Context awareness in biometric systems and methods: State of the art and future scenarios

Context Awareness in Biometric Systems and Methods: State of the Art and Future Scenarios

Michele Nappi, Stefano Ricciardi, Massimo Tistarelli

Abstract - In the last decade, research in biometrics has been focused on augmenting the algorithmic performance to address a growing range of applications, not limited to person authentication/recognition. The concept of context awareness emerged as a possible key-factor for both performance optimization and operational adaptation of the capture, extraction, matching and decision stages. This may be particularly effective for multi-biometrics systems. The knowledge of the context in which a task is being performed, may provide useful information to the system in several manners. For example, it may allow to adapt to a specific environmental condition, such as shadow or light exposure. On the other hand, it may be possible to select the best available algorithm, among a given set, to address the task at hand, which best performs within the given context. This paper aims to provide an overall vision of the main contributions available so far in the field of context-aware biometric systems and methods. The survey is not confined to a particular biometric modality or processing stage, but rather spans the state of the art of several biometric modalities and approaches. A taxonomy of context-aware biometric systems and methods is also proposed, along with a comparison of their features, goals and performances. The analysis will be complemented with a critical analysis of the state of the art and suggesting some future application scenarios.

Keywords: Biometric systems, context-awareness, context-adaptive biometrics, state of the art survey

1 Introduction

In In the last two decades, biometric systems and methods have been applied to a wide range of application domains.

This resulted in a vast corpus of research topics, ranging from the study of new modalities (physical, behavioral or a combination of both) to performance improvements. This trend affected each of the main computational stages of a biometric system, including uncontrolled capture conditions or the presence of malicious attacks. Regardless of the topic considered, it is worth noting that even the most effective method or the best performing modality, may not be the most suited for a particular context. