Opportunities for Biometric Technologies in Smart Environments

Olaf Henniger(✉), Naser Damer, and Andreas Braun

Fraunhofer Institute for Computer Graphics Research IGD, Darmstadt, Germany
olaf.henniger@igd.fraunhofer.de

Abstract. Smart environments describe spaces that are equipped with sensors, computing facilities and output systems that aim at providing their inhabitants with targeted services and supporting them in their tasks. Increasingly these are faced with challenges in differentiating multiple users and secure authentication. This paper outlines how biometric technologies can be applied in smart environments to overcome these challenges. We give an introduction to these domains and show various applications that can benefit from the combination of biometrics and smart environments.

Keywords: Smart environment · Biometrics · Multi-biometrics

1 Introduction

Smart environments use a multitude of information-processing methods and technologies to support their inhabitants in daily activities [3]. The basis for most applications are sensors and actuators that are placed in the environment or worn by the user. The purpose of the sensors is to analyse the current situation of the user in the environment – the context [15]. The most common example of a smart environment is the smart home where the system is used to track inhabitants, optimise energy usage, and provide multimedia or comfort functions. However, the concept can be extended to numerous environments, including museums, offices, shopping centers, or cars [3].

Many applications that are built for these context-aware systems are primarily aimed towards single users, with data processing methods that are optimised for this use case and the proliferation of single-user input and output channels. The market for smart homes has been increasing considerably in the past five years, leading to a proliferation of smart environments in multi-user scenarios. Often the systems circumvent the multi-user challenges by simply restricting the automated acquisition of contexts [14].

Within smart environments, the access to certain types of personal data should be restricted to authorised users. This is particularly relevant for health related information, e.g. gathered by devices that remotely measure physiological parameters. In the past few years research into distinguishing multiple users in smart environments and managing their individual contexts in parallel has

A. Braun et al. (Eds.): AmI 2017, LNCS 10217, pp. 175–182, 2017.
DOI: 10.1007/978-3-319-56997-0_14

become more active [4]. The two main approaches are user identification by a specific token or using biometric characteristics.

The strength of biometrics compared to tokens is that biometric characteristics are strongly bound to a person and cannot easily be forgotten or passed on to other people, be it intentionally or unintentionally. Biometrics enables the automated recognition of humans based on their biological or behavioural characteristics. This requires the detection of features that are discriminative for each person and make them recognisable. Some common methods are fingerprint, iris, and face recognition.

A variety of soft biometrics does not attempt to associate the detected biometric features to an individual person, but instead to groups of people, e.g. by detecting age, gender, or group-specific body parameters. This is sufficient for many applications, including several scenarios in smart environments. The multi-user challenge is a typical showcase for the use of soft biometrics, as it provides the opportunity for temporary assignment of user information.

In this paper, we discuss how biometric technologies can be used to provide solutions for the presented challenges that occur in smart environments. In Sect. 2 we give an overview of smart environments. In Sect. 3 we discuss user authentication needs in smart environments. In Sect. 4 we give an overview of biometric technologies that could be applied in smart environments. Section 5 summarises the results and gives an outlook.

2 Overview of Smart Environments

The notion of environments becoming smarter with the aid of information technologies has been a vision for several decades. In a famous article, Mark Weiser established the notion of Ubiquitous Computing where computational resources are invisibly placed in the environment and the computer is reduced to its input and output channel [17]. He envisioned devices similar to today's smartphones and tablets.

Figure 1 shows components hidden in a smart living environment. Early in smart environment research, the notion of platforms has become important. They are software components that manage communication between all devices and enable the creation of domain-specific rules [8]. Due to the heterogeneity of the components involved, they are often service-oriented, semantic platforms that provide a high level of abstraction such as the universAAL platform [7].

All components shown in Fig. 1 benefit from the continuing trend for embedded systems. Computing devices are becoming smaller and more efficient, which enables more advanced computing methods to be used, even on very small devices. Sensing units have become smaller and less energy-consuming over time. They may rely on MEMSs (micro electro-mechanical systems), very small mechanical systems that can be integrated on chips. Thus numerous sensors can be placed on a single chip, reducing cost and making them less obtrusive. Actuators may be all forms of devices that can express an output. They range from the switch that turns on the light, motors that move the blinds, to screens and audio systems, which have also become smaller, using embedded systems.

