Walking on the Cloud: Gait Recognition, a Wearable Solution

Aniello Castiglione[1], Kim-Kwang Raymond Choo[2], Maria De Marsico[3](✉), and Alessio Mecca[3]

[1] University of Salerno, Salerno, Italy
[2] The University of Texas at San Antonio, San Antonio, TX 78249, USA
[3] Sapienza University of Rome, Rome, Italy
demarsico@di.uniroma1.it

Abstract. Biometrics and cloud computing are converging towards a common application context aiming at deploying biometric authentication as a remote service (Biometrics as a Service - BaaS). The advantages for the final user is to be relieved from the burden related to acquire/maintain specific software, and to gain the ability of building personalized applications where biometric services can be embedded through suitable cloud APIs. Gait is one of the promising biometric traits that can be investigated in this scenario. In particular, this paper deals with the processing techniques based on wearable sensors, e.g., accelerometers. These sensors are nowadays ubiquitous in mobile devices, and allow the acquisition of lightweight signals that can be sent remotely for processing. As an example of possible applications, a positive recognition may automatically allow access to restricted zones without an explicit action by the user, that has just to approach the entrance walking normally.

Keywords: Gait recognition · Wearable sensors · Cloud services Biometrics as a Service · BaaS

1 Introduction

Modern mobile devices are not only ubiquitous, but also embed an increasing number of sensors. The original aim of those sensors is, basically, to provide an increasingly "natural" interaction (e.g., triggering functions just by shacking the device), and advanced features (e.g., sending directly a captured image). Thanks to them, the equipped smartphones, tablets and wearables can further lend themselves to unanticipated uses. It is worth noticing that the variety of tasks that are performed nowadays trough them, especially for some user groups, often overcomes the use of traditional desktop computers. However, for some specific applications, either storage or computational capabilities may still be not sufficient. This is the typical, if not main, context where cloud computing may represent an effective and efficient solution. Among the mobile applications gaining popularity, biometric authentication is one that can take significant advantage from the mobile+cloud architectural schema. The biometric community

M. H. Au et al. (Eds.): NSS 2018, LNCS 11058, pp. 174–186, 2018.
https://doi.org/10.1007/978-3-030-02744-5_13

usually classifies the biometric traits into two main categories, namely hard and soft. The hard ones better meet the conditions for a sufficient accuracy and reliability of subject recognition, e.g., universality, uniqueness, permanence, and ubiquitousness [19]. Popular examples, which are consolidated also in everyday practice, are face, fingerprint, and iris. Hard traits are basically static ones, i.e., bound to subject appearance and physical features. Thanks to good levels of discriminating power and permanence they can achieve good performance in terms of accurate recognition, especially in controlled conditions. However their strict relation to physical/appearance features makes systems based on "strong" traits suffer from the problems that typically affect pattern recognition based on visual characteristics, and that are caused by uneven illumination, different orientation with respect to a capture device, special trait configurations (e.g., expression in face). Moreover, just because they are "visible", they are easier to "copy" and are subject to spoofing. As a consequence, for those traits it is especially important to verify the liveness of the presented sample, in order to distinguish a real user from a photo or a video used for a presentation attack.

The biometric traits classified as soft, instead, lack to meet one or more of the required conditions mentioned above. Nevertheless, they can be useful at least to delimit specific classes of persons, and to reduce the search space in recognition operations. Some examples are represented by either physical traits bound to subject (static) appearance, e.g., face shape, height, skin or hair color, or demographic features (gender, age, ethnicity), that can be in turn inferred from physical appearance and identify groups of subjects rather than a single one. Several traits in the "soft" category are related to subject behavior instead: gait time progression, dynamics of signature, writing behavior in general, and keystroke dynamics are only some examples. The idea underlying the use of these traits to identify people is that, while humans are not very good at remembering passwords, they are quite good at simply being (and behaving as) themselves. But the same traits can be affected by behavioral as well as emotional factors, so that they may lack permanence. Moreover, they may still lack a completely reliable/accurate processing. Notwithstanding their limitations, those traits can be used in controlled conditions, or can further enforce recognition accuracy of strong ones. In addition, they are more difficult to forge and/or replicate.

