A review of soft biometrics for IoT

Igor Tomičić*, Petra Grd**, Miroslav Bača**
*Artificial Intelligence Laboratory, **Center for Forensics, Biometrics and Privacy
Faculty of Organization and Informatics
University of Zagreb
Pavlinska 2, 42000 Varaždin, Croatia
Email: (igor.tomicic, petra.grd, miroslav.baca)@foi.hr

***Abstract*— The Internet of Things (IoT) can be defined as everyday physical objects being connected to the internet and being able to identify themselves to other devices. In recent years the Internet of Things (IoT) was identified as one of the emerging technologies. Research in this area has increased considerably and future research will have to include other technologies such as biometrics to complement the development of IoT devices. The idea of this paper is to give an overview of biometric characteristics applicable to IoT with emphasis on soft biometric characteristics and possible application ideas in IoT.**

Keywords*— *biometrics, internet of things, soft biometric characteristics

I. Introduction

In recent years, the Internet of Things (IoT) has become one of the most researched and discussed topics in technology. With its wide application area it gained recognition across different fields. Researchers estimate that the IoT will consist of almost 50 billion objects by 2020 [1]. Gaikwad [1] states that "The major objectives for IoT are the creation of smart environments/spaces and self-aware things (for example: smart transport, products, cities, buildings, rural areas, energy, health, living, etc.) for climate, food, energy, mobility, digital society and health applications ".

In most of the IoT application areas, some form of person identification or classification is necessary. Henniger et al. [2] recognise two main approaches for user identification: (1) by a specific token and (2) using biometric characteristics. The main advantage of biometric characteristics is that they are bound to a person and cannot be forgotten, stolen or lost unlike passwords or tokens. Most common biometric characteristics used for person identification are hard biometric characteristics such as fingerprint, face or iris. The problems that are most frequently mentioned with usage of hard biometrics are the computational complexity and privacy. In order to circumvent those issues, soft biometrics can be used.

This paper gives an overview of soft biometric characteristics with emphasis on the characteristics which can be acquired at a distance. Advantages of using soft biometric characteristics in IoT will be described and their possible applications in IoT systems will be shown.

II. Biometrics

Biometrics can be defined as the science of recognising individuals based on their physical, behavioural, and physiological attributes such as fingerprint, face, iris, gait and voice [3]. These attributes are also known as biometric characteristics or traits. There are different ways in which these characteristics can be categorised. One such categorisation distinguishes between hard, or traditional, biometric characteristics and soft biometric characteristics. Hard biometric characteristics are those traditionally used for person identification based on their physical or behavioural features [4]. These characteristics can be divided into physical characteristics (DNA, ear, iris, retina, face, fingerprint, palm, veins, smell and body) and behavioral characteristics (gait, signature, keystroke dynamics, mouse move dynamics, voice, brain wave structure).

Soft biometric characteristics have been defined in many different ways. One of the first definitions of soft biometric was by Jain et al. [5] who defined soft biometrics as "the set of characteristics that provide some information for recognising individuals, but that are not capable of distinguishing between individuals, mainly due to their lack of distinctiveness and permanence." The most up to date and comprehensive definition of soft biometrics is by Dantcheva et al. [6]: "Soft biometric traits are physical, behavioural, or material accessories, which are associated with an individual, and which can be useful for recognising an individual. These attributes are typically gleaned from primary biometric data, are classifiable in pre-defined human understandable categories, and can be extracted in an automated manner. " Soft biometric traits can be classified in different groups. Dantcheva et al. [6] define four groups in which soft biometric traits are classified: (1) demographic, (2) anthropometric and geometric attributes, (3) medical attributes and (4) material and behavioral attributes. Demographic attributes include age, gender, ethnicity, eye color, hair color and skin color. Anthropometric and geometric attributes include body geometry and face geometry. Medical attributes are health condition, BMI, body weight and wrinkles. Material and behavioural attributes are hats, scarfs, bags, clothes, lenses, and glasses.

Application of soft biometrics has many advantages in comparison to hard biometric traits. Hard biometric traits can rarely be described using labels understood by people which only allows identification of users whose biometric signature

has been recorded previously. Soft biometric characteristics are often used by humans to describe others and therefore bridge the gap between biometric measurements and human descriptions [4]. Second great advantage of soft biometrics is non-invasiveness. Soft biometric characteristics can easily be collected at a distance [4] [7] [6] with no additional action from the subjects or their cooperation or consent. Another advantage is lower computational complexity of soft biometric characteristics. One important issue with hard biometric traits is the lack of privacy. The idea of soft biometrics most often is not to identify a person, but to identify a group a person belongs to, which means that soft biometric traits are not distinctive [6]. These advantages are the main reason why the field of soft biometrics is becoming more popular in recent years, especially for usage in smart environments.