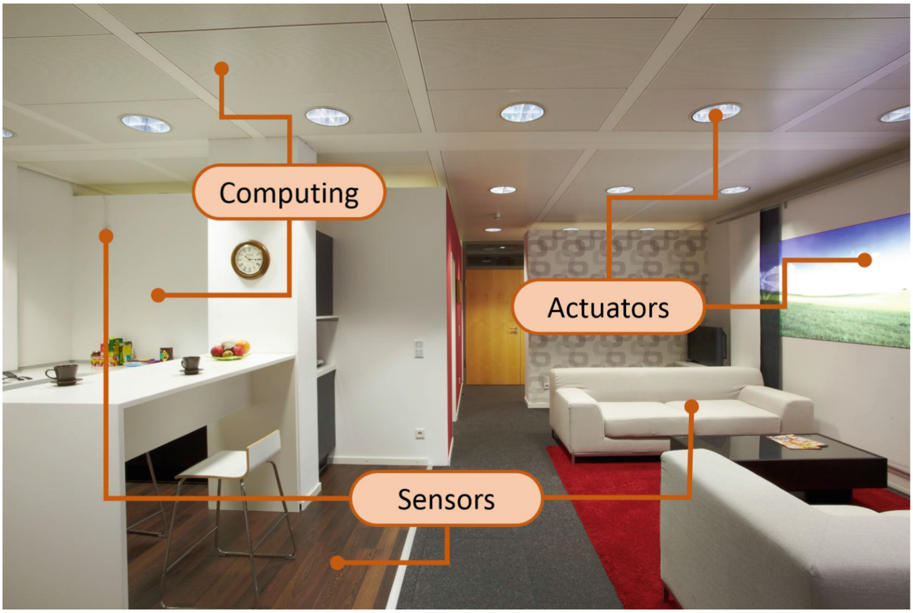

Fig. 1. Example of smart environment and hidden components

So far, most sensing systems do not fulfill the requirement stated by Weiser that they should be unobtrusive and ubiquitous. For example, cameras are powerful and well-suited for public environments, but there is a perceived lack of privacy in the private domain and they are difficult to hide from view. Therefore, recently, entirely invisible sensing systems have become an area of research. Such systems can be put into practice using e.g. capacitive sensing technology, which uses weak electric fields that are disturbed by human bodies moving through. They can be hidden behind any non-conductive material, making them suitable for invisible sensing in smart environments [2].

3 User Authentication Needs in Smart Environments

3.1 Overview

After introducing the technical prerequisites in the previous section, we want to briefly introduce common applications and services that are provided in a smart living environment:

- Information – the inhabitants get targeted and personalised information items, either from general sources, such as news sites on the web, or from personal sources including calendars, emails, and notifications,
- Communication – there are numerous communication services provided, ranging from classic phone systems to video systems in the living room, or telepresence systems, e.g. by special-purpose robots,

- Energy saving – sensor systems detect presence and location and are able to turn off non-essential systems, e.g. lighting and heating,
- Health and care services – health information can be collected by environmental sensors that are connected to the smart environment platform. In addition there can be communication facilities to medical or care personnel, or smart alerts if dangerous situations are recognised,
- Remote configuration, surveillance, and control – smart environments may be configured, monitored, and controlled remotely over the Internet.

Important factors for all of those services are personalisation and data security. As soon as multiple users are present in the environment, the systems need to know from which person they are currently collecting data and to whom they shall provide personalised services. The sensors are able to detect a very fine-grained image of the users' behaviour and eventually medically relevant information. Here it is important to protect the data from any outside access, but in addition also from unauthorised access by other user's in the environment. If the access shall be provided comfortably and seamlessly, smart authentication technologies have to be used.

3.2 Multi-user Challenge

So far, most smart environments have been developed with a focus on a single user. Research into multiple users has been performed for the past few years [14].

The presence of multiple users changes the behaviour of the environment, resulting in the adaptation of scenarios. For example, the smart environment should not turn off the lighting for energy saving as long as there is still another person in the room, and a smart bathroom mirror should only present the news relevant to the user that is currently in front of the mirror. We can distinguish the following classes of scenarios:

- Personalised content presentation,
- Deactivating single-user environment rules,
- Adaptation of sensing and reasoning.

Particularly, the adaptation of sensing and reasoning is an ongoing research topic [13]. Many typical sensing systems cannot inherently distinguish between several people. Therefore, it is necessary to combine multiple sources of information, using multi-sensor fusion.

3.3 Data Security and Continuous Authentication

Data security is an inherent challenge in smart environments [10]. The data that is created has to be protected against unauthorised access from the outside in order to protect behavioural and health-related information from being abused. Speech-recording objects that transmit all recordings by default to the cloud for the purpose of speech recognition[1] are a daunting example. Another example: By remotely accessing the information stored in the smart environment, an attacker could find out times of absence that would be suitable for a break-in or tell the smart environment to unlock doors and open windows for easier access.

Within the smart environment similar issues may occur. Person B may see medical information acquired from Person A or get detailed information about their behaviour or that of potential visitors. Authentication methods can be used to prevent this access, e.g. face recognition methods [11]. The authentication systems should support continuous authentication, for increased user acceptance, while being reliable.