This contribution deals with gait recognition, which is included among soft biometrics. There are different approaches tackling this problem, that can be divided into three classes. The earliest ones used for user recognition rely on machine vision-based techniques, that exploit visual models for both the static and dynamic aspects of the gait pattern of a subject. Gait analysis for medical applications traditionally exploits floor sensors-based techniques, that capture features of subject gait through special sensors equipping an ambient floor, e.g., pressure and/or weight sensors. Finally, wearable sensors-based techniques move sensors from the ambient to the subject body, therefore achieving an ubiquitous recognition ability. This latter class of techniques is the object of the present proposal. While verification (1:1 matching with a claimed identity) might be carried out locally, both security and privacy issues claim for a remote processing when identification (1:N matching) is requested. Moreover, the possible application of wearable sensor-based gait recognition as a cloud-related service is investigated, sketching a possible architecture. In fact, cloud computing offers an efficient storage/processing infrastructure to exploit mobile user authentication also with large scale populations.

2 Wearable Sensors: A Possible Solution for Gait Recognition?

The errors of a biometric recognition system occur either when a subject is confused with another due to inter-personal similarities, or when a subject is not recognized due to intra-personal differences. Both problems are related to the discriminative power of adopted traits and related approaches. In addition, both intrinsic and external variations can modify the appearance or, more generally, the characteristics of a biometric trait. This holds at a different level for hard and soft biometrics. For example, A-PIE variations (age, pose, illumination, and expression) affect face recognition. Gait is not an exception in the biometric scenario. Walking speed is the main factor affecting gait dynamics, but also the kind of shoes (e.g., heels for women shoes, or heavy working shoes [17,18]), the irregular ground slope, and also some temporary illness (e.g., leg contusions or other problems related to articulation or feet) can cause variations of the individual gait pattern. Gait recognition techniques that are based on processing silhouettes extracted from video sequences, can further suffer from common image processing problems, e.g., illumination, occlusion or self-occlusion, pose, and perspective with respect to the camera. The last two raise similar issues, but the first one is intrinsic to the user while the second is an extrinsic factor acting notwithstanding the user absolute position. Finally, clothes and carried objects can also affect the reliable extraction of silhouette features. In practice, each class of approaches may present specific problems, besides those that characterize this biometric trait (see Fig. 1). Gait recognition also presents some positive aspects. As for the other behavioral traits, it is quite difficult to copy or forge a gait pattern. In approaches based on machine vision, it can be carried out at a distance of 10 m or more, therefore the user is not necessarily aware of the recognition. In wearable sensor-based approaches distance is not a problem since the acquisition devices are located on user body, and in this case the user is usually cooperative. Floor sensor-based approaches are a special case, since the acquisition devices are inside the floor. In all cases, gait recognition is non-intrusive and does not require a strong cooperation from the user. Moreover, it is non-invasive because it does not require the user to do any specific action but walk, except for very limited cases. The following analysis focuses on wearable sensor-based techniques, in particular on advantages and issues characterizing sensors built in modern smartphones and other personal mobile devices [8,9]. The use of mobile devices to carry out biometric recognition is gaining increasing interest in scientific community. The wearable sensors embedded in smartphones, tablets and smart watches. e.g., accelerometers and gyroscopes, allow exploring new

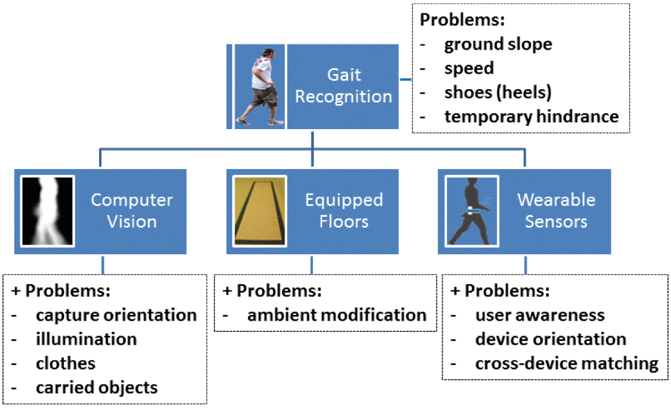

Fig. 1. Gait recognition methodologies and specific problems raised.

research topics that go beyond biometric recognition based on traditional traits, such as face and fingerprints. In general, a gait template acquired by an inertial sensor is made up by 3 time series. When an accelerometer is used, these are the acceleration values from the 3 axes over which the signal is captured. When a gyroscope is exploited too, there is a further triplet of signals, synchronized with the accelerometer ones, and acquired over the same 3 axes. Figure 2 shows an example from the BWR MultiDevice dataset [7] of the data recorded by an embedded accelerometer in a commercial smartphone, namely a OnePlus One.