III. The Internet of Things (IoT)

The Internet of Thing (IoT) is a heterogeneous field defined as “a variety of things or objects (...) which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbours to reach common goals” [8]. The devices referred to as "things" may include for example various kinds of sensors and actuators, mobile devices, car/vehicle computers, TV sets; but also non-ICT appliances like light bulbs, speakers, dishwashers, microwave ovens, refrigerators, electrical energy sources and building components [9], equipped with computing, communication and sensing capabilities. The ubiquitous nature of current IoT technologies can be observed through its numerous application areas, which include, but are not limited to: smart cities [10], smart power grids [11], smart health [12], smart transport [13], smart buildings [14], smart living solutions [15], smart human settlements [16], [17], [18], and other.

Within a smart living environment, there are several common application and services contexts that could utilise the identification possibilities based on soft biometrics [19]: targeted and personalised information, communication, energy management, health and care services, surveillance. Since those services may exist in a multi-user environments, security, privacy and personalization are all important factors that need to be considered. A more detailed "perspective on the background and current status of security, privacy and trust in smart environments" is overview in [20], arguing that there are many areas still not covered, such as access control, identity management, legal and socio-technical issues, and biometric aspects.

The use of biometrics within the ambient intelligence and IoT domains can be useful not only in understanding human behaviour, but also to identify the person, or class of persons with similar characteristics, so the service system could decide on their needs and desires through soft-biometric traits (height, weight, emotions, gestures, gait) [21].

The scope of the IEEE 2413 project falls within the standardisation of an Architectural Framework for the Internet of Things, encompassing for example descriptions of various IoT domains[1], depicted in Figure 1 [22].

In [23], possible IoT application domains are listed a follows: Aerospace and aviation (systems status monitoring, green operations); Automotive (systems status monitoring, V2V and V2I communication); Telecommunications; Intelligent Buildings (automatic energy metering/ home automation/ wireless monitoring); Medical Technology, Healthcare, (personal area networks, monitoring of parameters, positioning, real time location systems); Independent Living (wellness, mobility, monitoring of an aging population); Pharmaceutical; Retail, Logistics, Supply Chain Management; Manufacturing, Product Lifecycle Management (from cradle to grave); Processing industries - Oil and Gas; Safety, Security and Privacy; Environment Monitoring; People and Goods Transportation; Food traceability; Agriculture and Breeding; Media, entertainment and Ticketing; Insurance; Recycling.

IV. Literature Overview

In [19], authors illustrate problems regarding unauthorised access to data created within the smart environments, such as behavioural and heath-related information, with examples like speech-recognition, gaining insight into the residents’ whereabouts and break-in possibilities, gaining insights into another person’s medical records, etc. Considering the trade-off between biometric accuracy and usability, authors suggest the use of a number of biometric information sources (multi-biometrics) [24], where each biometrics source may be less accurate and more robust, but by fusing these different sources, the higher overall accuracy may be achieved.

Indoor localisation and fall detection are subjects of integrated ambient assisted living (AAL) solutions, where authors [25] present CapFloor, a "Flexible Capacitive Indoor Localization System". Arguing that existing solutions based on capacitive sensing systems have high installation requirements and high integration price, they propose a flexible, integrated solution based on open source hardware that consists of sensing mats capable of wirelessly transmitting data to a central platform with localization and fall detection services.

Authors in [26] propose the Internet of Biometric Things (IoBT) concept as a "cloud-centric biometric identification architecture consisting of connected devices that require biometric authentication." The proposed system couples biometric and context-aware authentication techniques in order to protect mobile applications from unauthorized access. As authors argue, biometric authentication has not been considered for IoT applications for two main reasons; 1) IoT architectures aim at automatization with no human interventions [27], 2) A number of IoT devices have limited computing capabilities, whereas hard and soft biometric identification methods include more complex calculations (decision making, identity prediction clasifiers, meta-biometric prediction classifiers [28]).

