable Intelligent Environments 3(2)(2017) 83-98.

[135] K.M. Subhani, M.K. DS, An investigative study for smart home security: issues, challenges and countermeasures, International Journal of Pharmacy & Technology 8(4)(2016) 19448-19459.

[136] A. Bin Karnain, A review on ZigBee security enhancement in smart home environment, in: Proc. Information Science and Security (ICISS), 2015.

[137] V. Vimarlund, S. Wass, Big data, smart homes and ambient assisted living, Yearbook of Medical Informatics 9(1)(2014) 143-9.

[138] L. Chen, C.D. Nugent, H. Wang, A knowledge-driven approach to activity recognition in smart homes, IEEE Transactions on Knowledge and Data Engineering 24(6)(2012) 961-974.

[139] Y. Strengers, Creating pleasance: new needs for the smart home. <http://www.demand.ac.uk/10/06/2016/creating-pleasance-new-needs-for-the-smart-home-yolande-strengers>, 2016 (accessed 13.01.2017).

[140] B. Winslow, Smart home strategies for user-centered functional assessment of older adults, International Journal of Automation and Smart Technology 5(4)(2015) 233-242.

[141] L. Liu, E. Stroulia, I. Nikolaidis, A. Miguel-Cruz, A. Rios Rincon, Smart homes and home health monitoring technologies

for older adults: a systematic review, International Journal of Medical Informatics 91(April)(2016) 44-59.

[142] J.C. Castillo, Á. Castro-González, A. Fernández-Caballero, J.M. Latorre, J.M. Pastor, A. Fernández-Sotos, M.A. Salichs, Software architecture for smart emotion recognition and regulation of the ageing adult, Cognitive Computation 8(2)(2016) 357-367.

[143] Q. Ni, A. Belén, G. Hernando, I.P. de la Cruz, The Elderly's Independent living in smart homes: a characterization of activities and sensing infrastructure survey to facilitate services development, Sensors 15(2015) 11312-11362.

[144] M. Amiribesheli, A. Benmansour, A. Bouchachia, A review of smart homes in healthcare, Journal of Ambient Intelligence and Humanized Computing 6(4)(2015) 495-517.

[145] T. Adiono, R.V.W. Putra, M.Y. Fathany, B.L. Lawu, K. Afifah, M.H. Santriaji, S. Fuada, Rapid prototyping methodology of lightweight electronic drivers for smart home appliances, International Journal of Electrical and Computer Engineering 6(5)(2016) 2114-2124.

[146] A.-G. Paetz, E. Dütschke, W. Fichtner, Smart homes as a means to sustainable energy consumption: a study of consumer perceptions, Journal of Consumer Policy 35(1)(2012) 23-41.

[147] A. Saad al-sumaiti, M.H. Ahmed, M.M. Salama, Smart home activities: a literature review, Electric Power Components and Systems 42(3-4)(2014) 294-305.

[148] U.S. Premarathne, Reliable context-aware multi-attribute continuous authentication framework for secure energy utilization management in smart homes, Energy 93(2015) 1210-1221.