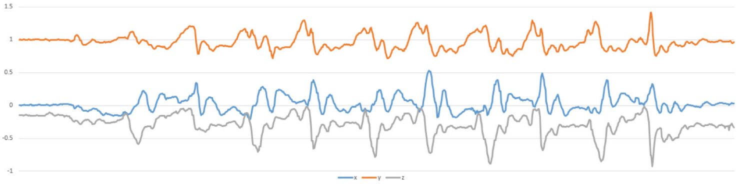

Fig. 2. An example of walking signal from the BWR Dataset.

Besides gait recognition, new behavioral patterns are also being investigated, whose analysis exploits ubiquitous and cheap user equipment. For instance, Google is developing the Abacus project [21], in the context of Google's Advanced Technology and Projects group (ATAP). This is a team and in-house technology incubator created by former DARPA. Abacus explores the use of the phone sensors to gather data about their user.

3 Related Works: Some Proposals for Gait Recognition via Wearable Devices

Works in literature addressing the topic of gait recognition via wearable devices report the use of different kinds of devices, sometimes not readily available in an everyday context. From an operational point of view, it is possible to sketch a rough classification into two main categories, out of which some examples follow. The first category includes proposals that rely on a preliminary step/cycle detection (in general, a cycle is a pair of steps). In this way, instead of comparing the full signals, "chunks" of them are matched, either choosing the best representative subset or fusing results from matching each chunk on its own. Two examples of this category are [17,18]. They exploit a Motion Recording Sensor (MRS), which measures acceleration in three orthogonal directions, namely up-down, forward-backward and sideways, with a sampling frequency of 100 Hz. The MRS includes an internal memory to record the signal and a port to transfer it. The device is attached to the ankle. Walking cycles are detected and normalized in time, so that each cycle contains 100 acceleration values. Matching is carried out by Euclidean distance, either between the average steps of each walk, or between each pair of steps respectively in the two works. The work in [15] exploits the accelerometer embedded in Google G1 phone. During gait signal recording, the phone is placed in a pocket attached to the belt of the subject on the right-hand side of the hip. The phone is positioned horizontal, the screen points to the body, the upper part of the phone points in walking direction. Matching exploits the classical Dynamic Time Warping (DTW) algorithm. This is also common to other methods. The use of DTW allows, up to a certain extent, to avoid constraining cycles to be of the same size. The last example reported here is the work in [26]. It adopts a completely different approach using signature points and neighbor search. Proposals in the second group lack the preliminary phase of step/cycle segmentation, and generally use machine learning techniques. For example, [22] exploits Support Vector Machine (SVM) technique. The gait characteristics are captured using the built-in accelerometer of the same kind of smartphone as in [15], but gait features are extracted from the times-series data from a selected time window without a preliminary identification of the contained gait cycles. Various features are extracted from the measured accelerations and used to train a SVM. It is interesting to notice that the extracted features include the Mel- and Bark-frequency cepstral coefficients (MFCC, BFCC) which are commonly used in speech and speaker recognition. As a further example, still capturing data by Google G1 phone, [23] exploits Hidden Markov Models (HMM) for modeling the time series data corresponding to the gait signal. A modified version of Viterbi algorithm is used for matching. The works in [24,25] both rely on k-NN algorithm, but the second one takes again cycles into consideration, and moreover exploits the addition of gyroscope signal. Finally, [31] is an evolution of the system proposed in [26], that fuses the use of the signature points with a preliminary clustering phase to increase the final performances.

4 From Wearable Sensors to the Cloud

In few words, the cloud model and its solutions especially address the needs of companies or consumers needing to exploit specific technologies, but lacking the necessary software/hardware/technical resources, or preferring an outsourcing strategy. Therefore, many major stakeholders started providing cloud services, also in the form APIs to be embedded in proprietary software (e.g., Microsoft Azure [30]).

Biometric applications are becoming more and more widespread and sophisticated [1]. Moreover, the last trend of the market is to make them available even on devices, e.g. personal mobiles, that may not be equipped with the necessary storage/computational resources. The Biometrics-as-a-Service (BaaS) model can be considered similar to the Software-as-a-Service (SaaS) model, because it provides software tools (in this case related to biometric recognition tasks) in the cloud and makes it available to customers. An example of prototypical consumer application that uses Cognitive Services included in Microsoft Azure is presented in [13,14].

The cloud paradigm raises new challenges, both related in general to cloud computing and Software-as-a-Service, and in particular to Biometrics-as-a-Service [5]. As for any cloud-based model, anomalous behavior from the application can be raised by misconfigurations, non-fatal hardware errors or by programming mistakes. These problems can derive, for example, from the virtualization layer, e.g., from the Virtual Machine (VM) Monitor, and they "*may cause failures, ranging from simply detectable crashes to unpredictable and erratic runtime behaviors*" [6]. Of course, problems in such level will propagate upwards the above levels. Moreover, software failures can also happen at higher levels, for example they can regard the hosted Web server or databases. The causes can be manifold, spacing from natural disasters, human errors, application bugs, erroneous configurations. Notwithstanding the possible cause(s) of rising issues, the service must be maintained available on a continuous basis (resilient). Otherwise a degradation of the quality of service (QoS) can be perceived by the users and practically represent a violation of the Service Level Agreement (SLA) contract. This may ultimately rise possible legal actions. In order to increase fault-tolerance, the cloud-based services tend to duplicate resources, e.g., physical servers in possibly different locations and more hosting per service. Interested reader can find more detailed information about cloud services in [27], while [16] provides an exhaustive description of structure, approaches and issues for systems dealing with mobile cloud computing. Finally, [29] provides information about security issues risen in this field.

The use of mobile devices for biometric gait recognition raises specific issues. First of all, capture of the reference sample to use for the future recognition operations (enrollment) may be carried out by the user without the assistance of an operator. This calls for user interaction features implementing a robust protocol, in order to support the acquisition of good quality signals even by non-expert users [2,10–12]. After capture and local processing of the biometric sample, this must be secured in order to avoid its theft. Recognition operations can be carried out either through a verification procedure, that entails an identity claim and a 1:1 matching, or an identification procedure. In this case the matching is 1:N, and requires to compare the new incoming sample (probe) with all enrolled ones (gallery). Of course, it is hard to hypothesize that this latter kind of operation can be carried out locally. One of the reasons that is often mentioned is the lack of sufficient computing power on present mobile devices. Actually, though being a real possible problem, this is not the main one. In order to carry out identification locally, any single personal device should store the complete gallery of samples of enrolled subjects. Besides being hardly feasible, both privacy and security issues advise against this solution. Notwithstanding any securing and/or anonymizing procedure, the replication on poorly attended/secured devices of potentially sensible data can create a serious flaw. Therefore, a secure transmission protocol must be devised, that submits a probe to recognize to a dedicated cloud service. The latter both includes storing facilities for possibly large size galleries, and enough computing resources to carry out recognition in real time even against massive amounts of data. In order to ensure data protection, the modeling of cryptographic protocols [3,4] and distributed ledger might be deployed to ensure the exclusive use of sensitive data, either local or distributed. Being the gait signal quite cheap in terms of storage (with respect to images) both storage and processing can be especially efficient.