Abate et al. [29] propose Multiagent Biometrics for Ambient Intelligence (MUBAI) architecture, "which specifies the

[1]Information about IEEE 2413 project is available at: http://standards.ieee.org/develop/project/2413.html

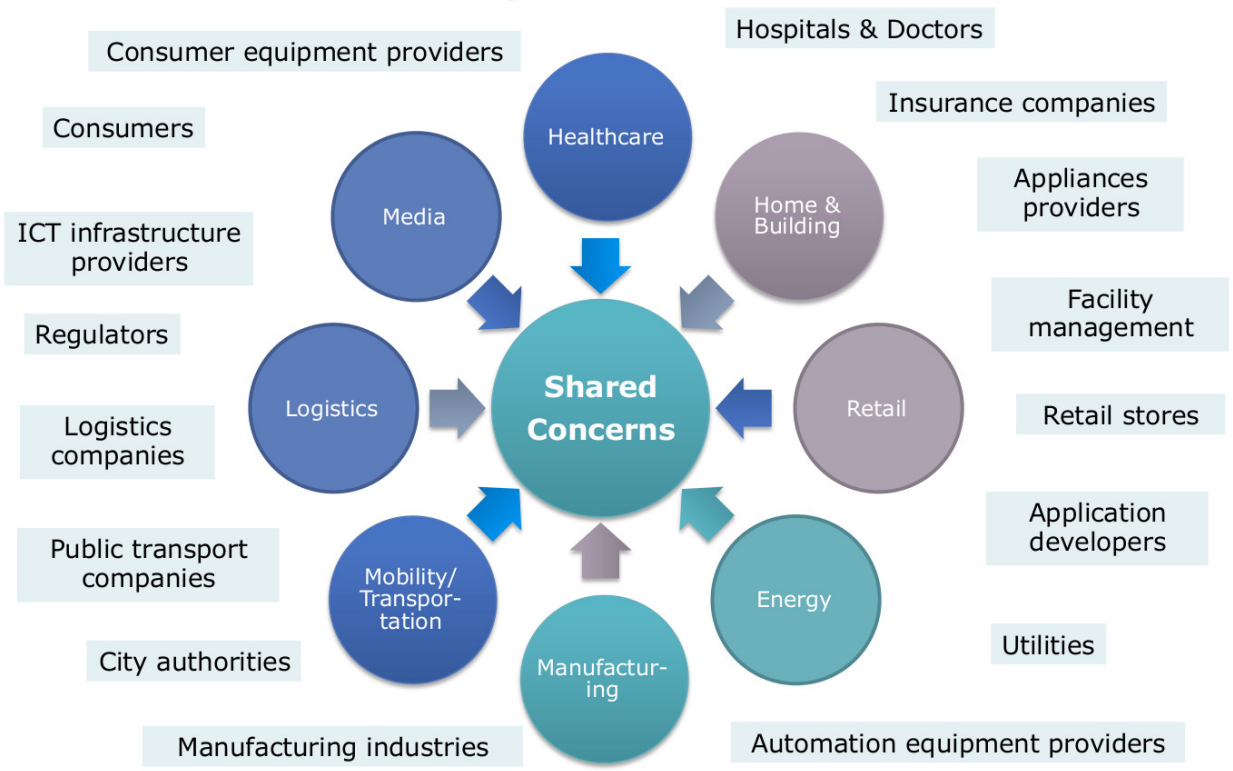

Fig. 1: Selected domains and staheholders in IoT [22]

composition of more biometric modules in a multiagent recognition system.", arguing that MUBAI architecture allows to achieve better results in comparison to single classifiers.

The biometric technology is also used in IoT context in [30], where authors propose an IoT based biometrics architecture that can be used for security and access control mechanisms and claim that the "system can be applied at all places where authentication is required". The biometric system involved is a multimodal one, with face and fingerprint traits under consideration.

The potential of biometric technologies within the general domain of ambient intelligence is analysed in [31], along with the effort to identify "some key technological issues which may respond to privacy concerns". Moreover, the authors tackle the usefulness of soft biometrics where, for example, facial expressions can be used to better relate the user with the surrounding environment, providing the input for the system enabling services, but with the clear advantage of not compromising user's privacy.

Using biometric data as a source for randomness is discussed in [32]. Authors assess the feasibility of using IoT devices to gather biometric data on human behaviour by using several smartphone sensors: magnetometer, gyroscope, rotation, accelerometer, gravity, linear acceleration and sound. The results showed that using one single sensor source is not adequate for creating randomness used in cryptographic applications, nor is the subject's gait, which would be better utilized in identifying the person.

Shahim et al. [33] propose a system that would use Raspberry Pi as an IoT device together with the leap motion controller in an attempt to authenticate system users through hand geometry and a series of gestures. User classification would be achieved through the machine learning classification techniques. Authors also suggest an application scenario, where medical surgeons would gain "access to an operating theatre once they have disinfected their hands and would not like to touch any surfaces before entering." Surgeons would thereby gesture towards the authentication system, which would grant or deny the access accordingly.

An intelligent add-on for the smart devices, which would enable continuous verification of users in a Social Internet of Things, is proposed in [34]. Authors have collected online behaviometrics of mobile users by extracting features from smartphone sensors and users' social network interactions. The results showed that "genuine users can be verified without any disruption 97% of the time whereas the users can keep using the devices 90% of the time without any disruption".

V. Soft biometric characteristics applicable to IoT domain

If we put biometric characteristics in the context of IoT application areas, biometric sensors and their distance from users play an important role. Tistarelli and Schouten [35] recognise that there are three categories of biometric sensing modalities: (1) contact, (2) contact-less and (3) at a distance. In using contact biometric devices users are required to touch the

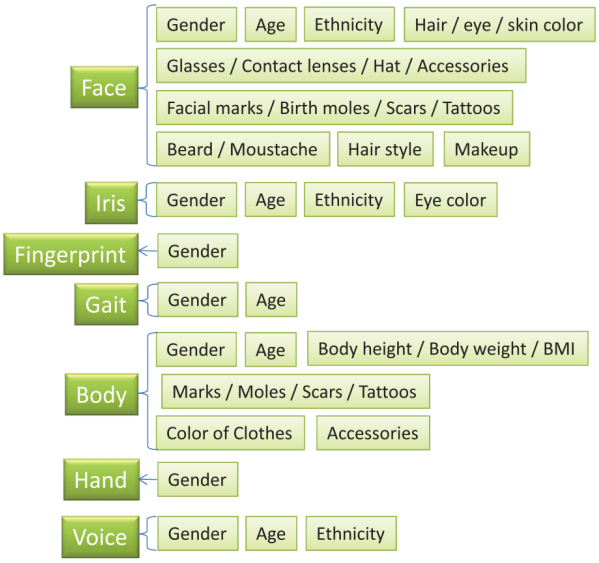

Fig. 2: Soft biometric information and biometric characteristics from which they can be acquired [6]

sensor, which is not the case in contact-less and at a distance biometric acquisition. The difference between contact-less and at a distance sensors is that in the former the distance between the user and the sensor is short. Sensors capable of biometric data acquisition at a distance do not require special actions from users. Biometric characteristics able to be acquired from at a distance sensors are particularly interesting in smart environment scenarios [35].

Dantcheva et al. [6] give a list of the soft biometric information which can be acquired from different biometric modalities (Figure 2). If only biometric modalities which can be acquired from at a distance sensors are taken into consideration, some of the modalities can be eliminated. Modalities appropriate for usage with at a distance sensors most commonly used in IoT are face, gait and body. As soft biometric information can be acquired from different biometric modalities, this elimination does not reduce the soft biometric information acquired (for example, gender information can be acquired from all of the previously mentioned biometric modalities).

As summarised within Table I, soft biometrics could be applied within several IoT domains. A smart home system can track resident's movements in order to conserve energy within rooms that are not currently occupied (switching off the lights, appliances, reducing ambient temperatures, etc.); if detecting that the resident is sleeping, it could lower the ambient temperature by a few degrees. The system could observe resident's body and face for signs of health-related symptoms and states, alerting the resident and/or health workers if deemed necessary. It could track resident's weight and BMI on daily basis, and offer diet and/or recreation activity advice accordingly. The system might detect home intruders by detecting unusual biometric traits, and alert authorities. It could also detect children and not allow them to open doors.

Within the Media domain, age, gender, ethnicity could present relevant factors in tailoring the customized channels, articles, news feeds, etc. Health related issues and emergencies could be discovered or anticipated based on person's age, gender, skin color or heartbeat, preventing possibly undesirable outcomes. Wearable devices, cameras, or other connected IoT devices equipped with appropriate sensors, could generate sufficient input for biometric systems.

Driving restrictions could be initiated on the basis of detected alcohol intoxication and/or insufficient age of the driver. The IoT system within the vehicle could respond to driver's voice commands, but also analyse the voice in order to detect possible risk situations (tiredness, intoxication, etc.).

