This is a postprint version of the following published document:

Lorena Gonzalez-Manzano, Jose M. De Fuentes, and Arturo Ribagorda. 2019. Leveraging User-related Internet of Things for Continuous Authentication: A Survey. ACM Comput. Surv. 52, 3, Article 53 (June 2019), 38 pages.

DOI: https://doi.org/10.1145/3314023

© 2019 Association for Computing Machinery. This is the author's version of the work. It is posted here by permission of ACM for your personal use. Not for redistribution. The definitive version was published in Lorena Gonzalez-Manzano, Jose M. De Fuentes, and Arturo Ribagorda. 2019. Leveraging User-related Internet of Things for Continuous Authentication: A Survey. ACM Comput. Surv. 52, 3, Article 53 (June 2019), 38 pages. DOI: https://doi.org/10.1145/3314023

Leveraging user-related Internet of Things for continuous authentication: a survey

LORENA GONZALEZ-MANZANO, Universidad Carlos III de Madrid
JOSE M. DE FUENTES, Universidad Carlos III de Madrid
ARTURO RIBAGORDA, Universidad Carlos III de Madrid

Among all Internet of Things (IoT) devices, a subset of them are related to users. Leveraging these user-related IoT elements, it is possible to ensure the identity of the user for a period of time, thus avoiding impersonation. This need is known as Continuous Authentication (CA). Since 2009, a plethora of IoT-based CA academic research and industrial contributions have been proposed. We offer a comprehensive overview of 58 research papers regarding the main components of such a CA system. The status of the industry is studied as well, covering 32 market contributions, research projects and related standards. Lessons learned, challenges and open issues to foster further research in this area are finally presented.

CCS Concepts: • **Security and privacy** → **Authentication**; • **General and reference** → *Cross-computing tools and techniques*; • **Information systems** → *Data mining*; • **Applied computing** → *Consumer products*;

Additional Key Words and Phrases: Continuous Authentication (CA), Internet Of Things (IoT), user-related IoT, IoT-based CA, CA algorithms, CA evaluation metrics, CA industry

ACM Reference format:
Lorena Gonzalez-Manzano, Jose M. de Fuentes, and Arturo Ribagorda. 2019. Leveraging user-related Internet of Things for continuous authentication: a survey. 1, 1, Article 1 (February 2019), 35 pages.
https://doi.org/10.1145/nnnnnnn.nnnnnnn

---

1 INTRODUCTION

In the age of interconnectivity, we are surrounded by technology which tries to make our lives easier. Fridges which inform the user about food to buy, smart bracelets to control our heart rate, smartphones to be permanently up-to-date anywhere, etc. Moreover, an increasing amount of constrained devices are including connectivity to enable remote management, such as video cameras or industrial sensors. This trend is known as Internet of things (IoT), a paradigm focused on the global interconnection of smart objects by means of extended network technologies [121]. A “thing” in IoT is everyday object, that is readable, recognizable, locatable, addressable, and controllable via the Internet [89]. A huge diversity of devices, like Radio Frequency IDentification (RFID) tags or even smartphones, are considered IoT devices [30]. Therefore, they have been applied in many different fields such as industrial systems or environmental analysis. Among all variants, this survey focuses on user-related IoT devices. This term refers to IoT devices that can either be ported by users (e.g., smartwatches) or that can collect and/or process data from them (e.g., security cameras).

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2019 Association for Computing Machinery.
Manuscript submitted to ACM

However, for simplicity reasons, we will use the term IoT devices hereinafter , though we will keep the term *user-related* when needed for clarity.

In this novel environment, security and privacy issues cannot be neglected, being 2010 the time when these topics became a matter of concern [113]. IoT devices like smartphones or smartwatches can connect or exchange data between them and a security flaw in one of them can be a key step to access another. On the other hand, as some IoT devices are typically carried by their owner, the mere presence of the device can be regarded as an evidence of presence of the owner. However, if these devices are robbed, the attacker could inherit the benefits of their possession. In some cases, device robbery trends are non-negligible. For example, according to Consumer Reports, more than 3 million handsets were stolen in 2013[1]. Besides, IoT devices may store a significant amount of sensitive data, which should only be accessed by authorized users [109]. These issues are specific to IoT devices and call for tailored mechanisms. In particular, it would be desirable that the IoT device could reliably determine the identity of the legitimate user, thus authenticating him/her. Such a user may be the porting one (e.g., in the case of smartwatches) or a subject under control (e.g., in the case of surveillance cameras). Ideally, this could be carried out constantly, ensuring that the user is not impersonated at any time. This would be needed, for example, to prevent malicious usage if the IoT device is robbed. This leads to a specific type of authentication called Continuous Authentication (CA).

CA has been explored for many years. One of the first contributions was developed in 1995 [165], proposing the analysis of typing characteristics of a user in an IBM PC keyboard. Years later, in 2000, [102] presented the use of the camera in a desktop computer to do a continuous analysis of users' faces. In 2006, [59] applied neural networks to also recognize users' typing patterns in a desktop machine. Despite these efforts, it was not until 2009 when the first proposal regarding IoT-based CA appeared [82]. It was focused on the analysis of users' heart rate. From then on, 58 scientific proposals have been developed. Moreover, to the best of authors' knowledge, there are 32 market initiatives with some publicly available information. The fast evolution pace and the diversity of IoT devices call for having a common ground for future developments.

There are multiple surveys focused on IoT security and privacy [80, 118, 197]. Others concentrate on IoT while briefly mentioning some security issues [110],[23, 81]. Regarding CA, some works focus on mobile devices exclusively [136, 155], while others present general aspects about CA without going into details [163, 172] and other proposal exclusively analyzes multibiometric features [21]. As a result, none of them performs a comprehensive and holistic study of CA by means of IoT.

To overcome these limitations, this paper presents a survey of IoT-based CA approaches, that is, CA techniques that involve user-related IoT devices, either from the academic or the industrial perspective. The scope of the survey will consist of CA proposals to continuously authenticate the user against an IoT device itself or against another third party[2]. To this extent, all steps involved in the CA process are studied for each academic proposal. Additionally, a holistic study is provided by the analysis of industry status, paying attention to CA research projects, standards and market products. Thus, this work aims to provide an overview of decisions taken to design an IoT-based CA system based on the experience provided by existing academic and industrial approaches. As a result, this analysis leads us to conclude weaknesses and open issues to address in further research.

The structure of the paper is the following: Section 2 introduces the concept of authentication and its relationship with IoT devices. The characterization of CA is introduced in Section 3. The CA process is described in Section 4 considering

---

[1] https://www.businessinsider.com/smartphone-theft-statistics-2014-5?IR=T, last access February 2019.

[2] Even if the term 'IoT' contains Internet, there might be CA approaches that are fully carried out in the device itself without any need for communication. For the sake of generality, this survey covers these approaches as well.

all existing academic works of CA in IoT. Then, Section 5 presents industry status of IoT-based CA developments. Lessons learned from the previous analysis are summarized in Section 6. Challenges and open issues are presented in Section 7. Section 8 analyzes related works and compares them with this proposal. Finally, Section 9 concludes the paper.

2 FROM AUTHENTICATION TO AUTHENTICATION IN IOT DEVICES

As a prerrequisite to understand Continuous Authentication (CA) in Internet of Things (IoT), it is important to clarify the foundations of traditional authentication and how it has been implemented into IoT devices. Therefore, this Section first introduces the concept of authentication (Section 2.1), and afterwards covers its enforcement in IoT devices (Section 2.2).

2.1 Authentication

Authentication is achieved through the use of identity credentials, also called identifiers, verifying that the user has been authorized to use the presented identifier [86]. In other words, thanks to authentication it is possible to ensure that a given entity is the one it claims to be.

Traditionally, an identifier can be something you know (e.g., a password), something you have (e.g., a card) or something you are (e.g., fingerprint traces). In order for an element to be considered as identifier, the following main features have to be fulfilled [48]:

- **Universality**: every subject should have at least one identifier.
- **Uniqueness and precision**: each person should have a unique and completely different identifier.
- **Permanence**: the identifier has to remain over time.
- **Storability**: it must be possible to store the identifier.
- **Simplicity**: the identifier should be easy to collect.

Historically, one of the preferred methods for authentication in IT environments leverages on passwords. A user chooses a password the first time he logs in a service and, from that moment on, every time he accesses to such service, the password is verified [129]. This technique suffers many drawbacks that should be managed, for instance stolen or forgotten passwords. Multifactor authentication alleviates the problem. It consists of requesting different elements, e.g. something one knows and has like a password together with a credit card. In this way, an illegitimate user has less opportunities to succeed.

With the aim to balance security and usability, biometric approaches are gaining momentum. On the one hand, they are regarded as more secure since biometric traits like the iris or the face are theoretically more difficult to reproduce. However, this type of authentication may produce false positives and negatives [58] and thus, the system should be properly tested prior to its usage. Among all biometric approaches, behavioral biometrics aim to find traces in the way the user behaves which are different from the remaining subjects [28, 144, 172]. In this regard, several approaches have been proposed, such as the analysis of screen touches to unlock a mobile phone [57]. According to a global survey of IBM security in 2018, 44 % of respondents perceive biometrics as the most secure authentication method, and 65% feel comfortable with this type of authentication [160]. The same report states that this method is expected to increase adoption due to the growing consumer base of smartphones.

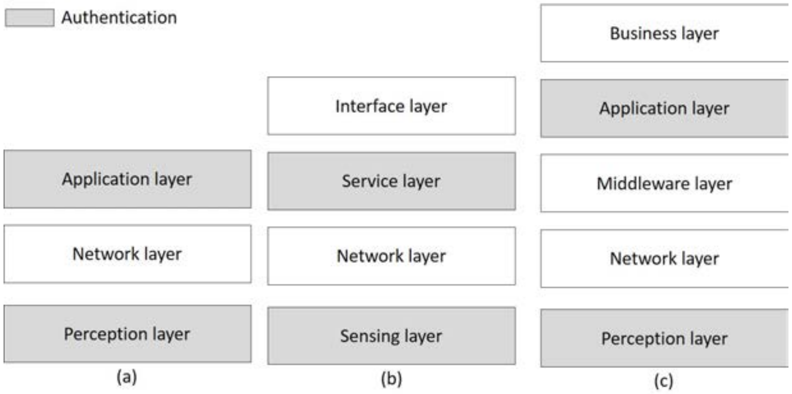


Fig. 1. IoT architectures. (a) 3-layer [190], (b) 4-layer [52], (c) 5-layer [98]

2.2 Authentication in IoT devices

Despite the great variety of IoT devices, the industry has adopted some reference architectures to guide their development [23]. In particular, three well-known ones are the 3-layer [190], 4-layer [52] and the 5-layer architectures [98] (Figure 1). The 3-layer architecture is appropriate at the initial stage of the development of IoT systems. The 4-layer architecture is service-oriented and specially useful for achieving interoperability between heterogeneous devices. By contrast, the 5-layer architecture is the first general architecture for IoT devices. In the following, we describe these architectures and highlight where authentication issues are considered.

In the 3-layer architecture, the perception layer is the lowest one. It represents physical IoT devices, e.g. sensors, that collect and process information. The network layer is the second one, whose main task is transmitting and processing data from the perception layer to the application one. This upper layer offers services to users to meet their needs.

The 4-layer architecture is analogous to the previous one in the network layer, while the perception and application layers are renamed as sensing and service layers respectively. The main difference is that the interface layer appears. It provides interaction between methods to users and other applications, which given the large number of IoT devices from different vendors and systems, is an alternative to avoid interaction problems.

In the 5-layer architecture, the middleware and the business layers appear. The perception and the network layers provide the same services as in the 3-layer architecture. The middleware allows working with heterogeneous IoT devices and connecting those that implement the same service. Subsequently, the application layer offers global management, providing users with services they demand. Finally, the business layer manages the whole IoT system, building models, graphs, etc. based on data received from the previous layer. It supports decision-making processes based on the analysis of huge amounts of data.

The existence of the aforementioned architectures does not mean that every IoT device is a relevant element for authentication. For example, industrial IoT sensors, smoke or air pollution sensors, or sensors used in farms for governing the production, they are not intended to authenticate any user. Nevertheless, a big amount of user-related IoT devices (e.g. wearables, implantable medical devices, etc.) may have a direct role in this regard. In these devices, the perception/sensing and the application/service ones are those specially involved in the authentication process. In the perception/ sensing layer some IoT devices collect data to be managed in the application/service layer which takes the final decision. The application one decides whether the user at stake is an authorized one or an impostor. For instance, the front camera of a smartphone (perception layer) may give information to an application (application layer) to decide if the user is the right one to open it. In case of the service layer, it decides whether enabling the interaction between services.

3 CHARACTERIZING CONTINUOUS AUTHENTICATION

The concept of traditional authentication presented in Section 2.1 refers to a one-shot process – the user is either authenticated or not after a decision taken at a given moment.

With the advent of sensing technologies (recall the perception layer of IoT devices, Section 2.2), a novel term called Continuous Authentication has appeared. In order to determine which mechanisms can be considered suitable for CA, it is necessary to provide a clear definition of the term. Although a plethora of definitions exist (e.g. [19, 167]), in the following we consider three of them. Thus, Stylios et al. [172] define CA as *'a new generation of security mechanisms that continuously monitor user behavior and use this as basis to re-authenticate them periodically throughout a login session'*. This definition highlights that CA performs the authentication decision repeatedly, considering user behavior. However, the frequency and the extent of the behavior concept are unclear. In this regard, Frank et al. [69] go a step beyond, stating that *'CA approaches monitor the user's interaction with the device, and ideally, at every point in time (or at least with a high frequency) the system estimates if the legitimate user is using the device.'*. Thus, from their point of view, the decision should be as frequent as possible and the behavior comes from the way the user interacts with the device. Last but not least, Ahmed and Traore [19] state that CA *consists of the process of positively veryifing the identity of a user in a repeated manner throughout a computing session.*

While these definitions give valuable insights on CA, we claim they are not comprehensive enough. On the one hand, Stylios et al's definition lacks of precision in the frequency. On the other hand, Frank et al's definition leave aside those approaches whose data comes from other sources different from the user interaction. With the advent of wearable computing, we claim that this is no longer valid – data about the user can be seamlessly retrieved without the need of an explicit interaction with the device. Concerning Ahmed and Traore's one, it refers to a computing session. Thus, giving access to a restricted area based on a given trait (e.g. gait) would fall outside of this definition. Moreover, none of the definitions consider the consequences of the denial of authentication. To overcome these limitations, we adopt the following definition:

Definition. Continuous Authentication (CA) refers to a security mechanism that monitors user actions at every point in time (or at least with a high frequency) during a session and determines if that user is the legitimate one. If it is not the case, suitable defensive mechanisms should be put in place.

The above definition (1) keeps the precision on how frequent the assessment should be done; (2) refines the term behavior by a more concrete term (actions) which do not necessarily need to be carried out in the device or within a computing session; and (3) considers the system reaction in the event of an user impersonation.

On the other hand, once CA is defined, its benefits have to be considered. The improvements of CA over a traditional authentication system can be analysed in terms of security, safety and comfort. Concerning security, CA aims to reduce the chances of impersonation. A non-CA system identifies the user at the very beginning of the process. Thus, if he/she is impersonated afterwards, the attacker inherits the legitimate user's rights. On the contrary, CA brings a better protection. For example, if an attacker steals a smartphone after illegally getting the password, CA could allow the device to suddenly block itself after observing that the usage pattern differs from that of the legitimate user[56].

In terms of safety, the continuous monitoring of users may prevent dangerous situations which cannot be avoided otherwise. For instance, a train driver is continuously authenticated, using an IoT device (e.g. smartwatch), to avoid impersonation or detecting some anomaly in the driver's health status that prevents driving adequately. If at some point in time an illegitimate user tries to drive the train or the driver's health status is not the right one, an alarm can be somehow triggered protecting the life of passengers.

Finally, authentication cannot provide the same comfort as CA. The main reason is that the study of users along time allows the identification of features that can be seamlessly retrieved. For instance, when entering home using a key, password or card (i.e., traditional authentication), the user can turn on or off the air conditioning.

4 CONTINUOUS AUTHENTICATION LEVERAGING IOT DEVICES

CA offers interesting features over authentication (recall Section 2.1) but it requires monitoring users over a period of time. Given the nature of IoT devices and their closeness to users, applying them for CA purposes is specially attractive. The increasing sensorial capabilities of some IoT devices simplifies collecting data from users that can serve as identifiers. In any case, it must be noted that our definition of IoT device does not imply that it will be referred to a single user. A security camera, for instance, could authenticate a set of authorized users. In this regard, this survey studies approaches that enforce CA using data collected from user-related IoT devices and in which the authentication process is carried out in the IoT device itself or in other entity or device.

In order to leverage IoT for CA purposes, a total of five steps depicted in Figure 2 have to be considered. Firstly the scenario where the authentication is going to be performed is selected. For example, authenticating someone while he/she is running. Of course, some approaches can apply to several scenarios or even be suitable for a generic one in which some conditions are met.

The selection of the user-related IoT device (e.g., smartphones, holters, etc.) in charge of collecting authentication data is the second step. Again, this step may define a particular device, a set of them or even a generic description of suitable IoT devices. In the latter case, a particular choice has to be defined for the experimental assessment of the approach.

The third step corresponds to the selection of features used in the authentication enforcement. This issue may depend on the considered IoT device and its sensorial capabilities. For example, smartphones are interesting to capture touchscreen events, while other devices like medical ones are specially useful to acquire human body signals.