Of course, a real market deployment requires to address problems specifically related to the gait signal. It is important to consider that the accelerometers present inter-device differences [7], that can be relevant even in the case of the same sensor model exiting from the same production line and built in identical conditions. Calibrations and systematic errors can especially happen when the sensor is built in a smartphone. This is because in this case the required accuracy is generally not especially high. In addition, the data might be either read with a constant frequency or on "significant" value changes, as for Android standard for accelerometer signal. This causes relevant differences in the "shape" of the captured signal. The acceleration values are not even independent from the sensor orientation and this creates further significant problems when the device in which the sensor is built-in can freely rotate. Different kinds of approaches are studied in literature in order to reduce these problems. These topics are addressed by ongoing research [15,21,24,31]. However, it is interesting to notice the possibility of significant improvement even with simple preliminary solutions. Tables 1 and 2 show results from a set of experiments carried out to validate the feasibility of a signal normalization procedure that can be carried out by the user when the application is installed on the telephone. Three smartphones of different brands were used to test cross-device performances, each with a different accelerometer model embedded, namely a OnePlus One (with a LIS3DH Accelerometer, by ST Microelectronics), a Samsung Galaxy S4 Active (with a K330 3-axes Accelerometer), and a Sony Xperia S (with a Bosch Sensortec BMA250 accelerometer). Walk signals belong to 25 subjects in two acquisition sessions with an average time distance of about 15 days. The subjects wore different kinds of shoes but no high heels. Each single session is composed by 6 acquisitions, 2 for each smartphone, for a total of 300 walk signals. The adopted procedure [7] allows to increase the accuracy of both intra- and inter-device (cross-device) matching. In Tables 1 and 2, the performance are measured in terms of Recognition Rate (RR) for closed set identification (the most popular 1:N matching modality in literature: the probe subject is always present in the system gallery): the higher the RR, the better; Equal Error Rate (EER) is used instead for both verification (1:1 matching with identity claim) and open set identification (1:N, but the probe user may not be an enrolled one): the lower the EER, the better. Two different matching algorithms are used, one applying Dynamic Time Warping (DTW) to the whole gait signal (WHOLE WALK), whose results are reported in Table 1, and the second one using a segmentation procedure to match single steps (SEPARATE STEPS), whose results are reported in Table 2. In the figure, AllDevices refers to a situation where the matched gait signal may be either captured by the same device or not. Device_vs_Device represents the average performance achieved by matching a probe captured with one device with a gallery sample captured by a different device. SameDevice represents the average performance achieved by matching only signals coming from the same device. O.D. stands for Original Dataset, while N.D. denotes the Normalized Dataset.

Table 1. Example of performance achieved by accelerometer-based gait recognition in a cross-device setting with a complete walk.

Closed Set Identification - WHOLE WALK			
Test	RR - O.D.	RR - N.D.	Improv.
AllDevices	52.0%	54.5%	4.81%
Device_vs_Device	35.3%	49.3%	39.62%
SameDevice	50.3%	52.0%	3.31%

Verification - WHOLE WALK			
Test	ERR - O.D.	ERR - N.D.	Improv.
AllDevices	31.8%	29.6%	7.43%
Device_vs_Device	31.4%	29.5%	6.23%
SameDevice	28.8%	29.0%	-0.69%

Open Set Identification - WHOLE WALK			
Test	ERR - O.D.	ERR - N.D.	Improv.
AllDevices	31.8%	29.6%	7.43%
Device_vs_Device	79.2%	72.3%	9.45%
SameDevice	25.2%	25.0%	0.67%

Once the above problems are addressed, the combination of mobile gait recognition and cloud storage/computing can create a kind of transparent authentication, e.g., to access protected areas. The user has no need to either claim an identity or carry out a specific operation. A pair of very small Bluetooth emitting sources (beacons) suitably positioned along the controlled pathway drives the

Table 2. Example of performance achieved by accelerometer-based gait recognition in a cross-device setting with segmented steps.

Closed Set Identification - SEPARATE STEPS			
Test	RR - O.D.	RR - N.D.	Improv.
AllDevices	22.5%	34.5%	53.33%
Device_vs_Device	15.2%	26.7%	47.06%
SameDevice	22.0%	29.0%	106.67%

Verification - SEPARATE STEPS			
Test	ERR - O.D.	ERR - N.D.	Improv.
AllDevices	50.0%	50.0%	0.00%
Device_vs_Device	47.2%	42.5%	11.17%
SameDevice	44.9%	43.1%	4.26%

Open Set Identification - SEPARATE STEPS			
Test	ERR - O.D.	ERR - N.D.	Improv.
AllDevices	83.3%	71.3%	16.83%
Device_vs_Device	92.2%	88.7%	3.95%
SameDevice	65.8%	47.7%	38.11%

start and stop of the sample acquisition. In general, the only function of beacons is to broadcast their IDs. Once they are registered within a specific application, capture of the broadcasted ID can trigger the start of signal acquisition as well as its termination and sending to the remote authentication/storage service. In this way, the user is free from the duty to start and stop capture and send the data. All operations happen according to the model of implicit interaction [28]. No cooperation is required by the user except for turning on Bluetooth on the mobile device and walk to reach the interested area (see Fig. 3).