Threat assessment could be performed by numerous IoT devices on airports, based on soft-biometric traits. Retail industry could offer customised shopping experiences and tailored product suggestions, but also perform long-term analysis of customer demographics and in-store behaviours. Soft biometrics' approach could also help in identifying potential shoplifters.

VI. Conclusion & Future Work

Although the currently available body of research shows a certain amount of work dealing with biometrics applications within the Internet of Things context, presented in Section IV, there are only a number of references for using soft biometrics within the IoT context.

In this paper, we summarized the state of the art in research concerning the application of biometrics within the relevant Internet of Things domains, focusing on soft biometric traits and their possible application scenarios. We have purposefully discarded some of the IoT domains that we've found to be unfeasible for soft-biometrics approaches, for example, domains which are not user-centric, or where there are no relevant human-computer interactions.

Our future work will progress on the non-intrusive soft-biometrics approach within the Internet of Things context, with special focus on the model development and specific technologies required to implement scenarios (included, but not limited to) discussed within this paper.

After the introductory section I we have introduced the biometrics concept in section II, with special focus on soft biometric characteristics, associated traits and its advantages in comparison to hard biometric approaches. Internet of Things concept was discussed in section III, where possible application domains for the use of soft biometrics were derived from related work. Section IV presented the state of the art research concerning the usage of biometrics in the Internet of Things application domains.

Acknowledgment

This work has been supported in full by the Croatian Science Foundation under the project number 3877.

IoT AD	Soft biometric information	Usage scenario
Home and Building	emotions	ambiental adjustments
	glasses, contact lenses, age, presence	localization; energy conservation; ambiental adjustments
	weight, height, BMI	diet recommendations
	age, gender	intruder detection; physical access control
Media	age, gender, ethnicity	customized media delivery
	age, gender, ethnicity	thematic group recommendations
Energy	glasses, contact lenses, age, scars	energy usage optimisation; demand side management ambient temperature adjustments
Healthcare	age, gender, skin color, heartbeat	medical emergency detection; body statistics; health recommendation systems
Mobility transportation	substance abuse, emotions, age	driving restrictions
	accessories, ethnicity, emotions	threat assessment
	substance abuse, emotions	vehicle voice commands
Retail	height, weight, gender, age, clothes, accessories	customised shopping experience, tailored product suggestions, customer demographics, in-store behaviours, potential perpetrator detection

TABLE I: Proposed soft biometrics within relevant IoT domains

REFERENCES

[1] R. Gaikwad, "Internet of things (iot): Revolution of internet for smart environment," Oracle, Tech. Rep., 2016.

[2] O. Henniger, N. Damer, and A. Braun, "Opportunities for biometric technologies in smart environments," *AmI 2017*, pp. 175–182, 2017.

[3] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of Biometrics*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2007.

[4] D. A. Reid and M. S. Nixon, "Using comparative human descriptions for soft biometrics," in *Biometrics (IJCB), 2011 International Joint Conference on*. IEEE, 2011.

[5] A. K. Jain, S. C. Dass, and K. Nandakumar, "Can soft biometric traits assist user recognition?" vol. 5404, 2004, pp. 5404 – 5404 – 12.

[6] A. Dantcheva, P. Elia, and A. Ross, "What else does your biometric data reveal? a survey on soft biometrics," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 3, 2016.

[7] D. A. Reid, M. S. Nixon, and S. V. Stevenage, "Soft biometrics; human identification using comparative descriptions," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 36, no. 6, 2014.

[8] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[9] Z. Hu, S. Frénot, B. Tourancheau, and G. Privat, "Iterative model-based identification of building components and appliances by means of sensor-actuator networks," 2011.

[10] P. Vlacheas, R. Giaffreda, V. Stavroulaki, D. Kelaidonis, V. Foteinos, G. Poulios, P. Demestichas, A. Somov, A. R. Biswas, and K. Moessner, "Enabling smart cities through a cognitive management framework for the internet of things," *IEEE communications magazine*, vol. 51, no. 6, pp. 102–111, 2013.

[11] 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*. IEEE, 2010, pp. 69–72.

[12] 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*. ACM, 2011, p. 131.

[13] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer *et al.*, "Internet of things strategic research roadmap," *Internet of Things-Global Technological and Societal Trends*, vol. 1, no. 2011, pp. 9–52, 2011.