Once features are collected, the authentication is enforced. It requires the use of a particular data analysis technique, as well as an algorithm like a classifier, to distinguish between authorized users and impostors. As the authentication is continuous, the enforcement should be constantly performed. Ideally, this should take place in real time, that is, while the data is collected. Depending on the IoT device, this might not be even feasible or require external elements (e.g., powerful servers) to be carried out. Moreover, it may have a non-negligible impact on the device resources. Hence, a proper evaluation of this aspect is crucial to ensure the practical suitability of the proposal to state-of-the-art devices.

The final step is to analyse the effectiveness of the proposal. To this extent, a typical approach is the use of a dataset, either ad-hoc or a publicly available one. Over this dataset, the proposed mechanism is applied and a given evaluation metric (such as the accuracy, the false positive/negative rate, etc.) is computed. As a difference to traditional authentication, CA may consider metrics to determine the suitability over time. For example, in a CA system it may be relevant to measure how much time the system takes to discover an attacker. On the other hand, CA systems may include a recovery mechanism for cases in which the legitimate user is wrongly regarded as an attacker. Thus, the recovery period is another issue at stake.

The following sections focus on each of the aforementioned phases. We describe the different alternatives that can be taken for each step, together with the description of 58 surveyed papers.

Fig. 2. Design process of an IoT-based CA approach

4.1 Scenario selection

Many scenarios can take advantage of the assorted nature of IoT devices. Several works highlight their use in smart cities, healthcare or transportation, to name a few [81, 121]. Nevertheless, authentication and CA in particular, reduces the application scope. In the following we introduce scenarios in which leveraging user-related IoT devices for CA is interesting, also discussing the benefits of CA in terms of security, safety and comfort introduced in Section 3:

- *Smart building* is a place equipped with IoT devices which may contribute to the quality of life of people, either reducing the power consumption, improving users' comfort or taking care of users' security [121, 149]. This category involves all buildings equipped with an ecosystem of IoT devices to collect data along time, such as smart homes or smart factories. The amount of devices and computing resources may be balanced regarding the investment and the utility. Nonetheless, despite the variety of existing applications, the use of CA can be considered in the following scenarios:
  - Open the savings box as long as the user behaves as expected. A user is monitored since entering his home/ office. If he enters either running or, on the contrary, moving slowly and silently until identifying the save box, it is not going to be opened if this behavior differs from the normal one.
  - Room comfort. Monitoring users in a room may allow the improvement of their comfort. If users are continuously authenticated, the room can be set up according to their preferences, for instance automatically setting their preferred temperature considering his/her habits. This would only be applicable when the set of potential users is previously known (e.g. working environment).

  Based on these scenarios, CA in smart buildings may help to improve comfort, enhancing users' experiences; and security, protecting users' belongings. Authentication could also be applied but CA goes a step forward strengthening these services.
- *Transportation* involves services related to the use and management of vehicles. The verification of being the right driver, not an impostor, while driving or being driving in the right conditions (e.g. appropriate heart rate) is a priority. This could be achieved, for instance, monitoring the brain, the sitting posture of the driver [126, 148] or even using face recognition. Another field of application is the continuous recognition, thus CA, of the driver's voice to only execute commands said by him [66]. In this last paper CA is considered during a session, in such a way that the access to the service, voice assistant, is verified every time the user speaks and not just at the beginning as traditional authentication systems suggest. The use of CA is directly linked to security and, even more important, to safety. Security because it ensures that the legitimate driver is the right one.
- *Healthcare* is one of the essential services in society and lots of advances go towards its enhancement. The link between technology and healthcare has let to introduce the concepts of e-health, m-health and s-health [170]. The first refers to the use of information and communication technologies within the health sector. Similarly, m-health corresponds to the use of mobile devices for healthcare purposes. Finally, the nexus between smart cities and mobile devices motivates the concept of s-health. All these concepts aim to improve the patients'

quality of life, e.g. [191] proposes a m-Health system for health monitoring protecting patients' privacy. In this vein, CA stands as a nice alternative to detect unexpected behavioral patterns (such as an abnormal heart rate) as soon as possible. The CA of doctors in terms of data privacy is also a priority. For instance, CA can be applied to ensure that access to patients' records is granted only to the right user (doctor in this case), who is identified along the whole process to avoid impersonations and thus, data leaks. In this way, CA contributes to achieving security. At the same time, it also contributes to safety – authenticating a patient continuously may help to detect, for example, that a holter has been compromised, and thus patient's life put at risk.

- *Retail services*, available for the whole population, are enhanced by an advanced communication and/or processing infrastructure. The range of settings and scenarios can be quite large. An example is the use of gait to authenticate users continuously when accessing a smart kiosk [139]. In this scenario the user movements are monitored along the way to the kiosk, being in this time when the CA process is enforced. Also trying to improve the customers experience, another example is continuously authenticating (regular) customers once entering a shop. Customers can be monitored to offer constant personalized attention, for instance advertising products such user may like. Additionally, another use case is the monitoring of the user behavior before using his smartphone for paying a product. If some malicious and/ or anomalous activity is executing in the smartphone along a certain period of time, it may raise an alarm or even block the payment.
  Many different uses of CA in retail services can be devised but apart from security, as it has been presented in previous examples, comfort is interesting herein. Retailers are eager to sell their products and the easier for clients, the more profitable for them. According to the kiosk example, it is more comfortable accessing to the kiosk and getting a magazine than requesting an identifier beforehand. In the same way, personalized attention is linked to comfort.
- *Military services* allow the provision of geographic situational awareness, communications and information sharing capabilities during tactical operations. [40] describes the first step towards the use of CA in this scenario. It presents the details of a prototyping activity in which two commercial biometric devices were integrated with a handheld communication device to perform CA. Then, comments to apply such implementation for a military-focused settings are described. Other possible example is the use of drones for controlling users above suspicion. Such users are continuously authenticated for a period of time and if some illegitimate activity is done by them, actions can be taken accordingly.
  In this scenario the use of CA to reach safety and security is presented in the previous example. Data should remain under the control of the legitimate users in a military action and the right procedures and systems should be provided to protect the lives of militaries and civilians.

According to this description, there are multiple scenarios where CA is promising. However, most of current proposals, 54 in total, present a general approach without being linked to any concrete scenario. These works are intended to be suitable for many of the mentioned scenarios. However, a proper suitability assessment should be carried out before their application in each particular setting. For instance, Preuveneers et al. use location to get dynamic context fingerprinting for continuous authentication [143]. However, in some circumstances, and also considering the element used for collecting data (e.g. GPS, Wi-Fi, etc), gathering location data could not be feasible. Issues like this encourage the evaluation of each proposal in a particular scenario.

4.2 Device selection

Nowadays, a plethora of devices may fall under the IoT category, for instance home electronic devices (e.g. smart fridges) [120]. However, as mentioned in Section 1, this survey focuses on user-related IoT devices. These devices are classified based on the level of closeness to the user:

- Portable devices: they are carried out by the user. Smartphones and tablets are well-known portable devices [46]. These devices are not always regarded as an integral part of IoT. Indeed, some authors consider them as devices that interact with IoT devices [100]. However, their evolution is making them similar to the expected capabilities of the traditional concept of IoT. Therefore, several authors consider them as part of IoT [30, 62, 131]. In this survey, we opt for this choice. This kind of devices are characterized by being easy to use, providing a wide set of services and being economically accessible to the majority of the population. Their adoption is expected to keep increasing [160]. Among other reasons, this is motivated because of their improved features such as high definition cameras [99].
- Wearables: they integrate key technologies (e.g. actuating, communication, low power computing, etc) into intelligent systems to bring new functionalities into clothes, patches, watches, glasses, and other body-mounted devices[3] [186].
- Implantable devices: due to their specific application, they are distinguished from regular wearables, although some works do not make such a distinction [61]. These devices are specially useful for healthcare monitoring, as it happens with pacemakers or heart monitoring implants [120].
- External devices: they are devices which collect and/or process users' data but are not ported by, weared by or implanted in users. Security cameras are other example, they may collect users' movements to be processed afterwards. Other external device could be a drone, which may collect users' data on the fly.

Some of the described devices count on limited resources, specially computation, storage and battery. This specially happens on wearables and implantable devices, which usually count on the order of few MHz of CPU, few 10s of KB of RAM, and few 100s of KB of ROM [43, 162]. This makes the design of new mechanisms and applications challenging.

In the studied proposals, most of them (40 cases) use portable devices, mobile phones (smartphones) in particular (e.g. [56, 142]), maybe due to their wide range of possible uses. Another subset of works apply wearable devices like smart glasses [47, 138], smart bracelets [40], shoes [194] or wearable sensors [82, 83, 117, 123, 195]. [15, 56, 124, 126, 144] apply a generic wearable and portable device. By contrast, one proposal applies an implantable device, a holter [105], while [171] an external one, which refers to a non-contact radar used to collect users' heart rate. On the other hand, [37, 114] do not mention any IoT device and [42] point out the use of an unspecified IoT device. Concerning the amount of IoT devices at stake, although the use of multiple IoT devices is an option, most proposals use a single IoT device. Additional IoT devices are commonly used when resource-constrained devices are at stake to improve processing capabilities. For example, in [42] a wearable uses a smartphone to process data due to its limited resources (more details in Section 4.4.3).

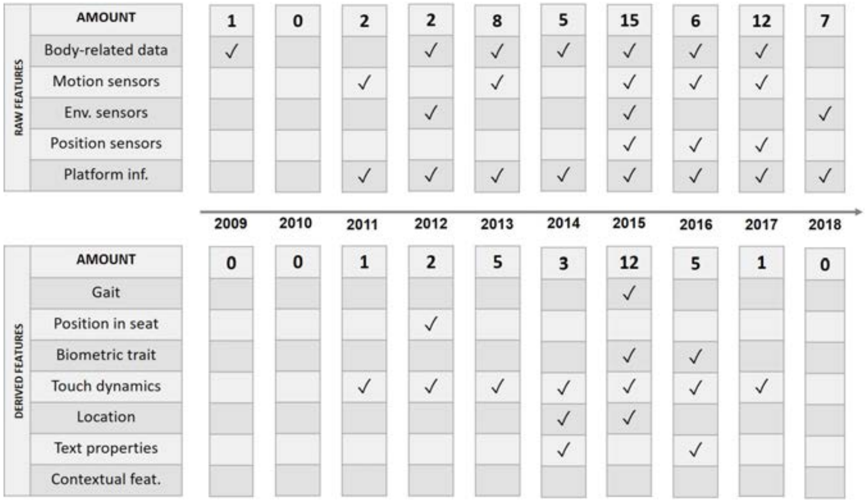
4.3 Feature selection

Authentication enforcement requires processing data collected from users. Such data can be described by a set of features. For instance, a biometric trait such as a fingerprint could be used for this purpose. In this paper we distinguish the following types of features:

---

[3] Given that users always carry out their smartphones, several works consider them to be wearable devices [123, 124, 195]. However, for the sake of clarity, in this survey they will be considered portable ones.

- *Raw features* are data directly obtained from a particular device, e.g. sensor, mobile device, etc. This information is directly used in the authentication process. It may come from different sources, as follows:
  - Sensors: elements that take input data from the environment. They are specially applied in mobile devices and wearables. Three different types are identified [27, 136]:
    - Motion sensors: they measure acceleration and rotation forces. They involve accelerometers, gravity sensors, gyroscopes, and rotational vector sensors.
    - Position sensors: they measure the physical placement of the device. They involve orientation sensors and magnetometers.
    - Environmental sensors: they measure environmental elements such as the temperature or the light. They involve barometers, photometers or thermometers, to name a few.
  - Mobile device platform information [136]: they involve all data that can be obtained from mobile devices different from the sensors described above. They involve WiFi/Bluetooth/Cell information, application usage, actions, camera, touchscreen events, microphone, calls, short messages (SMSs), device model, language, screen size, power consumption or caller/receiver data.
  - Body-related data: they refer to any kind of physiological and anatomical data. The use of physiological data, namely biosignals [93], is a common choice. This can be motivated by their significant variety (e.g., electric, magnetic or optic biosignals). They can be used for different purposes such as measuring the heart rate, the body temperature, etc. From all possible biosignals, ElectroCardioGram (ECG) data has already been shown to be successful in authentication processes [29, 105]. They are induced by electrical heart muscle excitation and thus used to measure heart rate. For the same purpose, the PhotoPlethysmoGram (PPG) signal is also commonly applied for authentication purposes [31, 37]. PPG bases on sensing the rate of blood flow as a consequence of the heart's pumping action. Apart from biosignals, there are anatomical data like the plantar pressure which is analyzed through heat maps [194].
- *Derived features* are data produced after some kind of processing of raw features. Within this type the following features are distinguished:
  - Gait: corresponds to the way humans move. For instance, it can be achieved using some motion sensors [139].
  - Position in a seat: refers to the way in which a person is sitting in a particular place.
  - Biometric trait: refers to biometric characteristics (e.g. face or eye) used for constructing a biometric profile. Cameras are the most commonly used accessory to extract these traits.
  - Touch dynamics: are the characteristics of the inputs received from a touchscreen when a user is interacting with a device. This term is usually related to keystrokes dynamics but we consider that this latter term is directly linked to 'touch' as a raw feature while touch dynamics goes a step forward, that is it has more input types such as multi-touch and touch movements [91]. For instance, it may involve the use of touch together with motion and/ or position sensors.
  - Location: is the physical location of a device. It could be directly obtained from enviromental sensors but also together with other mobile device platform information such as GPS or even by Bluetooth.
  - Text properties: are extracted from data input by users in devices (such as SMSs or instant messaging apps). Stylometry, linguistics (word profiling, lexical, syntactic and structural) or semantic properties are well-known examples.
  - Contextual features: these features depend on the environment at stake. For example, for vehicular scenarios, the driving speed, the actual lane or the current use of in-car features (e.g., break or throttle), to name a few.



RAW FEATURES	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
AMOUNT	1	0	2	2	8	5	15	6	12	7
Body-related data	✓			✓	✓	✓	✓	✓	✓	
Motion sensors			✓		✓		✓	✓	✓	
Env. sensors				✓			✓			✓
Position sensors							✓	✓	✓	
Platform inf.			✓	✓	✓	✓	✓	✓	✓	✓

DERIVED FEATURES	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
AMOUNT	0	0	1	2	5	3	12	5	1	0
Gait							✓			
Position in seat				✓						
Biometric trait							✓	✓		
Touch dynamics			✓	✓	✓	✓	✓	✓	✓	
Location						✓	✓			
Text properties						✓		✓		
Contextual feat.										

Fig. 3. Chronological evolution of the use of raw and derived features

Table 1. Use of raw and derived features in the considered papers

		#	References
RAW	Body-related	15	[82][148][105][37][83][117][123][42][171][114][126][40][84][122][111]
	Motion sensors	19	[166][187][51][125][189][139][168][138][195][144][124][66] [104] [106][111][112][45][60][15]
	Environmental sensors	3	[148][125][56]
	Position sensors	8	[122][51][125][44][138][112][45][60]
	Mobile device platform info	30	[108][166][67][148][69][50][68][198][187][94][192] [75][153][143][154][125][189][164][178][151][41][127][47] [44][116][138][66][28] [104][56]
DERIVED	Gait	1	[139]
	Position in the seat	1	[148]
	Biometric trait	3	[51][154][116]
	Touch dynamics	22	[166][67][69][50][68][198][187][192][75][153][84] [122][125][189][164][178][151][41][47][44] [168][138]
	Location	2	[142][153]
	Text properties	2	[153][71]
	Contextual features	1	[148]

Works can also be classified based on the amount of features (either raw and/ or derived) but as most proposals (28 in total) use multiple features, we stick to the raw/derived classification for analysis purposes. As depicted in Table 1, mobile devices platform data are the most common used raw features. Particularly, 10 proposals from *mobile device platform information* focus on *touch* exclusively. Consequently, *touch dynamics* is the most common derived feature, including all works with raw feature *touch* as well as [168], [122] and [84] in which *touch* is managed by *motion* and *positions sensors* respectively in the first works and by biosignals, impedances in particular, in the latter. *Body-related data* and *motion sensors* are used in 16 and 19 works respectively, which is also a representative number, where all works related to *body-related* data except for [194], apply biosignals. Note that identifiers should be created through these features and depending on their randomness and their likelihood to be unique and permanent, their management can become more or less challenging. For instance, in an scenario in which users live in the same area, *body-related* is supposed to be more discriminating than location.

The chronological evolution of the use of features helps to understand the beginnings of CA and where we are going. Figure 3 presents the use of raw and derived features chronologically. The first noticeable issue is that CA is quite a novel area of research which started 9 years ago but until 2013 no significant number of works were developed. The use of *motion sensors* and *biosignals* (more precisely, the ECG signal) were pioneer raw features being *motion* used for *touch dynamics* [82, 166]. Years later the use of *environmental* and *position sensors* became much more widespread, also putting the focus on *touch dynamics* [122, 125, 138]. *Mobile device platform information*, specially *touch*, is also used to some extent, e.g. [164], [178] or [44]. However, the use of *body-related data*, biosignals in particular, is experiencing a significant growth and in the last 3 years, in which 6 approaches have been proposed [194][123][42][171][114][40].

4.4 Authentication enforcement

To enforce the authentication process and determine if a user is legitimate or not, choosing the technique and algorithm to apply is the first step (Sections 4.4.1 and 4.4.2). The second step is to choose the computational platform to carry out the process (Section 4.4.3).

4.4.1 Technique selection. The reduced cost of storage devices facilitates the management of huge amounts of data. Moreover, the emergence of the cloud facilitates its storage at a low price or even for free. When there are too much data at stake its management and processing become a hefty task. Data mining tries to relieve this problem. These techniques aim to discover patterns in the analysed data [188].