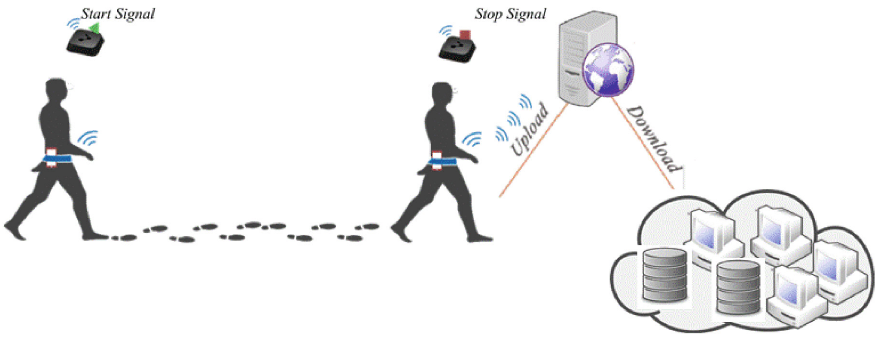

Fig. 3. A possible architecture for gait recognition via mobile devices and cloud resources.

From the point of view of privacy protection and robustness to spoofing, it is to say that these two aspects are both less critical when gait is involved. As for the former, acquiring the gait signal of a person does not allow to recover its identity, as it may happen for example with face images seen by chance in other contexts. As for the latter, mimicking the walking pattern of another person has been found to be very hard [20]. From the communication security point of view, the new standards, such as HTTPS with TLS 1.2[1] or the new 1.3 version, are increasing more and more their encryption/protection capabilities, allowing a secure data transfer between a mobile device and the recognition server/cloud service. Moreover, it is possible to include in the acquisition application the requirement for a specific "fingerprint" on the Certification Authority (CA) TLS certificate, effectively blocking rogue CA, possibly used in Man in the Middle (MITM) attacks.

This kind of architecture can also be adapted to other biometric traits. However, the only one that can be captured via mobile without any user explicit action is gait, and this makes related features particularly appealing. Figure 4

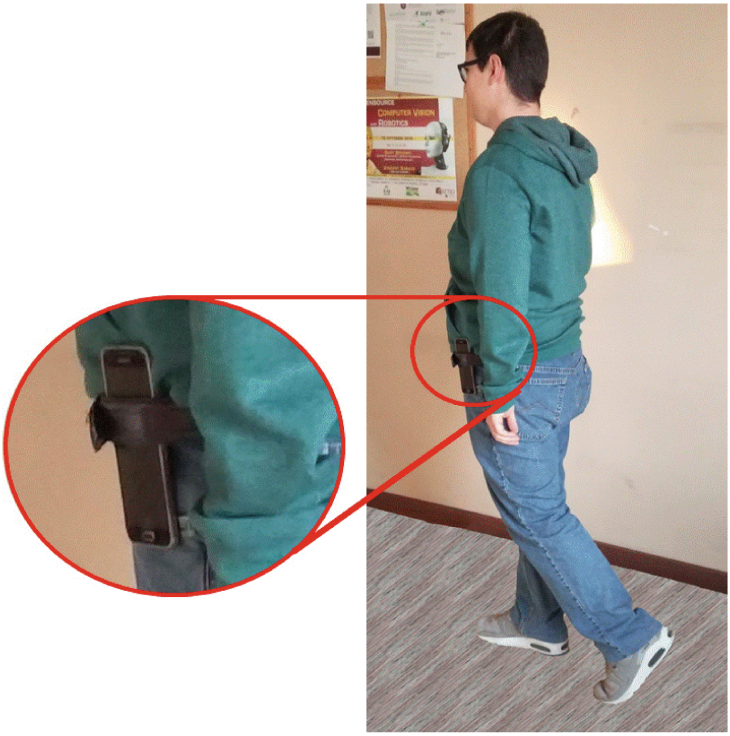

Fig. 4. The user simply carries the smartphone fixed to the belt.