4 Overview of Biometric Technologies

4.1 Biometric Characteristics

Some biometric characteristics are visible or measurable even without the active cooperation of the person. Such characteristics are called static biometric characteristics. Examples of static biometric characteristics include: Fingerprints, face, hand geometry, iris, and vein patterns. In practice, even capturing static biometric characteristics may be an obtrusive process: People have to present their characteristics to a biometric sensor or to remain in a certain pose for a while. The need to simplify and expedite the acquisition of biometric samples has led to the development of innovative biometric sensors (originally targeted at border control applications) including iris-at-a-distance systems and contactless fingerprint systems capturing fingerprints on the fly [16].

In contrast to static biometric characteristics, behavioural characteristics require an action from the person. Examples of behavioural biometric characteristics include: Voice, signature dynamics, keystroke dynamics, and gait.

4.2 Multi-biometrics

The nature of smart environment solutions requires the integration of automatic recognition solutions without jeopardising the overall usability. Ideally, such a biometric system should not require any special actions from the users. However, achieving both, high recognition accuracy and usability have always been a challenge to biometric technologies. An accurate biometric recognition requires limitations such as a specific biometric capture position, strict environment conditions (e.g. illumination), and the collaboration of the users. This trade-off between accuracy and usability/robustness can be eliminated by considering a number of biometric information sources within a smart information fusion approach [5].

[1] http://www.commercialfreechildhood.org/child-advocates-mobilize-stop-mattels-eavesdropping-hello-barbie.

Having more information sources allows each source to be less accurate and thus less sensitive to the environment conditions. Fusing the information provided by these different sources allows to achieve the required high level of accuracy. Most importantly, it allows the biometric system to be operated unobtrusively without requiring special actions from the users. The different biometric sources can be based on different characteristics, captures, algorithms, sensors, or instances.

4.3 Generic Biometric System

Figure 2 illustrates the general model of a biometric system: Biometric samples are acquired from a subject via a biometric capture device (sensor) and sent to a signal processing subsystem in order to extract distinctive, repeatable biometric features. The storage subsystem stores the resulting features or the captured biometric sample in a biometric enrolment database as a biometric reference. The comparison subsystem compares the features extracted from a probe biometric sample with references from the enrolment database to determine whether they match. A distinction is drawn between biometric verification – one-to-one comparison of biometric feature sets to confirm the claimed identity – and biometric identification – one-to-N comparison of biometric feature sets to identify a person among several persons registered in a database. The decision subsystem returns a decision regarding acceptance or rejection of the probe based upon the similarity between the features of probe and reference.

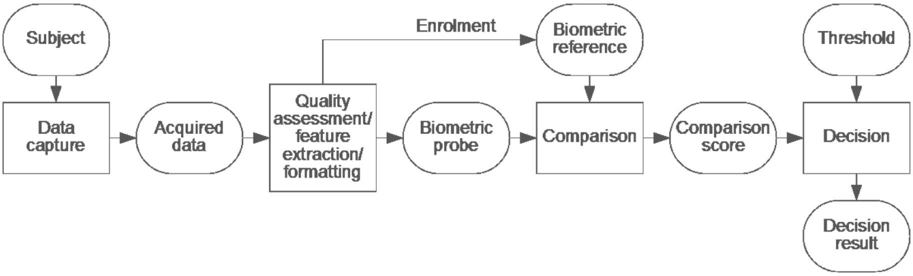

Fig. 2. Generic biometric system

Possible biometric authentication architectures differ in the locations where biometric reference data is stored and where the biometric comparison is carried out: a server, a client, a mobile device, or a security token such as a smart card. Possible architectures for biometric systems include [9]:

- Store on server, compare on server,
- Store on client, compare on client,
- Store on device, compare on device,
- Store on token, compare on server,

- Store on token, compare on device, and
- Store on token, compare on token.

For local authentication in a smart environment, the store-on-server compare-on-server architecture would be appropriate because it allows users to be authenticated anywhere in the environment where biometric sensors are available.

For biometric authentication of a user of a mobile device for remote access to a smart environment, the store-on-device compare-on-device architecture would be appropriate. The FIDO (Fast Identity Online) Alliance has specified a set of mechanisms for using local device authentication, including biometric store-on-device compare-on-device authentication, for secure online authentication [6].

4.4 Security and Usability Requirements and Recommendations

Biometric systems are threatened by attacks on several points: In particular, they may be attacked on the sensors by presenting a biometric look-alike or fake biometric characteristics. An impostor could also try to send recorded or otherwise acquired biometric data to the comparison component, evading the regular data capture device. Another possible point of attack is the data storage containing biometric references and thresholds, which should not be readable or alterable by attackers. Like any information technology system, biometric systems must be sufficiently protected against malicious attacks [12].