The most common use of data mining is the processing of data in a batch setting, such that all required training data is available, at the very beginning, as a whole set [34]. This dataset is typically split in two fragments – training samples and testing ones. All approaches, except for [42, 56, 143], focus on CA in IoT applying this technique.

However, it must be recalled that IoT-based CA has two specific issues – authentication is carried out with high frequency and IoT devices are resource constrained. With these requirements in mind, data stream mining techniques are at stake specially if the IoT device aims to be autonomous. They are able to work with streams (i.e. a potentially endless flow of data) investing moderate resources [34]. To achieve this goal, they process every sample just once, keeping a subset of recent ones in memory. They are designed to work in a limited amount of time and are intended to be ready to predict at any time. [42, 56, 143] are the only user-related IoT-based CA approaches which use this technique.

4.4.2 Enforcement algorithm selection. Once features are processed, the next step (recall Figure 2) is the use of an algorithm to determine if a given user is considered legitimate or impostor. In this regard, several options exist and they can be classified as follows:

- *Classification (C)* consists of predicting the right class for a user, that is legitimate or impostor. It can be performed using a supervised or an unsupervised algorithm. In the former case users' data is labeled and the output is already known – the user is either legitimate or impostor. In some way the algorithm is taught about what to learn. By contrast, in unsupervised algorithms the process is more complex because it is unknown if the user should be classified as legitimate or not beforehand. Some of the most common classifiers are the following:
  - Neural Networks (NN) are supervised or unsupervised classifiers composed of artificial neurons interconnected with each other to form a structure that mimics the behavior and neural processing of biological neurons [95]. Input neurons receive authentication features in the input layer and then, data is processed through other neurons either in an output layer or in a hidden one. Indeed, several hidden layers may exist. The output layer

is the one which provides the result – authentication granted or denied. [122] and [187] manage authentication using a classical NN, [15, 187] also work with NN but with multiple layers and [45] uses a variant of multilayer NN which is characterized for being specially appropriate for image processing.

- K-Nearest Neighbours method (K-NN) is a supervised classification algorithm. K-NN has been extensively used. Given an element, it is classified based on the 'k' nearest neighbors ('k' most similar instances) [96]. In other words, predictions for a new instance are made by searching through the entire training set for the 'k' most similar instances and summarizing the output variable for those 'k' instances. In this way, given a new input, it is classified considering the most similar known user. For this purpose, a distance metrics (such as those described in *Instance-Based Learning* below) could be applied. In terms of CA, [42, 69, 127] work with different values of 'k', while [60] fixes 'k'=1, [171] fixes 'k'=4, [104] fixes 'k'=11, [56] fixes 'k' to {3, 10, 21} and [50, 153, 178] do not provide any configuration information.
- Ensemble Learning (EL) combines multiple learning algorithms to perform a better prediction and they can be used in a supervised or unsupervised way [196]. Among existing EL algorithms, bagging and boosting are noticed. Bagging consists of training each classifier on a random redistribution of the training set. Then, it allows these classifiers to vote on a final decision [39]. However, just [114] applies this technique for CA by means of IoT. Otherwise, boosting produces a series of classifiers in which the training set is chosen based on the performance of the earlier classifiers in the series [70]. AdaBoost was the first boosting algorithm developed for binary classification [156] and it is used in [123] for IoT-based CA purposes. Gradient-Boosted Trees are also a common alternative specially appropriate when managing data of mixed type and the need to be robust to outliers. In this latter case they may provide predictions by combining many trees of limited depth preferably. It has also been applied in IoT-based CA [124, 144].
- Decision Trees (DT) are supervised classifiers that solve classification problems using a tree structure. Users are classified as legitimate or impostors by posing a series of questions about their features. Each node contains a question and every internal node points to one child node for each possible answer to the question [101]. Several works in IoT-based CA use an unspecified DT technique [50, 60, 68, 124]. By contrast, [44, 67, 187] mention the use of J48. It is a particular implementation of a DT which produces a high true positive rate [63]. Besides, a well-known type of DT, called Hoeffding tree, is also used in this context [143]. Hoeffding trees are data stream decision trees classifiers which grow the tree based on the Hoeffding bound. This bound quantifies the number of observations needed to estimate some statistics within a prescribed precision. Certain level of confidence is given to the best attribute to split the tree and the model is created based on the number of seen instances [34]. [56] applies Hoeffding trees for IoT-based CA. Another challenging type of DT and extension over bagging, is called Random Forest (RF). It creates a set of decision trees from training data. Then, it aggregates the votes from different DT to decide the final class of the test data item [134]. In IoT-based CA [44, 67, 68, 104, 195] deal with RF.
- Bayesian (BY) are statistical classifiers, commonly used in a supervised manner, that predict class membership based on probabilities [72]. In a nutshell, they compute the likelihood of an element belonging to a class considering how probable it is for each of its individual features. A couple of CA for IoT proposals, developed by Feng et al., apply this classifier [67, 68]. One well-known type of bayesian classifiers is Naive Bayes. It works under the Naive Bayes theorem which assumes that the effect of an attribute value on a given class is independent of other attributes values [107]. This is the case of [50, 56, 106, 194] for IoT-based CA.

  - Support Vector Machines (SVMs) are supervised classifiers which locate each users' data in a n-dimensional space, where n is the number of features and the value of such features linked to each coordinate. They are popular due to their robust mathematical theory. They have been applied in assorted fields from medicine to engineering [135]. Classification looks for finding the hyper-plane that differentiate the two classes (i.e., legitimate users and impostors). They usually perform linear classifications but non-linear ones can also be considered applying a kernel trick [157], which is a mathematical function to simplify the problem. There are different kernel functions, such as the linear, the polynomial, the Gaussian or Radial Basis Function (RBF). Most of approaches working on IoT-based CA use the classical SVM algorithm [28, 60, 84, 106, 111, 114, 117, 138, 168, 189] and from those using a kernel function, the RBF is the most representative one [45, 51, 69, 112, 123, 154, 192, 194] followed by the linear one [75, 116, 123, 164, 171]. By contrast, the use of polynomial [66] kernel is uncommon. Additionally, just [47] proposed the use of a Gaussian RBF kernel for CA by means of IoT and [139] use multiple weak SVM classifiers.
  - Ad-Hoc (AH) classifiers are those specially developed for a particular work. [47] proposed the use of Chebyshev classifier on the bases of Chebyshev's inequality [88], which states that no more than $1/n^2$ of a distribution's values are more than n standard deviations away from the mean. Concerning IoT-based CA, [71] uses a decision fusion classifier composed of several binary classifiers to distinguish between a couple of groups. On the other hand, [106] applies regression for classification purposes.
- *CLustering (CL)* consists of dividing data in homogeneous groups (clusters) such that all data in a cluster is more similar to each other than to others. CL can be considered a form of classification because it creates data with class (cluster) labels [175]. However, for the sake of clarity, we explain them separately. CL algorithms can be hierarchical or partitional. Hierarchical algorithms find successive clusters using previously established clusters, whereas partitional algorithms determine all clusters at a time [133]. Some of the most relevant CL algorithms are the following ones:
  - K-means (KM) is a partitional algorithm that assigns each point to the cluster whose center (centroid) is nearer. To do this, each data point n is assigned to the nearest mean, which can be calculated through the Euclidean distance or any other distance metric (see below *Instance-Based Learning* algorithms). Means are adjusted to match the sample means of the data points that they are responsible for [115]. Although it has not been applied in any of the considered papers, this stands as an interesting choice.
  - Gaussian Mixture Model (GMM) is also a partitional algorithm which assumes that all the data points are generated from a mixture of a finite number of Gaussian distributions (continuous probability distributions) [147]. Therefore, each cluster is formed by those elements that result from the combination of the same distributions.
  - Density-based clustering (D) algorithm [64], which can be partitional or hierarchical, is devised to discover arbitrary-shaped clusters. It focuses on finding a number of clusters regarding an estimation of the density distribution of data. This is the case of [28] which applies density based clusters for CA by means of IoT.
- *Instance-Based Learning (IBL)* consists of determining which user of the training set is closer to the user to authenticate using a distance function [188]. For this purpose, each user is represented by his features, typically expressed in numerical magnitudes. Each feature is thus a point in the potential value space. Using this representation, there are three well-known distance functions. The Euclidean distance is calculated as the length of the line segment connecting a pair of points given by the Pythagorean theorem. The Manhattan distance is the distance between two points in a grid, adding horizontal and vertical items. Finally, the Mahalanobis distance is

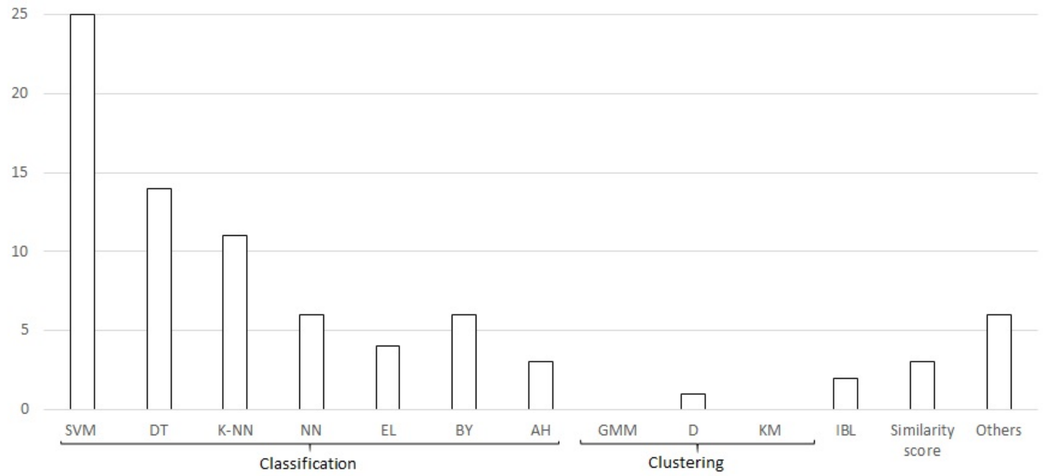


Fig. 4. Amount of papers per enforcement algorithm

used to measure the similarity between two random multidimensional variables. The calculus is similar to the Euclidean distance but considering correlation, that is covariance. A proposal uses the Euclidean distance [151] to continuously authenticate users, while just one uses Mahalanobis distance [82].

- *Similarity score* are approaches that enforce the authentication based on comparing an established value, achieved after some processing, with the test one. One common way is the use of thresholds to discriminate between legitimate users and impostors. This has been used in [126] for IoT-based CA. The sticking point is to set the appropriate threshold. Other possibilities are the development of some ad-hoc techniques, such as the used of correlation matrix [37] or specific functions [108] also applied for IoT-based CA purposes.
- *Others* multiple and assorted algorithms can be applied in the authentication enforcement process. In the considered works, there are some approaches based on ad-hoc procedures [125, 166]. On the other hand, others use novel techniques based on well-known models like the Markov Decision Process [41]. Even a regression algorithm called kernel ridge regression has been used for classification purposes [112]. Last but not least, innovative image processing algorithms have been applied after converting input data into images [198].

As shown in Figure 4, it is noticeable that SVM classifiers stand out over the rest with a total of 25 proposals. DT are also commonly used classifiers and 14 proposals take advantage of them. One of their strengths is that once the tree has been constructed the classification is straightforward. K-NN classifiers are also applied in 12 proposals, being their simplicity an essential characteristic – just a distance is computed to do the classification. It can also be seen that most proposals apply classification approaches and all of them supervised algorithms, which are a nice alternative to simplify the classification process.

In addition to the use of classifiers, 3 and 2 proposals use similarity scores and IBL respectively. These techniques are particularly appropriate when speed is demanding because their enforcement is significantly fast due to their simplicity. For this same reason, they are promising alternatives in devices with constrained resources where complex computations are not feasible.

4.4.3 Platform choice. The enforcement process can be performed in the device that collects the data (typically, the user-related IoT device) or in a third party. In the former case the main advantages are that it is faster (as it avoids transmission time) and it is more secure (in that no trusted third parties are needed). On the other hand, the enforcement of authentication in a third party may benefit from having more computation power in terms of energy, memory or storage. Besides, as the authentication should be continuous, the transmission should be permanent. This not only poses security problems but also increases management complexity since multiple devices are involved.

The resource constraints in wearables and implantable devices (recall Section 4.2) are typically addressed by outsourcing the complex computations to more powerful nodes. Thus, these devices focus on feature acquisition (e.g. [117, 171]), but processing is carried out by a portable device or a cloud-based server (called third party). This is specially remarkable in biosignal processing (e.g. ECG data) in which most papers do not specify where biosignals should be processed (e.g. [42][105]), though it can be assumed that it will be carried out in a third party. Indeed, a total of 21 proposals do the enforcement in a third party, namely a server (e.g. [44][139]), while in 10 of them (e.g. [117][114]) it is assumed but not directly specified. Conversely, 38 proposals enforce authentication in the IoT device that collects applied features, being portable devices (34) the most common ones (e.g. [166][104]), a couple of them do the enforcement in a wearable ([47][124]) and other couple in a device within a vehicle ([66][148]).

4.5 Evaluation analysis

Proposals can be evaluated theoretically, as well as empirically by doing some kind of experimentation. An outstanding CA contribution that aims to be applied in the real world should perform an experimental evaluation considering a particular dataset (Section 4.5.1) and some evaluation metrics (Section 4.5.2). Note that the operating system in which the CA process is carried out is another aspect to consider. However, as 28 proposals apply Android, other 30 do not provide any specification and just [187] develops an iOS application, this issue does not require further study.

4.5.1 Datasets. IoT-based CA proposals, as it commonly happens in other fields, have to be empirically evaluated to verify their feasibility in a real environment. The evaluation involves data developed ad-hoc for a given approach (42 proposals) or used from public sources (14 proposals). Each dataset usually contains data from multiple participants and the number of them could be an indicator of the relevance and adequacy of the dataset. However, in a CA system in which the authentication should be performed in a continuous way for unlimited time (ideally), collecting data in a long period of time is also relevant for the evaluation process.

Table 2 presents the number of participants per dataset (developed or public), together with the amount of time along which features have been collected per participant.

Going a little deeper, most datasets do not detail the time along which features are retrieved. This is important to assess whether the proposed mechanism is suitable for long usage periods. Indeed, just 37.5% of public datasets and 38.1% of the developed ones specify this time. Remarkably, there are some proposals in which developed datasets are created based on data of several months [71, 127], 60-90 minutes [125, 198], 2-6 hours [112, 168] or public databases which present data collected in 24 months [56], 24 hours [42, 105] or 2-6 hours [45, 111]. On the contrary, the rest of works use data collected along several minutes.

In terms of the number of participants to construct the dataset, in percentage (see Figure 5), the most significant amount of proposals, 28.6% of developed datasets involve between 11 and 30 users and the same percentage of public ones involve between 31 and 60 users. There are not public datasets with more than 301 participants. The fact that 7.1%

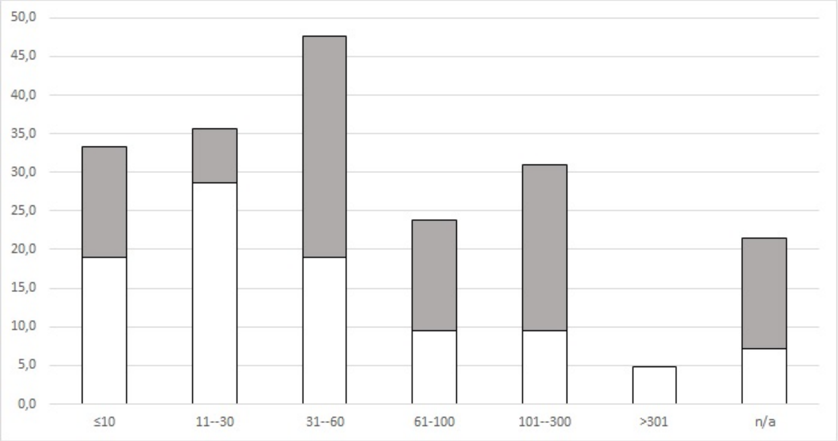


Fig. 5. Distribution (in %) of developed datasets (in white) and public ones (in gray) considering the amount of participants.

and 14.3% of proposals with developed and public datasets respectively do not specify the amount of participants, is an unexpected situation.

Regarding the nature of public datasets, 3 of them contain biomedical data [42, 105, 123], a pair of them touch activity [122, 151], a couple of them data from images [116, 154], motion sensors data [124, 144] , activity from mobile devices [94, 108] and data from smartphones and their sensors [56]. This latter pair use the same dataset that is Massachusetts Institute of Technology (MIT) Reality Dataset[4]. Indeed, 3 proposals [42, 94, 108] use MIT datasets. Moreover, [45, 111] use the dataset developed in [168].

As a final comment, [194] is the only paper which evaluates the proposal without giving details about the nature of the dataset.