[1] https://tools.ietf.org/html/rfc5246.

shows a possible use of the technology, with the smartphone simply fixed to the belt. There will be no need for pushing buttons, issuing commands, or whatever.

It is to say that for other biometric traits the combined use of biometric recognition and cloud computing is already a concrete possibility. An example is represented by Microsoft Cognitive Services[2], which are part of the Azure framework and include face, voice and emotion recognition services that can be called via provided APIs. Actually other service providers have also embraced the strategy of Biometrics as a Service (BaaS) or "Biometric security in the Cloud" to provide services to companies (see for example Fujitsu[3] and AWARE[4]). The next challenge is to widen the use of these technologies from company to user applications.

5 Conclusions

Gait recognition by wearable sensors is a promising approach that tries to solve problems related to computer vision-based techniques. The entailed signal capture procedure is definitely unobtrusive, since the user has only to wear a smartphone, which is nowadays an extremely common practice. Automatic capture can be triggered by small Bluetooth radio transmitters, according to the paradigm of implicit interaction. Authorized users can be free to move along the places where access is granted without needing to provide smartcards or passwords. However, even if the kind of produced signals (temporal series from accelerometers and other sensors) is lightweight if compared to images, large scale processing can still pose cost problems for in-house large scale applications. In this scenario, BaaS is a possible solution. BaaS may follow the same growth, from company to consumer, of other cloud-based services. Two issues are to be considered: price and privacy. The price of the service is normally computed on the basis of bunches of API calls, and therefore depends on the scale of the hosting application, and on the level of requested service. An extension to consumer applications calls for a reasonable scaling of present service costs for a more limited scope. For example, a private consumer might be attracted by the idea of automatically identifying on the doorstep only a small set (order of ten) of trusted subjects allowed to enter home. Privacy and safe storing of personal data have to be addressed too. A biometric service provider would become a critical collector of sensible data to be strongly protected. Once costs and security issues will be addressed, BaaS may really become a part of everyday life.

References

1. Abate, A.F., Nappi, M., Ricciardi, S.: I-am: implicitly authenticate me person authentication on mobile devices through ear shape and arm gesture. IEEE Trans. Syst. Man Cybern. Syst. **99**, 1–13 (2017)

[2] https://docs.microsoft.com/en-us/azure/cognitive-services/welcome.

[3] http://www.fujitsu.com/us/services/application-services/saas/biometrics-as-a-service/.

[4] https://www.aware.com/category/biometrics-as-a-service-baas/.