[14] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, and G. Borriello, "Building the internet of things using rfid: the rfid ecosystem experience," *IEEE Internet computing*, vol. 13, no. 3, 2009.

[15] 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*. Ieee, 2010, pp. 804–809.

[16] I. Tomičić and M. Schatten, "Agent-based framework for modeling and simulation of resources in self-sustainable human settlements: a case study on water management in an eco-village community in croatia," *International Journal of Sustainable Development & World Ecology*, vol. 23, no. 6, pp. 504–513, 2016.

[17] ——, "A case study on renewable energy management in an eco-village community in croatia–an agent based approach," *International journal of renewable energy research*, vol. 6, no. 4, pp. 1307–1317, 2016.

[18] I. Tomičić, "Agent-based framework for modelling and simulation of resource management in smart self-sustainable human settlements," Ph.D. dissertation, Fakultet organizacije i informatike, Sveučilište u Zagrebu, 2016.

[19] O. Henniger, N. Damer, and A. Braun, "Opportunities for biometric technologies in smart environments," in *European Conference on Ambient Intelligence*. Springer, 2017, pp. 175–182.

[20] P. Nixon, W. Wagealla, C. English, and S. Terzis, "Security, privacy, and trust issues in smart environments," 2005.

[21] V. Piuri, "Biometric technologies for ambient intelligence in the internet of things," in *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*. IEEE, 2013, pp. lxxi–lxxii.

[22] O. Logvinov, B. Kraemer, C. Adams, J. Heiles, G. Stuebing, M. Nielsen, and B. Mancuso, "Standard for an architectural framework for the internet of things (iot) ieee p2413," Tech. Rep. September, Tech. Rep., 2016.

[23] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, "Vision and challenges for realising the internet of things," *Cluster of European Research Projects on the Internet of Things, European Commision*, vol. 3, no. 3, pp. 34–36, 2010.

[24] N. Damer, A. Opel, A. Shahverdyan, M. Marsico, and A. Fred, "An overview on multi-biometric score-level fusion-verification and identification." in *ICPRAM*, 2013, pp. 647–653.

[25] A. Braun, H. Heggen, and R. Wichert, "Capfloor–a flexible capacitive indoor localization system," in *International Competition on Evaluating AAL Systems through Competitive Benchmarking*. Springer, 2011, pp. 26–35.

[26] B. Kantarci, M. Erol-Kantarci, and S. Schuckers, "Towards secure cloud-centric internet of biometric things," in *Cloud Networking (CloudNet), 2015 IEEE 4th International Conference on*. IEEE, 2015, pp. 81–83.

[27] S. Cirani, L. Davoli, G. Ferrari, R. Léone, P. Medagliani, M. Picone, and L. Veltri, "A scalable and self-configuring architecture for service discovery in the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 508–521, 2014.

[28] M. C. D. C. Abreu and M. Fairhurst, "Enhancing identity prediction using a novel approach to combining hard-and soft-biometric information," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 41, no. 5, pp. 599–607, 2011.

[29] A. F. Abate, M. De Marsico, D. Riccio, and G. Tortora, "Mubai: multiagent biometrics for ambient intelligence," *Journal of Ambient Intelligence and Humanized Computing*, vol. 2, no. 2, pp. 81–89, 2011.

[30] D. Shah *et al.*, "Iot based biometrics implementation on raspberry pi," *Procedia Computer Science*, vol. 79, pp. 328–336, 2016.
[31] M. Tistarelli and B. Schouten, "Biometrics in ambient intelligence," *Journal of Ambient Intelligence and Humanized Computing*, vol. 2, no. 2, pp. 113–126, 2011.
[32] L. M. Dinca and G. Hancke, "Behavioural sensor data as randomness source for iot devices," in *Industrial Electronics (ISIE), 2017 IEEE 26th International Symposium on*. IEEE, 2017, pp. 2038–2043.
[33] L.-P. Shahim, D. Snyman, T. du Toit, and H. Kruger, "Cost-effective biometric authentication using leap motion and iot devices."
[34] F. Anjomshoa, M. Aloqaily, B. Kantarci, M. Erol-Kantarci, and S. Schuckers, "Social behaviometrics for personalized devices in the internet of things era," *IEEE Access*, vol. 5, pp. 12 199–12 213, 2017.
[35] M. Tistarelli and B. Schouten, "Biometrics in ambient intelligence," *Journal of Ambient Intelligence and Humanized Computing*, vol. 2, no. 2, pp. 113–126, 2011.