More clearly visible biometric characteristics that may be used in a smart living environment such as face, ear, or gait are more prone to presentation attacks (spoofing) as they can be easily captured by attackers. Such attacks can be detected using a presentation attack detection component. Using multi-biometrics makes the biometric system less vulnerable to presentations attacks as it is harder for attackers to collect and mimic a larger number of biometric characteristics simultaneously.

5 Conclusions

We have given an introduction on challenges in smart environments and how biometric technologies can provide solutions. In future applications in this domain the need for supporting multi-user scenarios will become more apparent. The growing number of sensors, particularly in the monitoring of vital signs leads to additional concerns regarding data security and reliable authentication within the smart environments. However, these sensors can be of use for multi-biometric applications, by providing additional features that can be used in the authentication process.

In the future we want to exploit these technologies, e.g. by inclusion of environmental and behavioural information into multi-biometric systems. A candidate are smart floors that provide localisation and potential gait information [1]. The usability of biometric systems in smart environments is to be evaluated. We want to evaluate the user acceptance of various biometric systems in several smart environment pilot sites.

References

1. Braun, A., Heggen, H., Wichert, R.: CapFloor – a flexible capacitive indoor localization system. In: Chessa, S., Knauth, S. (eds.) EvAAL 2011. CCIS, vol. 309, pp. 26–35. Springer, Heidelberg (2012). doi:10.1007/978-3-642-33533-4_3
2. Braun, A., Wichert, R., Kuijper, A., Fellner, D.W.: Capacitive proximity sensing in smart environments. J. Ambient Intell. Smart Environ. **7**(4), 1–28 (2015)
3. Cook, D., Das, S.: Smart Environments: Technology, Protocols and Applications, vol. 43. Wiley, Hoboken (2004)
4. Cook, D.J., Das, S.K.: How smart are our environments? An updated look at the state of the art. Pervasive Mob. Comput. **3**(2), 53–73 (2007)
5. Damer, N., Opel, A., Shahverdyan, A.: An overview on multi-biometric score-level fusion - verification and identification. In: Marsico, M.D., Fred, A.L.N. (eds.) ICPRAM, pp. 647–653. SCITEPRESS, Setúbal (2013)
6. UAF (universal authentication framework) architectural overview. FIDO Alliance Implementation Draft fido-uaf-v1.1-id-20170202 (2017). http://fidoalliance.org
7. Hanke, S., Mayer, C., Hoeftberger, O., Boos, H., Wichert, R., Tazari, M.R., Wolf, P., Furfari, F.: universAAL - an open and consolidated AAL platform. In: Wichert, R., Eberhardt, B. (eds.) Ambient Assisted Living, pp. 127–140. Springer, Heidelberg (2011). http://www.springerlink.com/content/g5k52x925r198q76/
8. Helal, S., Mann, W., El-Zabadani, H., King, J., Kaddoura, Y., Jansen, E.: The Gator Tech smart house: a programmable pervasive space. Computer **38**(3), 50–60 (2005)
9. Study report on biometrics in e-authentication. INCITS M1/07-0185rev, version 1.0 (2007)
10. Nixon, P.A., Wagealla, W., English, C., Terzis, S.: Security, privacy and trust issues in smart environments. In: Smart Environments: Technologies, Protocols, and Applications, pp. 249–270 (2005)
11. Pentland, A., Choudhury, T.: Face recognition for smart environments. Computer **33**(2), 50–55 (2000)
12. Ratha, N., Connell, J., Bolle, R.: Enhancing security and privacy in biometrics-based authentication system. IBM Syst. J. **40**, 614–634 (2001)
13. Roy, N., Misra, A., Cook, D.: Ambient and smartphone sensor assisted ADL recognition in multi-inhabitant smart environments. J. Ambient Intell. Hum. Comput. **7**, 1–19 (2016)
14. Roy, N., Roy, A., Das, S.K.: Context-aware resource management in multi-inhabitant smart homes: a Nash H-learning based approach. In: Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications, PERCOM 2006, pp. 148–158 (2006). http://dx.doi.org/10.1109/PERCOM.2006.18
15. Schilit, B., Adams, N., Want, R.: Context-aware computing applications. In: Proceedings Workshop on Mobile Computing Systems and Applications, pp. 85–90. IEEE (1994)
16. Tistarelli, M., Li, S.Z., Chellappa, R. (eds.): Handbook of Remote Biometrics for Surveillance and Security. Springer, Heidelberg (2009)
17. Weiser, M.: The computer for the 21st century. Sci. Am. **265**(3), 94–104 (1991). http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html