2. Barra, S., De Marsico, M., Nappi, M., Narducci, F., Riccio, D.: A hand-based biometric system in visible light for mobile environments. Inf. Sci. (2018)
3. Castiglione, A., Santis, A.D., Masucci, B., Palmieri, F., Castiglione, A., Huang, X.: Cryptographic hierarchical access control for dynamic structures. IEEE Trans. Inf. Forensics Secur. **11**(10), 2349–2364 (2016). https://doi.org/10.1109/TIFS.2016.2581147
4. Castiglione, A., et al.: Hierarchical and shared access control. IEEE Trans. Inf. Forensics Secur. **11**(4), 850–865 (2016). https://doi.org/10.1109/TIFS.2015.2512533
5. Castiglione, A., Choo, K.K.R., Nappi, M., Narducci, F.: Biometrics in the cloud: challenges and research opportunities. IEEE Cloud Comput. **4**(4), 12–17 (2017)
6. Cinque, M., Russo, S., Esposito, C., Choo, K.K.R., Free-Nelson, F., Kamhoua, C.A.: Cloud reliability: possible sources of security and legal issues? IEEE Cloud Comput. **5**(3), 31–38 (2018)
7. De Marsico, M., De Pasquale, D., Mecca, A.: Embedded accelerometer signal normalization for cross-device gait recognition. In: 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1–5. IEEE (2016)
8. De Marsico, M., Mecca, A.: Biometric walk recognizer. In: Murino, V., Puppo, E., Sona, D., Cristani, M., Sansone, C. (eds.) ICIAP 2015. LNCS, vol. 9281, pp. 19–26. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-23222-5_3
9. De Marsico, M., Mecca, A.: Biometric walk recognizer. Multimedia Tools Appl. **76**(4), 4713–4745 (2017)
10. De Marsico, M., Nappi, M., Narducci, F., Proença, H.: Insights into the results of miche I-mobile iris challenge evaluation. Pattern Recogn. **74**, 286–304 (2018)
11. De Marsico, M., Nappi, M., Proença, H.: Results from miche II-mobile iris challenge evaluation II. Pattern Recogn. Lett. **91**, 3–10 (2017)
12. De Marsico, M., Nappi, M., Riccio, D., Wechsler, H.: Mobile iris challenge evaluation (miche)-I, biometric iris dataset and protocols. Pattern Recogn. Lett. **57**, 17–23 (2015)
13. De Marsico, M., Nemmi, E., Prenkaj, B., Saturni, G.: A smart peephole on the cloud. In: Battiato, S., Farinella, G.M., Leo, M., Gallo, G. (eds.) ICIAP 2017. LNCS, vol. 10590, pp. 364–374. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70742-6_34
14. De Marsico, M., Nemmi, E., Prenkaj, B., Saturni, G.: House in the (biometric) cloud: a possible application. IEEE Cloud Comput. **5**(4), 58–69 (2018)
15. Derawi, M.O., Nickel, C., Bours, P., Busch, C.: Unobtrusive user-authentication on mobile phones using biometric gait recognition. In: 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pp. 306–311. IEEE (2010)
16. Dinh, H.T., Lee, C., Niyato, D., Wang, P.: A survey of mobile cloud computing: architecture, applications, and approaches. Wirel. Commun. Mobile Comput. **13**(18), 1587–1611 (2013)
17. Gafurov, D., Snekkenes, E.: Towards understanding the uniqueness of gait biometric. In: 8th IEEE International Conference on Automatic Face & Gesture Recognition, FG 2008, pp. 1–8. IEEE (2008)
18. Gafurov, D., Snekkenes, E., Bours, P.: Improved gait recognition performance using cycle matching. In: 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 836–841. IEEE (2010)
19. Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. Circ. Syst. Video Technol. **14**(1), 4–20 (2000)

20. Muaaz, M., Mayrhofer, R.: Smartphone-based gait recognition: from authentication to imitation. IEEE Trans. Mobile Comput. **16**(11), 3209–3221 (2017)
21. Neverova, N., et al.: Learning human identity from motion patterns. IEEE Access **4**, 1810–1820 (2016)
22. Nickel, C., Brandt, H., Busch, C.: Classification of acceleration data for biometric gait recognition on mobile devices. BIOSIG **11**, 57–66 (2011)
23. Nickel, C., Busch, C., Rangarajan, S., Möbius, M.: Using hidden markov models for accelerometer-based biometric gait recognition. In: 2011 IEEE 7th International Colloquium on Signal Processing and Its Applications (CSPA), pp. 58–63. IEEE (2011)
24. Nickel, C., Wirtl, T., Busch, C.: Authentication of smartphone users based on the way they walk using K-NN algorithm. In: 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pp. 16–20. IEEE (2012)
25. Nowlan, M.F.: Human identification via gait recognition using accelerometer gyro forces. Yale Computer Science (2009). http://www.cs.yale.edu/homes/mfn3/pub/mfngaitid.pdf. Accessed 12 Nov 2013
26. Pan, G., Zhang, Y., Wu, Z.: Accelerometer-based gait recognition via voting by signature points. Electr. Lett. **45**(22), 1116–1118 (2009)
27. Rimal, B.P., Choi, E., Lumb, I.: A taxonomy and survey of cloud computing systems. In: Fifth International Joint Conference on INC, IMS and IDC, NCM 2009, pp. 44–51. IEEE (2009)
28. Schmidt, A.: Implicit human computer interaction through context. Pers. Technol. **4**(2–3), 191–199 (2000)
29. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. **34**(1), 1–11 (2011)
30. Wilder, B.: Cloud Architecture Patterns: Using Microsoft Azure. O'Reilly Media Inc., Sebastopol (2012)
31. Zhang, Y., Pan, G., Jia, K., Lu, M., Wang, Y., Wu, Z.: Accelerometer-based gait recognition by sparse representation of signature points with clusters. IEEE Trans. Cybern. **45**(9), 1864–1875 (2015)