Table 2. Dataset analysis. '-' represents an unknown value

	Public		Developed	
Num users	Time	References	Time	References
<=10	32 min.	[124]	18 min.	[60]
	24 hours	[42]	-	[117][143][84][50][187][166][40]
11–30	-	[144]	30 min.	[195]
			15 min.	[82]
			15 min.	[51]
			30-60 min.	[198]
			5-10 days	[44][104]
			-	[47][192][178][142][66][126]
31–60	24 months	[56]	Multiple session 2 hours	[138]
	-	[154][151][116]	2 min.	[37]
			-	[69][164][67][139][106][15]
61-100	2-6 hours	[111][45]	2 min.	[171]
			90 min.	[125]
			2-6 hours	[168][112]
101–300	24 hours	[105]	19 months	[127]
	-	[94][108]	5 months	[71]
				[114][189]
>301	-	-	-	[114][75]
-	-	[123][122]	-	[68][153]
			26 days	[28]

---

[4] http://realitycommons.media.mit.edu/realitymining.html , last access January 2018

Table 3. Evaluation metric analysis

	#	References
Conf. matrix	5	[124][143][166][189][106]
TP	6	[195][42][171][84][66][28]
TN	1	[171]
FP	4	[195][42][66][28]
FN	2	[84][56]
TPR	3	[47][75][116]
FAR	**29**	[138][144][124][123][105][37][117][114][122][94][69][192][51][154][125][164][68][151][198][44][187][67][116][71][126][104][194][112][45]
TAR	3	[51][154][198]
FRR	**26**	[47][144][138][124][123][105][37][117][122][94][69][192][125][164][68][151][44][187][67][127][71][126][104][194][112][45]
ROC	**12**	[114][192][75][51][154][125][164][198][44][126][124][42]
EER	**27**	[47][138][144][124][123][105][171][37][117][114][168][122][94][69][192][125][178][151][198][108][71][153][126][111][112][60][15]
Precision	7	[195][124][42][50][116][189][60]
Recall	5	[124][42][116][189][60]
Accuracy	7	[124][189][139][171][104][45][60]
F-measure	5	[42][171][189][45][60]
Usability	19	[123][50][56][171][94][68][151][198][67] {[66][117][83][143][69][51][153][84][125][126]}*
Energy cons.	9	[195][168][166][66] {[125][108][71][142][138]}*

*Only mentioned. In bold, most used metrics

4.5.2 *Evaluation metrics.* After choosing a dataset, the authentication process is carried out and lastly, the output is analysed to determine the adequacy of the system. To do this, the following evaluation metrics can be used:

- *Confusion matrix* [65] is commonly used to evaluate the classifier performance. It describes how many members of a class have been classified in each of the existing classes. Based on this matrix, four evaluation metrics can be computed:
  - False positive (FP) (respectively, False negative (FN)) is the amount of authenticated users that should be rejected (resp. legitimate) but they were predicted as legitimate (resp. impostors). This affects the security of the system and should be as minimum as possible.
  - True positive (TP) (respectively, True negative (TN)) is the amount of authenticated users that should be legitimate (resp. rejected) and they were predicted as such. The maximization of this ratio is the main goal.
- *Accuracy* [141] is the number of right predictions (i.e.,TP + TN) divided by the total number of authentication decisions. This issue should be maximized.
- *False rejection rate (FRR)* (also called *False Negative Rate (FNR)* or *False Non Match Rate (FNMR)*) [65] is the percentage ratio of the number of legitimate users predicted as impostors against the total number of legitimate user (FN/(FN + TP)).
- *False acceptance rate (FAR)* (also called *False Positive Rate (FPR)* or *False Match Rate (FMR)*) [65] is the percentage ratio of the number of impostors predicted as legitimate users against the total number of impostors (FP/(FP + TN)).
- *Equal Error Rate (EER)* [92] is the point at which the FAR and FRR cross and it is particularly applied in biometric systems. Lower EER means higher system accuracy.
- *True rejection rate (TRR)* is the probability of the system to correctly reject impostors. Ideally this metric should be 100%.
- *True acceptance rate (TAR)* is the probability of the system to correctly identify legitimate users. It should be maximum.

- Receiver Operating Characteristic (ROC) [65] is used to evaluate classifiers output quality. It is represented as a curve, such that FP is located on X-axis and TP on Y-axis. Ideally, the curve should grow towards the top-left meaning that the model does correct predictions. The area under the curve is commonly used as a measure of quality. The area of a perfect classifier tend to be close to 1.
- *Recall* (or Sensitivity) [141] is the proportion of users that are correctly predicted as positives, either being legitimate or not (TP/(TP+FN)). It should be as high as possible trying to maximize TP.
- *Precision* (or Confidence) [141] is the proportion of predicted legitimate users that are correctly real legitimate (TP/(TP+FP)). A balance with Recall should be achieved, again maximizing TP.
- *F-measure* (or F-score) [78] is the harmonic mean (average of ratios, percentages) of precision and recall (2x((precision x recall)/(precision+recall))). It can be considered an alternative to measure accuracy, which should be maximized.
- Usability refers to the simplicity of using the CA system. It is linked to a pair of issues, the minimization of FN and then preventing the system to be blocked unnecessarily; and the minimization of the time the system is blocked unnecessarily.
- Energy consumption consists of studying the use of energy involved in the CA process. In IoT, resource constrained devices are generally applied and energy consumption should be minimum to help maximize the life time of the device.

From all evaluation metrics, FAR, FRR and EER stand out over the rest with 29, 26 and 28 proposals respectively (Table 3). Afterwards, ROC is used in 12 works from which just [124][42][75] consider ROC area. Usability and energy consumption present interesting results. The former is addressed from different perspectives. It has been considered in 6 proposals (e.g. [67], [198]) using metrics such as FAR or FRR. On the other hand, [123][50][56] deal with usability minimizing the blocking time, [66] analyses it based on a survey, [117][83][143][69][51][153] mention it and [84][125][126] point it out as a matter of future work. Similarly, energy consumption is measured in [195][168][166][66], mentioned in [125][108][71][142] and considered as a future issue in [138]. It is also noticed that TRR is not measured in any proposal. On the other hand, [148] does not perform any kind of evaluation, [41] is not focused on the evaluation of the authentication system and [142] only presents a theoretical evaluation.

5 INDUSTRY STATUS: RESEARCH PROJECTS, MARKET PERSPECTIVES AND STANDARDS

The industry has also been involved in developing IoT-based CA products. This matter is studied from the point of view of research projects (Section 5.1), the market (Section 5.2) and existing standards (Section 5.3).

5.1 Research projects analysis

The status of IoT-based CA advances can be also identified in research projects. The first CA project began in 2006, it was called HUMABIO [2] and it was focused on the use of CA in critical environments like laboratories. From then on, looking for CA research projects that can be found in English, 12 have been granted, where the ending date of half of them is between 2018 and 2020 [4–8] and a couple of them have been completed in 2017 [3, 17]. This shows the current interest in the development of CA solutions.

These projects are funded by international and national agencies – 5 of them are granted by the European Union [2, 3, 6, 17, 145] and another 5 by the US National Science Foundation (NSF) [4, 5, 5, 7, 8].

Concerning their goals, Pico [3] is the only project which presents a hardware solution (i.e., a token). It uses short-range radio to authenticate users continuously throughout a session in applications which can be locked or unlocked based on the presence of users' Pico. By contrast, there are projects in which CA is commonly enforced using data collected from wearable devices [2, 4–6]. For instance, [4] leverages multiple sensors embedded in handheld and wearable devices for strong user authentication. It tries to combine data from wearables and cues extracted from the phone itself to continuously and unobtrusively verify the authenticity of the user. Moreover, [8] proposes the use of touches in the screen of mobile devices improving security and usability of authentication, e.g. detecting unauthorized access to a mobile device in a continuous manner. Biosignals and heart rate specially, continues being the most popular one and it is used in [7] for CA purposes. In line with academic research (recall Section 2), *biosignals* and *touch* seem to be promising IoT-based CA features which worth studying.

All projects have to be evaluated according to their goals. However, a usability analysis is essential to prevent the development of approaches that turn out to be unsuitable for the real world. Though all projects are evaluated, [8] is the only one that mentions the need of usability of authentication and [6] goes a step forward pointing out the need of balancing usability, privacy and performance.

5.2 Market perspectives

The benefits of CA have crossed many boundaries and the market has welcome this kind of initiatives. A total of 32 companies have developed a CA product. Most of them do not directly link their products to IoT but they are studied for being CA products which can be used and/or integrated into IoT devices. Table 4 presents companies, name of developed products (if any), CA features and if it is a hardware (HW) or a software (SW) product. In the latter case, it depicts the type and possible devices in which it can be used. Note that x means not addressed and '–' not mentioned.

Very limited information is provided about the insights of the authentication process. This is an expected issue because secrets usually remain hidden for competitive reasons. Companies mention some general features used in the CA process but without going into details. Behavioral analysis is the most common approach, 6 products consider behavioral biometrics and 5 users' behavior. Moreover, *touch* is used in 7 products and *contextual features* in 6. The use of *biosignals* is relevant in 5 products. However, 9 companies do not specify any kind of feature.

Other issue to notice is the fact that most products are software and just [158][132][32][169] offer a hardware solution. The benefit of a software solution is that it does not require the possession of a particular device to do the authentication, thus relieving for the burden of having many gadgets. Besides, they are usually cheaper or there are some parts of the product which can be used for free or for a small amount of money. Likewise, a software can be easily updated through the Internet. On the contrary, a HW solution can be designed with ergonomics in mind, thus potentially leading to higher comfort and usability levels. More importantly, there are features like *biosignals* which should be collected by some kind of HW device, e.g. a wearable [169].

In terms of software products, we can distinguish between those which are a product themselves; or those which are toolsets, e.g. an API, thus used to create a CA solution. A total of 21 companies offer products, while there are 6 which provide a toolset. From those offering a product, most of them present applications for mobile devices [18, 20, 103, 132, 199], and other significant set present software solutions without specification [26, 35, 73, 90, 97, 128, 130, 174]. However, there are 10 software products which do not detail the type of product which is offered and the generic term 'solution' is used instead.

Concerning software products, regardless of the type, they are mostly developed for mobile devices (17 products). Web security is also a concern for several companies, 6 in particular. Nonetheless, it is surprising to identify that 8

Table 4. Market analysis. CA products

			SW	
Product name	**Features**	**HW**	**Type**	**Devices**
[20]	Touch, contextual features	x	Product	Mobile
SensifyID [199]	User behavior, contextual features	x	Product	Web, mobile and sensor devices
Kryptowire's Continuous Authentication [103]	Touch	x	Product	Mobile
[140]	Touch	x	Toolset	-
[35]	Behavioural biometrics	x	Product	-
ThisData Verify API [179]	User behavior		Toolset	-
BehavioSense [33]	User behavior	x	Product	Desktop and mobile
Behavior ID [177]	Touch	x	Toolset	Web and mobile
SecureAuth IdP [158]	Behavioural biometrics	Identity Provider	Product	-
DIGIPASS for Apps Behavioral Authentication [184]	Touch	x	Toolset	Mobile
[159]	Behavioural biometrics	x	Toolset	-
IdentityX [54]	-	x	-	-
NoPassword [130]	Touch, contextual features	x	Product	Mobile, web and desktops (workstations)
[146]	Biosignal, gait, location, biometric traits	-	-	-
OneClick [77]	-	x	Product	Mobile and web
Nymi band, Nymi Companion application [132]	Biosignal	Wearable	Product	Mobile
Aetna mobile app [18]	User behavior	x	Product	Mobile
[181]	Touch	x	Toolset	-
VeridiumID [185]	Behavioural biometrics	x	Product	Mobile
UnifyID [183]		x	Product	Mobile and web
[174]		x	Product	Web
[97]	Biometric traits	x	Product	Mobile and desktop
TickStream.CV [26]	Text properties and more	x	Product	-
[137]	Behavioural biometrics, contextual features	x	-	-
Olea HeartSignature [128]	Biosignal	x	Product	-
Cognitive CA [16]	-	-	-	-
FastAccess and 3DVerify [161]	Biometric trait	-	Product	Mobile and desktop
[74]	-	-	-	-
[32]	Biosignal	Biosensor for wearable and smart devices	-	
biolock [169]	Biosignal	Biosensor emdded into steering wheel and a mobile application	-	-
idNSure [90]	-	x	Product	-
Bitwoke FIDO Authenticator [36]	User behavior	-	-	-

companies do not provide information about devices in which their products can be used. Even worst is the fact that 5 companies do not mention the type of software and the type of device they are offering and a couple of them do not even mention if they offer a hardware or a software product.

5.3 Standards

In the standardisation field, both the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) play a relevant role in the information technology area. ISO/IEC:9798 specifies a family of entity authentication protocols. It consists of five parts, the first one provides background for the other parts (Part1 [10]). Authentication protocols are divided in four parts, protocols using symmetric encryption (Part 2 [11]), those using digital signatures (Part 3 [12]), those using cryptographic check functions such as message authentication codes (Part 4 [13]) and those applying zero-knowledge techniques (Part 5 [14]).

Other standard is ISO/IEC 29115:2013 [9]. It provides a framework for managing entity authentication assurance in a given context. Basically, it presents four levels of assurance, guidelines to reach such levels, as well as guidelines to exchange results of the authentication and others concerning controls to mitigate authentication threats.

More recently, ISO/IEC 17922 [1] describes a telebiometric (remote life measurement) authentication scheme. A biometric hardware security module (BHSM) is used for the telebiometric authentication of a user who has an ITU-T X.509 public key certificate embedded in the BHSM. Then, it presents the requirements to enforce a secure deployment of a BHSM.

Currently under review, ISO/IEC 24761 [182] describes the structure and data of the authentication context for biometrics. It is used for checking the validity of the result of a biometric verification process executed at a remote site.

Despite the existence of several standards related to authentication, CA has been neglected. There is a need for CA standards regarding the development of CA systems which help tackle problems like the following ones:

- How many features should be applied in a CA system? Does it depend on the context (i.e. IoT)?
- What is the amount of EER or FP/TP admissible in a CA system? In this way, what is the max-min time the device should be blocked if the authentication fails and considers a user illegitimate? In this regard, what kind of enforcement algorithms could be applied?
- Trying to reduce usability problems, what should be the highest power consumption of a CA system?

6 LESSONS LEARNED

Based on the performed survey, a set of eight lessons learned can be pointed out. They are intended not only to clarify the main takeaway points for each issue. For the sake of clarity, these lessons are ordered following the general scheme of this paper and not in terms of their relevance.

Lesson 1. CA by means of user-related IoT devices is receiving extensive attention from both industry and academia. The significant amount of papers that have been found, along with the number of market initiatives, highlight the relevance of this research field. According to their distribution in time, these efforts have been constantly supported in almost a decade.

Lesson 2. Academic proposals are largely unlinked to particular scenarios. This trend seems to be natural in immature research areas, in which the foundations are still to be laid. In these cases, theoretical approaches are needed to set the grounds for future developments. However, after the analysis it has become clear that this is not the case of IoT-based CA. There are two facts that support this claim. On the one hand, the said great amount of initiatives point out the maturity of this area. On the other hand, it must be noted that IoT devices have been developed much before the application in CA, and even CA is an evolution of the widely explored matter of authentication. As a result, the degree of theoretical uncertainty is limited.

Lesson 3. Portable devices are preferred. In line with their adoption through time, portable devices, and mobile phones in particular, are the most common IoT devices for CA. When more constrained devices are considered, such as wearable or implantable ones, it is common to rely on third parties (e.g. a powerful server or a cloud-based infrastructure) to carry out the computation, either totally or partially.

Lesson 4. Behavioral biometrics is receiving extensive attention, mainly leveraging biosignals, touch and location data. Most considered papers address one particular form of this branch of biometrics. The generalization of the said sensorial capabilities of IoT devices has enabled this evolution over time. Recalling the previous lesson, it is important to analyse the relationship of devices and features. Table 5 summarizes this analysis. In short, portable devices appear to be the one-for-all solution. This may probably be due to the amount of sensors they have, the facility of their use (e.g. located in our pocket) and its economic price. Wearables (e.g. smart glasses [47]) are also used for collecting multiple raw features specially, but despite the simplicity of their use, the price can be a differentiating factor. Moreover, they typically do not offer as many possibilities as portable devices. On the other hand, the acquisition of body-related data, namely biosignals, is usually achieved by implantable devices. Since these devices may not be accessible to everyone at anytime, the use of wearables could be a nice alternative [40].

Table 5. Devices used to extract each feature

		Portable	Wearables	Implantable	External
RAW	Body-related d.	*x*	√	√	√
	S.Motion	√	√	*x*	*x*
	S.Environmental	√	*x*	*x*	*x*
	S.Position	√	√	*x*	*x*
	Accesories m.d.	√	√	*x*	*x*
DERIVED	Gait	√	*x*	*x*	*x*
	Position in the seat	*x*	*x*	*x*	*x*
	Biometric trait	√	*x*	*x*	*x*
	Touch dynamics	√	√	*x*	*x*
	Location	√	*x*	*x*	*x*
	Text properties	*x*	*x*	*x*	*x*
	Contextial f.	*x*	*x*	*x*	*x*

Lesson 5. Classifiers are by far the preferred technology for authentication enforcement in academia. Since the vast majority of papers consider different variants of existing classifiers, this can be considered as the *de facto* standard in this research area. This evidence seems to favor future developments based on existing techniques, rather than ad-hoc approaches. Apart from this fact, it is interesting to explore the link between features and algorithms to spot open research directions. Table 6 summarizes this analysis. Surprisingly, features *contextual features* and *position in the seat* have not been studied based on any particular algorithm yet. Similarly, other like *environmental sensors* are just applied for K-NN (in stream version) and Others algorithms. By contrast, features like *touch dynamics*, *mobile device information* and *motion sensors* have been studied in regard to most algorithms, namely in 10, 11 and 9 algorithms respectively.

Table 6. Features vs Algorithms

		Classifiers								Clustering					
		NN	K-NN	EL	DT	RF	BY	SVM	AH	KM	GMM	D	IBL	Similarity score	Others
RAW	Body-related d.	*x*	Stream/√	√	*x*	*x*	√	√	*x*	*x*	*x*	*x*	√	√	*x*
	Motion sensors	√	√	√	√	√	√	√	√	*x*	*x*	*x*	*x*	*x*	√
	Environmental sensors	*x*	Stream	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	√
	Position sensors	√	√	*x*	√	*x*	*x*	√	*x*	*x*	*x*	*x*	*x*	*x*	√
	Mobile device platform info	√	√	*x*	Stream/ √	√	√	√	√	*x*	*x*	√	√	√	√
DERIVED	Gait	*x*	*x*	*x*	*x*	*x*	*x*	√	*x*	*x*	*x*	*x*	*x*	*x*	*x*
	Position in the seat	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*
	Biometric trait	*x*	*x*	*x*	*x*	*x*	*x*	√	*x*	*x*	*x*	*x*	*x*	*x*	*x*
	Touch dynamics	√	√	*x*	√	√	√	√	√	*x*	*x*	*x*	√	√	√
	Location	*x*	√	*x*	Stream	*x*	*x*	*x*	√	*x*	*x*	*x*	*x*	*x*	*x*
	Text properties	√	√	*x*	*x*	*x*	*x*	*x*	√	*x*	*x*	*x*	*x*	*x*	*x*
	Contextual f.	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*

Lesson 6. There is a consensus on evaluation metrics. When it comes to assessing research proposals, most authors rely upon a reduced set of metrics – FAR, FRR and EER being the preferred choices.

Lesson 7. Market approaches are prioritizing software products based on similar features to those in academic works. The market analysis has shown a prevalence of software products in detriment of hardware ones. Although this may be caused to the productions costs and pace, this fact can encourage novel investments in hardware-based products. Concerning the set of features for achieving CA, market initiatives are significantly based on different features related to behavioral biometrics. Specifically, both market and academia show the prevalence of *body-related data*, particularly biosignals, and *touch* features. This market-academia alignment may be beneficial to further improve the maturity of this field, since research results are more likely to be transferred to the market. As an example of the benefit of this symbiosis, the work by Nakanishi et al. has pointed out the increased resilience achieved by a multi-device CA technique in vehicles [126]. However, the market has not exploited this direction yet.

Lesson 8. CA standards are lacking. Despite the said connection between academia and market, the lack of standards can become a barrier for the development of this area. In the absence of standards, the lack of best practices and common grounds may contribute to have duplicate efforts, recurring errors and a lack of assessment guidelines.

7 CHALLENGES AND OPEN ISSUES

Many IoT-based CA systems have been developed either in the academy or in the industry. In this regard, challenges to overcome and open issues to address are pointed out herein. They are classified according to those identified along the proposed study and those devised by authors as a consequence of the study.

- **Identified along the study**
  1. **Need of focused proposals**. The development of IoT-based CA approaches used in a general scenario are a nice alternative. However, choosing concrete scenarios is highly recommended because each of them has particular characteristics which prevent the use of a general approach to reach conclusive results. It means that there is a need to consider that the realism of datasets should be as close to reality as possible to avoid deviations from the real world. For instance, touching a mobile phone screen while running, walking or standing, may produce extremely different results. Likewise, the heart rate of a child is not the same as an elderly man. In general, except for [144] in which collected data involves participants carrying out different activities (e.g., walking, jogging, etc.), no dataset considers situations out of a controlled environment. As a side effect, there are some particular scenarios that still remain unexplored. For example, there is not any single proposal focused on healthcare applications.
  2. **Need of lightweight approaches**. IoT devices have intrinsic limitations in terms of battery and storage, though these limitations may differ between devices. A lack of lightweight CA approaches is identified in this regard. This trend is similar to what happened in the early times of smartcards. Thus, this research line may build upon previous cryptographic primitives that were specially developed for those resource-limited devices.
  3. **Release of comprehensive datasets**. Our analysis shows that there is a need of publicly available large-scale datasets, both in terms of users and collection time. In their absence, authors are using small datasets which can be an obstacle for the generalization of the achieved results. In this regard, usability considerations cannot be neglected if public acceptance is a matter for an IoT-based CA approach. In the absence of rich datasets, the analysis of this feature cannot lead to representative conclusions. The same situation happens with energy considerations.

     Completeness of a dataset is defined as being big enough and having data collected from IoT devices of different brands and versions, different operating systems and operating system versions. The size of the dataset is essential to attest the validity of results and specially for CA the bigger the dataset, the better. In the same way, it is possible that IoT devices, either having different brand, version, operating system or operating system version, do not collect exactly the same data. This could affect system parameters or algorithms and thus, impact the success of the CA system.

(4) **Demand of CA standards**. Standards for CA systems have to be developed to help in the specification of parameters and algorithms. This could be the main step to improve these systems and, above all, to simplify their comparison. Indeed, comparisons are essential to choose the best alternative for each scenario.

(5) **Selection of the best blocking strategy against illegitimate users to reach a compromise between security, usability and, in some cases, safety**. In an authentication system the execution of some kind of blocking activity when an impostor is authenticated is mandatory. However, this problem is far from having a trivial solution specially when security, usability or even safety come into play. In case of IoT devices like smartphones, blocking the phone and asking for a password could be the most suitable and common solution but it cannot be applied to all scenarios. For instance, a CA system in a car studies how the legitimate user is sitting but if an illegitimate user is detected while driving, a possible solution is to automatically call the police and/ or the car owner. This issue is commonly left out of the scope in most of proposals but it should be specially considered in those affecting safety, such as [148] in which the driving speed is a feature.

(6) **Deep study of enforcement algorithms**. Currently, K-NN is one of the most used enforcement algorithms but there are others like GMM or KM which are left aside. An analysis of the appropriateness of chosen algorithms for each feature would help researcher on choosing the most suitable algorithm.

- **Devised as a consequence of the study**

(7) **Threats analysis**. Each particular scenario can be affected by a set of threats, even being similar between scenarios. In this way, it is not the same to consider an attacker which tries to impersonate a user trying to create fake features, than considering an attacker that steals the IoT device that collects the CA features. Therefore, building a comprehensive threat taxonomy will be helpful for two reasons. On the one hand, it will help researchers on identifying threats. On the other hand, proposals will be easily comparable as they base on the same underlying model.

(8) **IoT-based CA vs privacy**. The development of usable approaches is a desirable issue and the use of CA is an alternative (recall Section 3). Nonetheless, from a security point of view usability cannot be prior to privacy [49]. There is a gap between the use of IoT-based CA and the privacy issues that could arise. For instance, the GPS data to continuously authenticate a user has already been used but considerations towards privacy problems are not a priority. In this example, if users' positions are somehow discovered by illegitimate users, undesirable causes may occur (e.g. burglaries of houses). Not all IoT-based CA features are privacy-related but an study on this direction would be an interesting way to analyse the usability that CA offers and the security that all systems should provide.

(9) **IoT-based CA in the cloud.** Given resource limitations, namely battery and storage, of IoT devices used for CA, the support of the cloud poses interesting possibilities. There is a limited number of proposals that use the cloud to manage CA (e.g. [47]). Thus, protocols and schemes should be developed to specify how data should be transmitted from the IoT device to the cloud and vice versa, as well as how data has to be processed either in the IoT device or in the cloud. For instance, [79] proposes a framework for securely and privately outsourcing continuous authentication to a server based on touch data. This paper could be considered an initial step in this regard.

(10) **Enhancement of CA systems in smartphones and capacity of data collection in wearables. The development of CA systems** should go towards the enhancement of CA approaches for smartphones because they are well-known and worldwide used. Moreover, the industry should work towards the improvement of the capacity of data collection in wearables. Biosignals in particular are interesting CA features but only a portion of wearables are able to retrieve these signals.

(11) **Prevention and analysis of injection attacks in IoT devices**. Researchers and developers rely on IoT devices as trusted sources to collect data. What could happen if sources are attacked? If collected data is not as accurate as expected, an illegitimate user could be authenticated as the legitimate one. For instance, in a CA system based on the gyroscope, if this sensor is attacked and manipulated to provide fake data, access could be illegitimately granted. Some study mentions the problem of injection attacks in sensors, e.g. in a particular type of accelerometers [180], but there is a growing need of research in this direction. Indeed, it is close to a family of techniques called adversarial machine learning [87], which have not been explored in the context of IoT yet.

(12) **Selection of the optimal set of features according to the risk level posed by the attacker**. There are many different features but not all of them can be attacked in the same way. Expectedly, higher risk is relegated to those features which are easier targets in a given scenario. For instance, it is presumably easier to create a malicious WiFi access point than attacking the gyroscope of a smartphone. Thus, prior to the selection of features, the risk to use one or another should be evaluated. Specifically, a study presenting a general overview of this challenge remains as an open issue.

(13) **Dynamic CA systems resilient to environmental and/ or context changes**. There are features which are collected in cooperation with a third element, e.g. WiFi or GPS. The unavailability of these elements for a period of time should be managed. For example, if a user is continuously authenticated considering the WiFi signal strength/direction (among other features), and the connection is lost at some point in time, the authentication process should be able to manage the situation. Some authentication works introduce the idea of dynamism, e.g. the login identifier changes each time [55], but they are neither focused on IoT nor on CA.

(14) **Privacy-preserving trust management of IoT data sources**. Current IoT-based CA approaches rely upon a single device to provide data. However, if the device is compromised or malfunctioning, the whole CA enforcement can be put at risk. Given the great amount of IoT devices, the consistency of the provided data by one of them can be confronted with information coming from anothers. Despite the existing venues for future research on this matter [193], managing trust in the context of CA may raise additional privacy concerns if data from other subjects comes into play. Therefore, it is necessary to research on trust management mechanisms that are privacy-respectful.

Figure 6 summarizes open issues and challenges related to steps of the design process of a IoT-based CA system. For instance, in the 'enforcement step' the use of *lightweight approaches* should be considered and/ or developed. Other example is the *selection of the optimal set of features according to the risk level posed by the attacker*, which should be carried out in line with the 'feature selection' step. Note that the *demand of CA standards* is transversal because such standards should be developed regardless of the steps of a CA system.

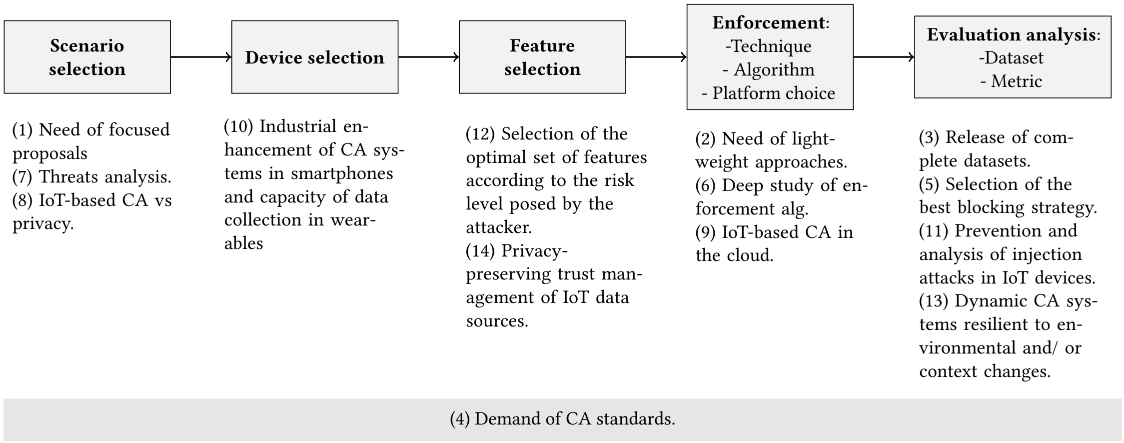


Fig. 6. Open issues and challenges in regard to the design process of an IoT-based CA approach

8 RELATED WORK

The novelty of this proposal is studied by comparison against surveys focused on IoT security and surveys focused on IoT-based CA. Table 7 presents a summary.

First of all, security in IoT has been studied to some extent specially since 2015. Most proposals devote some attention to authentication (√), discussing some issues in this regard, while four of them mention authentication but very superficially (√*). Surprisingly, [53] does not even mention authentication and none of the proposals refers to CA. Besides, authentication is studied for multiple purposes. There are authentication protocols such as [23], which introduces authentication to describe the IEEE 802.15.4 protocol. It is used to define the operation of low-rate wireless personal area networks. Authentication has also been considered in Wireless sensor networks (WSN) [197], sensors distributed to monitor phisical and environmental conditions and authentication is mandatory to regulate access to collected data; and Radio Frequency Identification (RFID) [38, 118], a technology to identify objects located at a certain distance without direct contact. RFID tags are specially well-known for this purpose. Indeed, [150] refers to authentication in IoT entities like servers or clients and just [76] and [193] use the term user authentication, which is what we consider herein.

Moving towards IoT-based CA proposals, half of them focus on mobile devices [136, 155, 176]. [155, 163] are short papers which try to provide a general overview about continuous authentication, being [155] specially focused on mobile devices. Also presenting a quite general approach [172] introduces the title of CA approaches and features applied. However, it is not directly related to IoT, it works on behavioral biometrics. Also indirectly related to IoT, [21, 22] put the focus on multibiometric authentication, introducing briefly features, datasets and evaluation metrics. A final remark refers to the number of studied works. [21, 22, 136, 172] study 29, 28, 30 and 29 works respectively but more proposals have already been developed and not exclusively for mobile devices. Similarly, [176] studies 47 proposals but, apart from being exclusively focused on touch dynamics, its focus is not CA.

9 CONCLUSIONS

We are surrounded by technology which connects to the Internet, called Internet-of-Things (IoT). The widespread adoption of IoT and the fact that users commonly use user-related IoT devices everywhere and everytime, encourage the

Table 7. Related work summary

IoT security surveys				
Title	Year	Authentication	CA	Authentication purpose
An overview of privacy and security issues in the internet of things [118]	2010	√	*x*	RFID
Security in the Internet of Things: A Review [173]	2012	√*	*x*	Protocol
A survey on the internet of things security [197]	2013	√	*x*	WSN
On the features and challenges of security and privacy in distributed internet of things [150]	2013	√	*x*	IoT entities
A survey on trust management for Internet of Things [193]	2014	√*	*x*	User and IoT devices
Internet of things: A survey on enabling technologies, protocols, and applications [23]	2015	√	*x*	Protocol
Security for the internet of things: a survey of existing protocols and open research issues [80]	2015	√	*x*	Protocol
Survey of security and privacy issues of Internet of Things [38]	2015	√	*x*	RFID
Security and Privacy Challenges in Industrial Internet of Things [152]	2015	√*	*x*	WSN
Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things [85]	2015	√	*x*	IoT device
Smart Cities: A Survey on Data Management, Security, and Enabling Technologies [76]	2017	√*	*x*	Users
Internet of Things: Survey on Security and Privacy [119]	2017	√	*x*	Protocol
Smart secure homes: a survey of smart home technologies that sense, assess, and respond to security threats [53]	2017	X	*x*	*x*
Internet of things Security: A Survey [24]	2017	√	*x*	IoT device
Internet of Things: A survey on the security of IoT frameworks [25]	2018	√	*x*	IoT device

CA IoT surveys			
Title	Year	Description	# studied works
A Survey of Continuous and Transparent Multibiometric Authentication Systems [21]	2015	It presents an analysis of works related to continuous and multibiometric authentication but they are not really focused on IoT. It also depicts and introduces very briefly features, datasets and evaluation metrics.	29
Continuous and transparent multimodal authentication: reviewing the state of the art [22]	2016	It describes authentication methods and technologies to afterwards present a review of existing continuous and transparent multimodal authentication approaches. In these CA approches evaluation metrics, number of participants in the evaluation, applied features and devices are mentioned.	28
Expanding continuous authentication with mobile devices [155]	2015	It simply mentions the good point of continuous authentication, specially in mobile devices.	Short paper
A Review of Continuous Authentication Using Behavioral Biometrics [172]	2016	It presents a general overvire of continuous authentication approaches introducing their title and features involved. It is not specially focused on IoT but in CA through behavioral biometrics.	30
Continuous user authentication on mobile devices: Recent progress and remaining challenges [136]	2016	It focuses on continuous authentication approaches in mobile devices paying attention to the type of used classifier, features and performance rate, including the evaluation metric.	29
A survey on touch dynamics authentication in mobile devices [176]	2016	It presents a timeline of touch dynamics, algorithms applied, used datasets and main evaluation metrics.	47
Continuous Authentication and Authorization for the Internet of Things [163]	2017	It mentions some continuous authentication features. It does not really perform an analysis of existing works because it is a short paper.	Short paper

use of IoT for authentication purposes. In particular, the authentication of users persistently, which is called Continuous Authentication (CA), relieves the problem of being impersonated at any time. This paper presents a comprehensive study of IoT-based CA from the academic and industrial point of view. To the best of the authors knowledge, all academic proposals up to now (58 in total) are studied regarding steps of the authentication process. Likewise, the industry status is considered in terms of existing research projects, the market (32 products in total) and developed standards. From the analysis a set of open issues and weaknesses to address in future works are outlined.

In summary, this survey seeks to help researches and practitioners in the development of new solutions having a holistic view about the current status of IoT-based CA developments, which is a current and dynamic area.

ACKNOWLEDGEMENTS

This work was supported by the MINECO grant TIN2016-79095-C2-2-R (SMOG-DEV) and by the CAM grants S2013/ICE-3095 (CIBERDINE) and P2018/TCS4566 (CYNAMON-CM) both co-funded with European FEDER funds.

REFERENCES

[1] ISO/IEC 17922. 2017. Security techniques – Telebiometric authentication framework using biometric hardware security module. https://www.iso.org/standard/61023.html. (2017). Last access Feb. 2018.

[2] Sixth Framework Programme (FP6). STREP Specific Targeted Research Project 2006-2008. [n. d.]. HUMABIO (HUman Monitoring and Authentication using Biodynamic Indicators and behaviOural Analysis). http://www.humabio-eu.org/. ([n. d.]). Last access Feb. 2018.

[3] Seventh Framework Programme (FP7). ERC-SG ERC Starting Grant 2013-2017. [n. d.]. Pico: no more passwords. http://mypico.org/. ([n. d.]). Last access Feb. 2018.

[4] National Science Foundation (NSF) 2015-2018. [n. d.]. Spoof-Resistant Smartphone Authentication using Cooperating Wearables. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1527795&HistoricalAwards=false. ([n. d.]). Last access Feb. 2018.

[5] National Science Foundation (NSF) 2016-2019. [n. d.]. Continuous Human-User Authentication by Induced Procedural Visual-Motor Biometrics. https://nsf.gov/awardsearch/showAward?AWD_ID=1718116&HistoricalAwards=false. ([n. d.]). Last access Feb. 2018.

[6] Horizon 2020 Innovation Framework Programme. MSCA-ITN-ETN European Training Networks 2017-2020. [n. d.]. AMBER - enhAnced Mobile BiomEtRics. https://www.amber-biometrics.eu/. ([n. d.]). Last access Feb. 2018.

[7] National Science Foundation (NSF) 2017-2020. [n. d.]. Cardiac Password: Exploring a Non-Contact and Continuous Approach to Secure User Authentication. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1718483&HistoricalAwards=false. ([n. d.]). Last access Feb. 2018.

[8] National Science Foundation (NSF) 2017-2020. [n. d.]. Implicit One-handed Mobile User Authentication by Induced Thumb Biometrics on Touch-screen Handheld Devices. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1704800&HistoricalAwards=false. ([n. d.]). Last access Feb. 2018.

[9] ISO/IEC 29115. 2013. Security techniques – Entity authentication assurance framework. https://www.iso.org/standard/45138.html. (2013). Last access Feb. 2018.

[10] ISO/IEC 9798-1. 2010. Entity authentication – Part 1: General. https://www.iso.org/standard/53634.html. (2010). Last access Feb. 2018.

[11] ISO/IEC 9798-2. 2008. Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms. https://www.iso.org/standard/50522.html. (2008). Last access Feb. 2018.

[12] ISO/IEC 9798-3. 2017. Entity authentication – Part 3: Mechanisms using digital signature techniques. https://www.iso.org/standard/67115.html. (2017). Last access Feb. 2018.

[13] ISO/IEC 9798-4. 1999. Entity authentication – Part 4: Mechanisms using a cryptographic check function. https://www.iso.org/standard/31488.html. (1999). Last access Feb. 2018.

[14] ISO/IEC 9798-5. 2009. Entity authentication – Part 5: Mechanisms using zero-knowledge techniques. https://www.iso.org/standard/50456.html. (2009). Last access Feb. 2018.

[15] A. Acar, H. Aksu, A. S. Uluagac, and K. Akkaya. 2018. WACA: Wearable-Assisted Continuous Authentication. In *2018 IEEE Security and Privacy Workshops (SPW)*. 264–269.

[16] Acceptto. [n. d.]. First Cognitive Continuous Authentication. https://www.acceptto.com/continuous-authentication.html. ([n. d.]). Last access Feb. 2018.

[17] Horizon 2020 Innovation Framework Programme. Innovation action 2015-2017. [n. d.]. Face and body Analysis Natural Computer Interaction (FANCI). http://cordis.europa.eu/project/rcn/85410_en.html. ([n. d.]). Last access Feb. 2018.

[18] Aetna. [n. d.]. Next Generation Authentication. https://news.aetna.com/2017/08/aetnas-next-generation-authentication/. ([n. d.]). Last access Feb. 2018.

[19] Ahmed Awad E Ahmed and Issa Traoré. 2012. Performance Metrics and Models for Continuous Authentication Systems. In *Continuous Authentication Using Biometrics: Data, Models, and Metrics*. IGI Global, 23–39.

[20] aimbrain. [n. d.]. Improve your user experience with continuous authentication. https://aimbrain.com/step-up-authentication-process/. ([n. d.]). Last access Feb. 2018.

[21] Abdulwahid Al Abdulwahid, Nathan Clarke, Ingo Stengel, Steven Furnell, and Christoph Reich. 2015. A survey of continuous and transparent multibiometric authentication systems. In *Proceedings of the 14th European Conference on Cyber Warfare and Security*. 1–10.

[22] Abdulwahid Al Abdulwahid, Nathan Clarke, Ingo Stengel, Steven Furnell, and Christoph Reich. 2016. Continuous and transparent multimodal authentication: reviewing the state of the art. *Cluster Computing* 19, 1 (2016), 455–474.

[23] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials* 17, 4 (2015), 2347–2376.

[24] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi. 2017. Internet of things Security: A Survey. *Journal of Network and Computer Applications* (2017).

[25] Mahmoud Ammar, Giovanni Russello, and Bruno Crispo. 2018. Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications* 38 (2018), 8–27.

[26] Intensity analytics. [n. d.]. TickStream.CV. http://intensityanalytics.com/products/tickstream.cv.aspx. ([n. d.]). Last access Feb. 2018.

[27] Android. [n. d.]. Sensors Overview (Android developers). https://developer.android.com/guide/topics/sensors/sensors_overview.html. ([n. d.]). [Online; accessed December-2017].

[28] Fazel Anjomshoa, Moayad Aloqaily, Burak Kantarci, Melike Erol-Kantarci, and Stephanie Schuckers. 2017. Social behaviometrics for personalized devices in the internet of things era. *IEEE Access* 5 (2017), 12199–12213.

[29] Juan Sebastian Arteaga-Falconi, Hussein Al Osman, and Abdulmotaleb El Saddik. 2016. ECG authentication for mobile devices. *IEEE Transactions on Instrumentation and Measurement* 65, 3 (2016), 591–600.

[30] Luigi Atzori, Antonio Iera, and Giacomo Morabito. 2010. The Internet of Things: A survey. *Computer Networks* 54, 15 (2010), 2787 – 2805. https://doi.org/10.1016/j.comnet.2010.05.010

[31] Shu-Di Bao, Yuan-Ting Zhang, and Lian-Feng Shen. 2005. Physiological signal based entity authentication for body area sensor networks and mobile healthcare systems. In *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the*. IEEE, 2455–2458.

[32] BEAT4KEY. [n. d.]. Embedded biometrics. http://www.beat4key.com/products/. ([n. d.]). Last access Feb. 2018.

[33] BehavioSec. [n. d.]. Continuous Authentication with Passive Behavioral Biometrics. https://www.behaviosec.com/. ([n. d.]). Last access Feb. 2018.

[34] Albert Bifet and Richard Kirkby. 2009. Data stream mining a practical approach. (2009).

[35] Biocatch. [n. d.]. Less friction. Less fraud. https://www.biocatch.com/. ([n. d.]). Last access Feb. 2018.

[36] Bitwoke. [n. d.]. Secure A.I. based edge analytics powering smart connected devices. https://www.bitwoke.com/. ([n. d.]). Last access Feb. 2018.

[37] Angelo Bonissi, Ruggero Donida Labati, Luca Perico, Roberto Sassi, Fabio Scotti, and Luca Sparagino. 2013. A preliminary study on continuous authentication methods for photoplethysmographic biometrics. In *Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2013 IEEE Workshop on*. IEEE, 28–33.

[38] Tuhin Borgohain, Uday Kumar, and Sugata Sanyal. 2015. Survey of security and privacy issues of Internet of Things. *arXiv preprint arXiv:1501.02211* (2015).

[39] Leo Breiman. 1996. Bagging predictors. *Machine learning* 24, 2 (1996), 123–140.

[40] J David Brown, William Pase, Chris McKenzie, Mazda Salmanian, and Helen Tang. 2017. A Prototype Implementation of Continuous Authentication for Tactical Applications. In *Ad Hoc Networks*. Springer, 342–353.

[41] Arun Balaji Buduru and Stephen S Yau. 2015. An effective approach to continuous user authentication for touch screen smart devices. In *Software Quality, Reliability and Security (QRS), 2015 IEEE International Conference on*. IEEE, 219–226.

[42] Carmen Camara, Pedro Peris-Lopez, Lorena Gonzalez-Manzano, and Juan Tapiador. 2017. Real-time electrocardiogram streams for continuous authentication. *Applied Soft Computing* (2017).

[43] Carmen Camara, Pedro Peris-Lopez, and Juan E Tapiador. 2015. Security and privacy issues in implantable medical devices: A comprehensive survey. *Journal of biomedical informatics* 55 (2015), 272–289.

[44] Gerardo Canfora, Paolo Di Notte, Francesco Mercaldo, and Corrado Aaron Visaggio. 2016. Silent and Continuous Authentication in Mobile Environment.. In *SECRYPT*. 97–108.

[45] Mario Parreño Centeno, Yu Guan, and Aad van Moorsel. 2018. Mobile Based Continuous Authentication Using Deep Features. *2nd International Workshop on Embedded and Mobile Deep Learning* (2018).

[46] PEW Research Center. [n. d.]. Mobile Fact Sheet. http://www.pewinternet.org/fact-sheet/mobile/. ([n. d.]). [Online; accessed Sep-2018].

[47] Jagmohan Chauhan, Hassan Jameel Asghar, Anirban Mahanti, and Mohamed Ali Kaafar. 2016. Gesture-Based Continuous Authentication for Wearable Devices: The Smart Glasses Use Case. In *International Conference on Applied Cryptography and Network Security*. Springer, 648–665.

[48] Roger Clarke. 1994. Human identification in information systems: Management challenges and public policy issues. *Information Technology & People* 7, 4 (1994), 6–37.

[49] Lorrie Faith Cranor and Norbou Buchler. 2014. Better together: Usability and security go hand in hand. *IEEE Security & Privacy* 12, 6 (2014), 89–93.

[50] Heather Crawford, Karen Renaud, and Tim Storer. 2013. A framework for continuous, transparent mobile device authentication. *Computers & Security* 39 (2013), 127–136.

[51] David Crouse, Hu Han, Deepak Chandra, Brandon Barbello, and Anil K Jain. 2015. Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data. In *Biometrics (ICB), 2015 International Conference on*. IEEE, 135–142.

[52] Li Da Xu, Wu He, and Shancang Li. 2014. Internet of things in industries: A survey. *IEEE Transactions on industrial informatics* 10, 4 (2014), 2233–2243.

[53] Jessamyn Dahmen, Diane J Cook, Xiaobo Wang, and Wang Honglei. 2017. Smart secure homes: a survey of smart home technologies that sense, assess, and respond to security threats. *Journal of Reliable Intelligent Environments* (2017), 1–16.

[54] Daon. [n. d.]. Join our ecosystem. https://www.daon.com/company/join-our-ecosystem. ([n. d.]). Last access Feb. 2018.

[55] Manik Lal Das, Ashutosh Saxena, and Ved P Gulati. 2004. A dynamic ID-based remote user authentication scheme. *IEEE transactions on Consumer Electronics* 50, 2 (2004), 629–631.

[56] Jose Maria de Fuentes, Lorena Gonzalez-Manzano, and Arturo Ribagorda. 2018. Secure and Usable User-in-a-Context Continuous Authentication in Smartphones Leveraging Non-Assisted Sensors. *Sensors* 18, 4 (2018), 1219.

[57] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. 2012. Touch me once and i know it's you!: implicit authentication based on touch screen patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 987–996.

[58] Michael P Down and RJ Sands. 2004. Biometrics: An overview of the technology, challenges and control considerations. *Information Systems Control Journal* 4 (2004), 53–56.

[59] Sergio Roberto de Lima e Silva, Mauro Roisenberg, et al. 2006. Continuous authentication by keystroke dynamics using committee machines. In *International Conference on Intelligence and Security Informatics*. Springer, 686–687.

[60] Muhammad Ehatisham-ul Haq, Muhammad Awais Azam, Usman Naeem, Yasar Amin, and Jonathan Loo. 2018. Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing. *Journal of Network and Computer Applications* 109 (2018), 24–35.

[61] Saad El Jaouhari, Ahmed Bouabdallah, Jean-Marie Bonnin, and Tayeb Lemlouma. 2017. Toward a Smart Health-care Architecture Using WebRTC and WoT. In *World Conference on Information Systems and Technologies*. Springer, 531–540.

[62] Mehdia Ajana El Khaddar and Mohammed Boulmalf. 2017. Smartphone: the ultimate IoT and IoE device. In *Smartphones from an Applied Research Perspective*. InTech.

[63] Arihito Endo, Takeo Shibata, and Hiroshi Tanaka. 2008. Comparison of Seven Algorithms to Predict Breast Cancer Survival (< Special Issue> Contribution to 21 Century Intelligent Technologies and Bioinformatics). *International Journal of Biomedical Soft Computing and Human Sciences: the official journal of the Biomedical Fuzzy Systems Association* 13, 2 (2008), 11–16.

[64] Martin Ester, Hans-Peter Kriegel, Jörg Sander, Xiaowei Xu, et al. 1996. A density-based algorithm for discovering clusters in large spatial databases with noise.. In *Kdd*, Vol. 96. 226–231.

[65] Tom Fawcett. 2006. An introduction to ROC analysis. *Pattern recognition letters* 27, 8 (2006), 861–874.

[66] Huan Feng, Kassem Fawaz, and Kang G Shin. 2017. Continuous Authentication for Voice Assistants. *arXiv preprint arXiv:1701.04507* (2017).

[67] Tao Feng, Ziyi Liu, Kyeong-An Kwon, Weidong Shi, Bogdan Carbunar, Yifei Jiang, and Nhung Nguyen. 2012. Continuous mobile authentication using touchscreen gestures. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*. IEEE, 451–456.

[68] Tao Feng, Xi Zhao, Bogdan Carbunar, and Weidong Shi. 2013. Continuous mobile authentication using virtual key typing biometrics. In *Trust, security and privacy in computing and communications (TrustCom), 2013 12th IEEE international conference on*. IEEE, 1547–1552.

[69] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. 2013. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security* 8, 1 (2013), 136–148.

[70] Yoav Freund, Robert E Schapire, et al. 1996. Experiments with a new boosting algorithm. In *Icml*, Vol. 96. 148–156.

[71] Lex Fridman, Steven Weber, Rachel Greenstadt, and Moshe Kam. 2016. Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS location. *IEEE Systems Journal* (2016).

[72] Nir Friedman, Dan Geiger, and Moises Goldszmidt. 1997. Bayesian network classifiers. *Machine learning* 29, 2-3 (1997), 131–163.

[73] fusionpipe. [n. d.]. Optiimize end user convenience without copromising security. https://fusionpipe.com/quikid. ([n. d.]). Last access Feb. 2018.

[74] Futurae. [n. d.]. Authentication Suite. https://futurae.com/product/. ([n. d.]). Last access Feb. 2018.

[75] Hugo Gascon, Sebastian Uellenbeck, Christopher Wolf, and Konrad Rieck. 2014. Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior.. In *Sicherheit*. 1–12.

[76] Ammar Gharaibeh, Mohammad A Salahuddin, Sayed Jahed Hussini, Abdallah Khreishah, Issa Khalil, Mohsen Guizani, and Ala Al-Fuqaha. 2017. Smart Cities: A Survey on Data Management, Security, and Enabling Technologies. *IEEE Communications Surveys & Tutorials* 19, 4 (2017), 2456–2501.

[77] IDEE GmbH. [n. d.]. There is only one you. https://getidee.com/. ([n. d.]). Last access Feb. 2018.

[78] Cyril Goutte and Eric Gaussier. 2005. A probabilistic interpretation of precision, recall and F-score, with implication for evaluation.. In *ECIR*, Vol. 5. Springer, 345–359.

[79] Sathya Govindarajan, Paolo Gasti, and Kiran S Balagani. 2013. Secure privacy-preserving protocols for outsourcing continuous authentication of smartphone users with touch data. In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on*. IEEE, 1–8.

[80] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva. 2015. Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials* 17, 3 (2015), 1294–1312.

[81] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems* 29, 7 (2013), 1645–1660.

[82] Mouhcine Guennoun, Najoua Abbad, Jonas Talom, Sk Md Mizanur Rahman, and Khalil El-Khatib. 2009. Continuous authentication by electrocardiogram data. In *Science and Technology for Humanity (TIC-STH), 2009 IEEE Toronto international conference*. IEEE, 40–42.

[83] Kashif Habib, Arild Torjusen, and Wolfgang Leister. 2014. A novel authentication framework based on bio-metric and radio fingerprinting for the IoT in eHealth. In *Proceedings of International Conference on Smart Systems, Devices and Technologies (SMART)*. 32–37.

[84] Christian Holz and Marius Knaust. 2015. Biometric touch sensing: Seamlessly augmenting each touch with continuous authentication. In *Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology*. ACM, 303–312.

[85] Md Mahmud Hossain, Maziar Fotouhi, and Ragib Hasan. 2015. Towards an analysis of security issues, challenges, and open problems in the internet of things. In *Services (SERVICES), 2015 IEEE World Congress on*. IEEE, 21–28.

[86] Vincent C Hu, David Ferraiolo, Rick Kuhn, Arthur R Friedman, Alan J Lang, Margaret M Cogdell, Adam Schnitzer, Kenneth Sandlin, Robert Miller, Karen Scarfone, et al. 2013. Guide to attribute based access control (ABAC) definition and considerations (draft). *NIST special publication* 800, 162 (2013).

[87] Ling Huang, Anthony D Joseph, Blaine Nelson, Benjamin IP Rubinstein, and JD Tygar. 2011. Adversarial machine learning. In *Proceedings of the 4th ACM workshop on Security and artificial intelligence*. ACM, 43–58.

[88] Peter J Huber. 1967. The behavior of maximum likelihood estimates under nonstandard conditions. In *Proceedings of the fifth Berkeley symposium on mathematical statistics and probability*, Vol. 1. Berkeley, CA, 221–233.

[89] SCB Intelligence. 2008. Six technologies with potential impacts on US interests out to 2025. *National Intelligent Concil, Tech. Rep* (2008).

[90] InterDigital. [n. d.]. idNSure. http://www.interdigital.com/solution/idnsure. ([n. d.]). Last access Feb. 2018.

[91] Lijun Jiang and Weizhi Meng. 2017. Smartphone User Authentication Using Touch Dynamics in the Big Data Era: Challenges and Opportunities. In *Biometric Security and Privacy*. Springer, 163–178.

[92] Biing-Hwang Juang, Wu Hou, and Chin-Hui Lee. 1997. Minimum classification error rate methods for speech recognition. *IEEE Transactions on Speech and Audio processing* 5, 3 (1997), 257–265.

[93] Eugenijus Kaniusas. 2012. Fundamentals of biosignals. In *Biomedical Signals and Sensors I*. Springer, 1–26.

[94] Sevasti Karatzouni. 2014. Non-Intrusive Continuous User Authentication for Mobile Devices. (2014).

[95] Apostolos Katidiotis, Kostas Tsagkaris, and Panagiotis Demestichas. 2010. Performance evaluation of artificial neural network-based learning schemes for cognitive radio systems. *Computers & Electrical Engineering* 36, 3 (2010), 518–535.

[96] James M Keller, Michael R Gray, and James A Givens. 1985. A fuzzy k-nearest neighbor algorithm. *IEEE transactions on systems, man, and cybernetics* 4 (1985), 580–585.

[97] KeyLemon. [n. d.]. Oasis Faces. Mobile banking. https://www.keylemon.com/. ([n. d.]). Last access Feb. 2018.

[98] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan. 2012. Future internet: the internet of things architecture, possible applications and key challenges. In *Frontiers of Information Technology (FIT), 2012 10th International Conference on*. IEEE, 257–260.

[99] Kalevi Kilkki, Martti Mäntylä, Kimmo Karhu, Heikki Hämmäinen, and Heikki Ailisto. 2017. A disruption framework. *Technological Forecasting and Social Change* (2017).

[100] Jaeho Kim and Jang-Won Lee. 2014. OpenIoT: An open service framework for the Internet of Things. In *Internet of Things (WF-IoT), 2014 IEEE World Forum on*. IEEE, 89–93.

[101] Carl Kingsford and Steven L Salzberg. 2008. What are decision trees? *Nature biotechnology* 26, 9 (2008), 1011–1013.

[102] Andrew J Klosterman and Gregory R Ganger. 2000. *Secure continuous biometric-enhanced authentication*. Technical Report. CARNEGIE-MELLON UNIV PITTSBURGH PA DEPT OF COMPUTER SCIENCE.

[103] kryptowire. [n. d.]. Continuous Authentication. https://www.kryptowire.com/continuous-authentication.php. ([n. d.]). Last access Feb. 2018.

[104] Rajesh Kumar, Vir V Phoha, and Abdul Serwadda. 2016. Continuous authentication of smartphone users by fusing typing, swiping, and phone movement patterns. In *Biometrics Theory, Applications and Systems (BTAS), 2016 IEEE 8th International Conference on*. IEEE, 1–8.

[105] Ruggero Donida Labati, Roberto Sassi, and Fabio Scotti. 2013. ECG biometric recognition: Permanence analysis of QRS signals for 24 hours continuous authentication. In *Information Forensics and Security (WIFS), 2013 IEEE International Workshop on*. IEEE, 31–36.

[106] Wei-Han Lee and Ruby B Lee. 2017. Implicit Smartphone User Authentication with Sensors and Contextual Machine Learning. In *Dependable Systems and Networks (DSN), 2017 47th Annual IEEE/IFIP International Conference on*. IEEE, 297–308.

[107] K Ming Leung. 2007. Naive bayesian classifier. *Polytechnic University Department of Computer Science/Finance and Risk Engineering* (2007).

[108] Fudong Li, Nathan Clarke, Maria Papadaki, and Paul Dowland. 2011. Behaviour profiling for transparent authentication for mobile devices. In *European Conference on Cyber Warfare and Security*. Academic Conferences International Limited, 307.

[109] Shancang Li and Li Da Xu. 2017. *Securing the internet of things*. Syngress.

[110] Shancang Li, Li Da Xu, and Shanshan Zhao. 2018. 5G internet of things: A survey. *Journal of Industrial Information Integration* 10 (2018), 1–9.

[111] Yantao Li, Hailong Hu, and Gang Zhou. 2018. Using Data Augmentation in Continuous Authentication on Smartphones. *IEEE Internet of Things Journal* (2018).

[112] Yantao Li, Hailong Hu, Gang Zhou, and Shaojiang Deng. 2018. Sensor-based Continuous Authentication Using Cost-Effective Kernel Ridge Regression. *IEEE Access* (2018).

[113] Fei Liu, Chee-Wee Tan, Eric TK Lim, and Ben Choi. 2017. Traversing knowledge networks: an algorithmic historiography of extant literature on the Internet of Things (IoT). *Journal of Management Analytics* 4, 1 (2017), 3–34.

[114] Wael Louis, Majid Komeili, and Dimitrios Hatzinakos. 2016. Continuous Authentication Using One-Dimensional Multi-Resolution Local Binary Patterns (1DMRLBP) in ECG Biometrics. *IEEE Transactions on Information Forensics and Security* 11, 12 (2016), 2818–2832.

[115] David MacKay. 2003. An example inference task: clustering. *Information theory, inference and learning algorithms* 20 (2003), 284–292.

[116] Upal Mahbub, Vishal M Patel, Deepak Chandra, Brandon Barbello, and Rama Chellappa. 2016. Partial face detection for continuous authentication. In *Image Processing (ICIP), 2016 IEEE International Conference on*. IEEE, 2991–2995.

[117] Yasuo Matsuyama, Michitaro Shozawa, and Ryota Yokote. 2015. Brain signal's low-frequency fits the continuous authentication. *Neurocomputing* 164 (2015), 137–143.

[118] Carlo Maria Medaglia and Alexandru Serbanati. 2010. An overview of privacy and security issues in the internet of things. In *The Internet of Things*. Springer, 389–395.

[119] Diego M Mendez, Ioannis Papapanagiotou, and Baijian Yang. 2017. Internet of things: Survey on security and privacy. *arXiv preprint arXiv:1707.01879* (2017).

[120] Michael Miller. 2015. *The Internet of things: How smart TVs, smart cars, smart homes, and smart cities are changing the world*. Pearson Education.

[121] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. 2012. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks* 10, 7 (2012), 1497–1516.

[122] Soumik Mondal and Patrick Bours. 2015. Continuous authentication and identification for mobile devices: Combining security and forensics. In *Information Forensics and Security (WIFS), 2015 IEEE International Workshop on*. IEEE, 1–6.

[123] Arsalan Mosenia, Susmita Sur-Kolay, Anand Raghunathan, and Niraj K Jha. 2017. CABA: Continuous authentication based on BioAura. *IEEE Trans. Comput.* 66, 5 (2017), 759–772.

[124] Tamalika Mukherjee. 2017. *An Approach to Software Development for Continuous Authentication of Smart Wearable Device Users*. Ph.D. Dissertation. Arizona State University.

[125] Rahul Murmuria, Angelos Stavrou, Daniel Barbará, and Dan Fleck. 2015. Continuous authentication on mobile devices using power consumption, touch gestures and physical movement of users. In *International Workshop on Recent Advances in Intrusion Detection*. Springer, 405–424.

[126] Isao Nakanishi, Sadanao Baba, Koutaro Ozaki, and Shigang Li. 2013. Using brain waves as transparent biometrics for on-demand driver authentication. *International journal of biometrics* 5, 3-4 (2013), 288–305.

[127] Tempestt J Neal, Damon L Woodard, and Aaron D Striegel. 2015. Mobile device application, Bluetooth, and Wi-Fi usage data as behavioral biometric traits. In *Biometrics Theory, Applications and Systems (BTAS), 2015 IEEE 7th International Conference on*. IEEE, 1–6.

[128] OLEA Sensor Networks. [n. d.]. Olea HeartSignature. http://www.oleasys.com/heartsignature. ([n. d.]). Last access Feb. 2018.

[129] B Clifford Neuman and Theodore Ts'o. 1994. Kerberos: An authentication service for computer networks. *IEEE Communications magazine* 32, 9 (1994), 33–38.

[130] NoPassword. [n. d.]. Authentication. https://www2.nopassword.com/authentication/. ([n. d.]). Last access Feb. 2018.

[131] Symantec Norton. [n. d.]. What is The Internet of Things (IoT)? https://us.norton.com/internetsecurity-iot.html. ([n. d.]). [Online; accessed Sep-2018].

[132] nymi. [n. d.]. The nymi ecosystem. https://downloads.nymi.com/sdkDoc/doc-v3.1.5.326-326_5df03a4/index.html#introduction. ([n. d.]). Last access Feb. 2018.

[133] Mahamed GH Omran, Andries P Engelbrecht, and Ayed Salman. 2007. An overview of clustering methods. *Intelligent Data Analysis* 11, 6 (2007), 583–605.

[134] Mahesh Pal. 2005. Random forest classifier for remote sensing classification. *International Journal of Remote Sensing* 26, 1 (2005), 217–222.

[135] Krupal S Parikh and Trupti P Shah. 2016. Support Vector Machine–A Large Margin Classifier to Diagnose Skin Illnesses. *Procedia Technology* 23 (2016), 369–375.

[136] Vishal M Patel, Rama Chellappa, Deepak Chandra, and Brandon Barbello. 2016. Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine* 33, 4 (2016), 49–61.

[137] Eleven Paths. [n. d.]. Centralized Access Control Solution. https://www.elevenpaths.com/solutions/smart-web-access/index.html. ([n. d.]). Last access Feb. 2018.

[138] Ge Peng, Gang Zhou, David T Nguyen, Xin Qi, Qing Yang, and Shuangquan Wang. 2017. Continuous Authentication With Touch Behavioral Biometrics and Voice on Wearable Glasses. *IEEE Transactions on Human-Machine Systems* 47, 3 (2017), 404–416.

[139] Duong-Tien Phan, Nhan Nguyen-Trong Dam, Minh-Phuc Nguyen, Minh-Triet Tran, and Toan-Thinh Truong. 2015. Smart Kiosk with Gait-Based Continuous Authentication. In *International Conference on Distributed, Ambient, and Pervasive Interactions*. Springer, 188–200.

[140] Plurilock. [n. d.]. Continuous proof of presence. https://www.plurilock.com/. ([n. d.]). Last access Feb. 2018.

[141] David Martin Powers. 2011. Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation. (2011).

[142] Uthpala Subodhani Premarathne. 2015. Reliable context-aware multi-attribute continuous authentication framework for secure energy utilization management in smart homes. *Energy* 93 (2015), 1210–1221.

[143] Davy Preuveneers and Wouter Joosen. 2015. SmartAuth: dynamic context fingerprinting for continuous user authentication. In *Proceedings of the 30th Annual ACM Symposium on Applied Computing*. ACM, 2185–2191.

[144] Davy Preuveneers, Wouter Joosen, et al. 2017. Improving Resilience of Behaviometric Based Continuous Authentication with Multiple Accelerometers. In *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 473–485.

[145] Seventh Framework Programme (FP7). Collaborative project 2008-2011. [n. d.]. Unobtrusive authentication using activity related and soft biometrics (ACTIBIO). http://cordis.europa.eu/project/rcn/85410_en.html. ([n. d.]). Last access Feb. 2018.

[146] Qualcomm. [n. d.]. Security and privacy vision. https://www.qualcomm.com/invention/cognitive-technologies/security-privacy-vision. ([n. d.]). Last access Feb. 2018.

[147] Carl Edward Rasmussen. 2000. The infinite Gaussian mixture model. In *Advances in neural information processing systems*. 554–560.

[148] Andreas Riener. 2012. Sitting postures and electrocardiograms: a method for continuous and non-disruptive driver authentication. In *Continuous Authentication Using Biometrics: Data, Models, and Metrics*. IGI Global, 137–168.

[149] Rosslin John Robles and Tai-hoon Kim. 2010. Applications, Systems and Methods in Smart Home Technology: A. *Int. Journal of Advanced Science And Technology* 15 (2010).

[150] Rodrigo Roman, Jianying Zhou, and Javier Lopez. 2013. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks* 57, 10 (2013), 2266–2279.

[151] Aditi Roy, Tzipora Halevi, and Nasir Memon. 2015. An HMM-based multi-sensor approach for continuous mobile authentication. In *Military Communications Conference, MILCOM 2015-2015 IEEE*. IEEE, 1311–1316.

[152] Ahmad-Reza Sadeghi, Christian Wachsmann, and Michael Waidner. 2015. Security and privacy challenges in industrial internet of things. In *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE*. IEEE, 1–6.

[153] Hataichanok Saevanee, Nathan Clarke, Steven Furnell, and Valerio Biscione. 2014. Text-based active authentication for mobile devices. In *IFIP International Information Security Conference*. Springer, 99–112.

[154] Pouya Samangouei, Vishal M Patel, and Rama Chellappa. 2015. Attribute-based continuous user authentication on mobile devices. In *Biometrics Theory, Applications and Systems (BTAS), 2015 IEEE 7th International Conference on*. IEEE, 1–8.

[155] Kim B Schaffer. 2015. Expanding continuous authentication with mobile devices. *Computer* 48, 11 (2015), 92–95.

[156] Robert E Schapire. 2013. Explaining adaboost. In *Empirical inference*. Springer, 37–52.

[157] Bernhard Schölkopf. 2001. The kernel trick for distances. In *Advances in neural information processing systems*. 301–307.

[158] Secureauth. [n. d.]. Go Beyond Two-Factor Authentication. https://www.secureauth.com/. ([n. d.]). Last access Feb. 2018.

[159] securedtouch. [n. d.]. Behevioral biometrics. https://securedtouch.com/behavioral-biometrics/. ([n. d.]). Last access Feb. 2018.

[160] IBM security. 2018. Future of Identity Study. (2018).

[161] SensibleVision. [n. d.]. Innovation for real-world users. http://www.sensiblevision.com/en-us/about/aboutus.aspx. ([n. d.]). Last access Feb. 2018.

[162] Hossein Shafagh, Anwar Hithnawi, and Simon Duquennoy. 2017. Towards Blockchain-based Auditable Storage and Sharing of IoT Data. *arXiv preprint arXiv:1705.08230* (2017).

[163] Muhammad Shahzad and Munindar P Singh. 2017. Continuous Authentication and Authorization for the Internet of Things. *IEEE Internet Computing* 21, 2 (2017), 86–90.

[164] Chao Shen, Yong Zhang, Zhongmin Cai, Tianwen Yu, and Xiaohong Guan. 2015. Touch-interaction behavior for continuous user authentication on smartphones. In *Biometrics (ICB), 2015 International Conference on*. IEEE, 157–162.

[165] SJ Shepherd. 1995. Continuous authentication by analysis of keyboard typing characteristics. (1995).

[166] Weidong Shi, Jun Yang, Yifei Jiang, Feng Yang, and Yingen Xiong. 2011. Senguard: Passive user identification on smartphones using multiple sensors. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2011 IEEE 7th International Conference on*. IEEE, 141–148.

[167] Terence Sim, Sheng Zhang, Rajkumar Janakiraman, and Sandeep Kumar. 2007. Continuous verification using multimodal biometrics. *IEEE transactions on pattern analysis and machine intelligence* 29, 4 (2007), 687–700.

[168] Zdeňka Sitová, Jaroslav Šeděnka, Qing Yang, Ge Peng, Gang Zhou, Paolo Gasti, and Kiran S Balagani. 2016. HMOG: New behavioral biometric features for continuous authentication of smartphone users. *IEEE Transactions on Information Forensics and Security* 11, 5 (2016), 877–892.

[169] softserve. [n. d.]. Meet biolock: smart biometrics for tomorrow. https://www.softserveinc.com/en-us/tech/blogs/biolock-smart-identity-authentication/. ([n. d.]). Last access Feb. 2018.

[170] Agusti Solanas, Constantinos Patsakis, Mauro Conti, Ioannis S Vlachos, Victoria Ramos, Francisco Falcone, Octavian Postolache, Pablo A Pérez-Martínez, Roberto Di Pietro, Despina N Perrea, et al. 2014. Smart health: a context-aware health paradigm within smart cities. *IEEE Communications Magazine* 52, 8 (2014), 74–81.

[171] Chen Song, Feng Lin, Yan Zhuang, Wenyao Xu, Changzhi Li, and Kui Ren. 2017. Cardiac Scan: A Non-Contact and Continuous Heart-Based User Authentication System. (2017).

[172] Ioannis C Stylios, Olga Thanou, Iosif Androulidakis, and Elena Zaitseva. 2016. A Review of Continuous Authentication Using Behavioral Biometrics. In *Proceedings of the SouthEast European Design Automation, Computer Engineering, Computer Networks and Social Media Conference*. ACM, 72–79.

[173] Hui Suo, Jiafu Wan, Caifeng Zou, and Jianqi Liu. 2012. Security in the internet of things: a review. In *Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on*, Vol. 3. IEEE, 648–651.

[174] Symantec. [n. d.]. Consumer Multi-Factor Authentication Solutions. https://www.symantec.com/theme/multi-factor-authentication-solutions. ([n. d.]). Last access Feb. 2018.

[175] Pang-Ning Tan, Michael Steinbach, Vipin Kumar, et al. 2006. Cluster analysis: basic concepts and algorithms. *Introduction to data mining* 8 (2006), 487–568.

[176] Pin Shen Teh, Ning Zhang, Andrew Beng Jin Teoh, and Ke Chen. 2016. A survey on touch dynamics authentication in mobile devices. *Computers & Security* 59 (2016), 210–235.

[177] TeleSign. [n. d.]. TeleSign targets account takeover fraud with behavioral biometrics technology. https://www.telesign.com/blog/post/telesign-targets-account-takeover-fraud-with-behavioral-biometrics-technology/. ([n. d.]). Last access Feb. 2018.

[178] Marlies Temper, Simon Tjoa, and Manfred Kaiser. 2015. Touch to Authenticate—Continuous Biometric Authentication on Mobile Devices. In *Software Security and Assurance (ICSSA), International Conference on*. IEEE, 30–35.

[179] ThisData. [n. d.]. Use our security APIs to make risk based decisions in your applications. https://thisdata.com/. ([n. d.]). Last access Feb. 2018.

[180] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu. 2017. WALNUT: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks. In *Security and Privacy (EuroS&P), 2017 IEEE European Symposium on*. IEEE, 3–18.

[181] typingdna. [n. d.]. Typing biometrics authentication API based on keystroke dynamics. https://www.typingdna.com/authentication-api.html. ([n. d.]). Last access Feb. 2018.

[182] ISO/IEC 24761 (under review). 2009. Security techniques – Authentication context for biometrics. https://www.iso.org/standard/41531.html. (2009). Last access Feb. 2018.

[183] UnifyID. [n. d.]. Join our team. https://unify.id/desginer-application.html. ([n. d.]). Last access Feb. 2018.

[184] vasco. [n. d.]. Behevioral biometrics. https://www.vasco.com/products/application-security/behavioral-authentication.html. ([n. d.]). Last access Feb. 2018.

[185] Veridium. [n. d.]. Behavioral Biometrics: Continuous Authentication. https://www.veridiumid.com/blog/behavioral-biometrics-continuous-authentication/. ([n. d.]). Last access Feb. 2018.

[186] Ovidiu Vermesan, Markus Eisenhauer, H Sunmaeker, Patrick Guillemin, Martin Serrano, Elias Z Tragos, Javier Valino, A van der Wees, A Gluhak, and R Bahr. 2017. Internet of Things Cognitive Transformation Technology Research Trends and Applications. *Cognitive Hyperconnected Digital Transformation; Vermesan, O., Bacquet, J., Eds* (2017), 17–95.

[187] Yuji Watanabe, Tsutomu Fujita, et al. 2013. Toward Introduction of Immunity-based Model to Continuous Behavior-based User Authentication on Smart Phone. *Procedia Computer Science* 22 (2013), 1319–1327.

[188] Ian H Witten, Eibe Frank, Mark A Hall, and Christopher J Pal. 2016. *Data Mining: Practical machine learning tools and techniques*. Morgan Kaufmann.

[189] Jain-Shing Wu, Wan-Ching Lin, Chih-Ta Lin, and Te-En Wei. 2015. Smartphone continuous authentication based on keystroke and gesture profiling. In *Security Technology (ICCST), 2015 International Carnahan Conference on*. IEEE, 191–197.

[190] Miao Wu, Ting-Jie Lu, Fei-Yang Ling, Jing Sun, and Hui-Ying Du. 2010. Research on the architecture of Internet of things. In *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, Vol. 5. IEEE, V5–484.

[191] Boyi Xu, Lida Xu, Hongming Cai, Lihong Jiang, Yang Luo, and Yizhi Gu. 2017. The design of an m-Health monitoring system based on a cloud computing platform. *Enterprise Information Systems* 11, 1 (2017), 17–36.

[192] Hui Xu, Yangfan Zhou, and Michael R Lyu. 2014. Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones. In *Symposium On Usable Privacy and Security, SOUPS*, Vol. 14. 187–198.

[193] Zheng Yan, Peng Zhang, and Athanasios V Vasilakos. 2014. A survey on trust management for Internet of Things. *Journal of network and computer applications* 42 (2014), 120–134.

[194] Kuo-Hui Yeh, Chunhua Su, Wayne Chiu, and Lu Zhou. 2018. I Walk, Therefore I Am: Continuous User Authentication with Plantar Biometrics. *IEEE Communications Magazine* 56, 2 (2018), 150–157.

[195] Yunze Zeng, Amit Pande, Jindan Zhu, and Prasant Mohapatra. 2017. WearIA: Wearable Device Implicit Authentication based on Activity Information. (2017).

[196] Cha Zhang and Yunqian Ma. 2012. *Ensemble machine learning: methods and applications*. Springer.

[197] Kai Zhao and Lina Ge. 2013. A survey on the internet of things security. In *Computational Intelligence and Security (CIS), 2013 9th International Conference on*. IEEE, 663–667.

[198] Xi Zhao, Tao Feng, and Weidong Shi. 2013. Continuous mobile authentication using a novel graphic touch gesture feature. In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on*. IEEE, 1–6.

[199] zighra. [n. d.]. Smart identity defense. https://zighra.com/. ([n. d.]). Last access Feb. 2018.

Table 1. Analysis of academic approaches (Part 1)

			Features		Enforcement		Evaluation				
Cite	**Year**	**Device**	Raw	Derived	Algorithm	Own Device (OD)/ Third Party (TP)	Developed (D)/ Public (P)	# participants	Data length	Metric	**Operating system**
[47]	2016	Wearable (Smart glasses)	Touch	Touch dynamics	SVM (gaussian RBF kernel) , AH(Chebyshev classifier pero developed by them)	OD (wearable)	D	30	-	TPR, FPR, EER	Android
[138]	2017	Wearable (Smart glasses)	Touch, accelerometer, gyroscope, magnetometer, microphone, s. motion, s. position	Touch dynamics	SVM	TP (computer)	D	32	Multiple session 2h	FAR, FRR, EER, energy consumption for future work	Android
[195]	2017	Werable sensors	Accelerometer, s. motion		RF	TP (smartphone, collect data through wearable)	D	30	30min	TP, FP, precision, energy consumption	Android
[144]	2017	Wearable device not specified	Accelerometers, s. motion		EL (Boosting)	TP assumed but not mentioned	P (REALD-ISP benchmark dataset)	17		FAR, FRR, EER	-
[124]	2017	Wearable device not specified	Accelerometer, gyroscope, s. motion		EL (Boosting)	OD (wearable)	P (Pervasive Systems Research Group's (PSRG) Sensor Activity Dataset)	10	32min	EER, area ROC, precision, recall, accuracy, confusion matrix, FAR, FRR	Android
[123]	2017	Warable sensors	Physiological data (bio signal)		SVM (linear and RDF kernel), EL (Boosting)	TP (server)	P (MIMICII)	Not specified	Entired stay	FAR, FRR, EER, Usability (FAW, FRW)	-
[105]	2013	Implantable (holder)	Physiological data (bio signal)		-	TP assumed but not mentioned	P (E-HOL-03-0202-003 Intercity Digital Electrocardiogram Alliance -IDEAL database)	185	24h	FAR, FRR, EER	-
[42]	2017	Mention IoT device but not specified	Physiological data (bio signal)		Stream K-NN	TP assumed but not mentioned	P (MIT-BIH Normal Sinus Rhythm Database)	10	24h	TP, FP, Precision, Recall, f-measure, ROC area	-
[171]	2017	External device (non-contact radar)	Physiological data (bio signal)		SVM(linear kernel), K-NN	TP assumed but not mentioned	D	78	2min	TP, TN, EER, F-measure, Balanced accuracy (BAC), usability	Android
[37]	2013	-	Physiological data (PPG bio signal)		Similarity score	TP assumed but not mentioned	D	44	2min	FAR, FRR, EER	-
[117]	2015	Wearable sensors	Near-infrared spectroscopy (NIRS) signals		SVM	TP assumed but not mentioned	D	10	-	FAR, FRR, EER	-
[82]	2009	Wearable sensors	Physiological data (ECG bio signal)		IBL	TP assumed but not mentioned	D	16	15min	Usability just mentioned very briefly	-
[83]	2014	Wearable sensors	Physiological data (ECG bio signal and blood pressure)		Similarity score	TP (portable device and server)		-	-	Usability mentioned but not really measured	-
[114]	2016	-	Physiological data (ECG bio signal)		EL (Bagging)	TP assumed but not mentioned	D	1012, 290	-	FAR, FRR, EER, ROC	Android
[168]	2016	Portable (mobile device)	Accelerometer, gyroscope, s. motion	Touch dynamics	SVM	OD (portable device)	D	100	2-6h	EER, energy consumption	Android
[143]	2015	Portable (mobile device)	Wifi, Cell, GPS, device model, language, screen size		Data stream DT	OD (portable device)	D	6	-	Confusion matrix. Usability mentioned	-
[84]	2015	Portable (mobile device)	Physiological data (bio signal)	Touch dynamics	SVM	OD (portable device)	D	10	-	TP, FN, usability for future work	Windows
[122]	2015	Portable (mobile device)	Actions, orientation, bio signals, s. position	Touch dynamics	NN , SVM	OD (portable device)	P (Publicly available swipe gesture dataset)	Nos specified	-	FAR, FRR, EER	Android
[94]	2014	Portable (mobile device)	Calls, SMS, Application usage		-	OD (portable device)	P (MIT Reality Dataset)	106		FAR, FRR, EER, usability through FAR and FRR	-
[69]	2013	Portable (mobile device)	Touch	Touch dynamics	K-NN , SVM (RBF function)	OD (portable device)	D	41	-	FAR, FRR, EER, usability mentioned	Android
[192]	2014	Portable (mobile device)	Touch	Touch dynamics	SVM (RBF kernel)	OD (portable device)	D	30	1month	FAR, FRR, EER, ROC	Android
[75]	2014	Portable (mobile device)	Touch	Touch dynamics	SVM (linear kernel)	OD (portable device)	D	315	-	TPR, FPR, ROC, ROC area	Android
[51]	2015	Portable (mobile device)	Gyroscope, accelerometer, magnetometer, s.motion, s. position	Biometric feature	SVM (RBF kernel)	OD (portable device)	D	24	15min	FAR, TAR, ROC, usability mentioned	Android
[154]	2015	Portable (mobile device)		Biometric feature	SVM (RBF kernel)	OD (portable device)	P (PubFig dataset)	152, 50		FAR, TAR, ROC	-
[125]	2015	Portable (mobile device)	Power consumption, touch, accelerometer, gyroscope, magnetometer, barometer, photometer, calls, actions, s. motion, s. position, s. environmental	Touch dynamics	Others (StrOUD)	OD (portable device)	D	73	90min	FAR,FRR, ROC,EER, usability for future work, energy consumption mentioned not measured	Android
[50]	2013	Portable (mobile device)	Touch, microphone	Touch dynamics	K-NN , DT , BY	OD (portable device)	D	2	-	Precision, usability	-
[189]	2015	Portable (mobile device)	Touch, accelerometer, gyroscope, s. motion	Touch dynamics	SVM	OD (portable device)	D	150	-	Coonfusion matrix, recall, accuracy, precision, F-measure	Android

Table 2. Analysis of academic approaches (Part 2)

			Features		**Enforcement**		**Evaluation**				
Cite	**Year**	**Device**	Raw	Derived	Algorithm	Own Device (OD)/ Third Party (TP)	Developed (D)/ Public (P)	# participants	Data length	Metric	**Operating system**
[164]	2015	Portable (mobile device)	Touch	Touch dynamics	SVM (linear kernel)	OD (portable device)	D	51	-	FAR, FRR, ROC	Android
[178]	2015	Portable (mobile device)	Touch	Touch dynamics	K-NN	OD (portable device)	D	22	-	EER	Android
[68]	2013	Portable (mobile device)	Touch	Touch dynamics	DT , RF , BY	OD (portable device)	D	Nos specified	-	FAR, FRR, usability through FAR y FRR	Android
[151]	2015	Portable (mobile device)	Touch	Touch dynamics	IBL	OD (portable device)	P (Dataset of [69])	42	-	FAR, FRR, EER, Usability measured in terms of FRR	Android
[198]	2013	Portable (mobile device)	Touch	Touch dynamics	Others (Image processing)	OD (portable device)	D	30	30-60min	FAR, TAR, ROC, usability measured through EER	Android
[44]	2016	Portable (mobile device)	Touch, orientation, cell, s. position	Touch dynamics	DT , RF	TP (server)	D	21	10days	FAR, FRR, ROC	Android
[187]	2013	Portable (mobile device)	Touch, accelerometer, s. motion	Touch dynamics	DT , NN	OD (portable device)	D	5	-	FAR, FRR	iOS, Android
[67]	2012	Portable (mobile device)	Touch	Touch dynamics	DT , RF , BY	OD (portable device)	D	40	-	FAR, FRR, usability through FAR y FRR	Android
[116]	2016	Portable (mobile device)	Camera	Biometric feature	SVM (linear kernel)	OD (portable device)	P (Active Authentication Dataset (AA-01))	50	-	TPR, FPR, FAR precision, recall	-
[41]	2015	Portable (mobile device)	Touch	Touch dynamics	Others (Markov decision process)	OD (portable device)		-		Evaluation of the proposed system but not the authentication itself	-
[108]	2011	Portable (mobile device)	Application usage, calls, touch		Similarity score	OD (portable device)	P (MIT Reality dataset)	106	-	EER, energy consumption mentioned	-
[127]	2015	Portable (mobile device)	Application usage, bluetooth, Wi-Fi		K-NN	OD (portable device)	D	200	19months	FRR	-
[71]	2016	Portable (mobile device)	Touch, application usage, GPS	Text properties	AH(DF)	OD (portable device)	D	200	5months	FAR, FRR, EER, energy consumption mentioned	Android
[166]	2011	Portable (mobile device)	Touch, accelerometer, microphone, s. motion	Touch dynamics	Others (Space-time multi-modality)	OD (portable device)	D	7	-	Confusion matrix, energy consumption measured	Linux (Nokia mobile)
[153]	2014	Portable (mobile device)	Touch, caller/receiver data	Text properties, touch dynamics, location	K-NN , NN	OD (portable device)	D	Nos specified	-	EER, usability mentioned	-
[139]	2015	Portable (mobile device)	Accelerometer, gravity sensor, gyroscope, rotational sensors, s. motion	Gait	SVM	TP (server)	D	38	-	Accuracy	Android
[142]	2015	Portable (mobile device)		Location	-	TP (server)	D	18	-	Theoretical, energy consumption mentioned	-
[66]	2017	Portable (mobile device)	Accelerometer, microphone, s. motion		SVM (polinomial kernel)	OD (vehicle)	D	18	-	Usability through a survey energy consumption (of the wearable), TP, FP	-
[148]	2012	Portable (mobile device)	GPS, bio signal, barometer, speed, s. environmental	Position in seat, Driving speed		OD (vehicle)		-	-		-
[126]	2013	Mention devied but not specified	Physiological data (bio signal)		Similarity score	TP assumed but not mentioned	D	23	-	Usability for future, FRR, FAR, ROC, EER	-
[28]	2017	Portable (mobile device)	Wifi, application usage, location		SVM, D	TP (server)	D	-	26 days	TP, FP	Android
[106]	2017	Portable (mobile device)	S. motion		SVM, BY(naive bayes), AH. (Linear regresion, Kernel ridge regression)	TP (server)	D	35	-	Confusion matrix	Android
[104]	2016	Portable (mobile device)	S. motion, touch		K-NN, RF	OD (portable device)	D	28	7 days	FRR, FAR, accuracy	Android
[40]	2017	Werable (bracelet)	Physiological data (bio signal)		-	OD (portable device)	D	2	-	-	Android
[56]	2018	Portable (mobile device)	Power consumption, s. environmental, transmitted data		Stream K-NN	OD (portable device)	Sherlock DB (http://bigdata.ise.bgu.ac.il/sherlock/#/dataset)	50	24 months	FN, usability	-
[194]	2018	Wearable (shoes)	Anatomical data (plantar pressure)		SVM (gaussian RBF kernel), BY(naive bayes),	TP (computer)	-	-	-	FAR, FRR	-
[111]	2018	Portable (mobile device)	Gyroscope, accelerometer, s.motion		SVM	OD (portable device)	P [168]	100	2-6hours	EER	-
[112]	2018	Portable (mobile device)	Gyroscope, accelerometer, magnetometer, s.motion, s. position		SVM (gaussian RBF kernel), Others	OD (portable device)	D	100	2-6hours	FAR, FRR, EER	-
[45]	2018	Portable (mobile device)	Gyroscope, accelerometer, magnetometer, s.motion, s. position		SVM (gaussian RBF kernel), NN	OD (portable device)	P [168]	100	2-6hours	FAR, FRR, Accuracy, F-measure	-
[60]	2018	Portable (mobile device)	Gyroscope, accelerometer, magnetometer, s.motion, s. position		K-NN, SVM, DT	OD (portable device)	D	10	18min	Accuracy, precision, recall, f-measure, EER	-
[15]	2018	Wearable (any, e.g. smartwatch)	Gyroscope, accelerometer, s.motion		NN	TP (computer)	D	34	-	EER	-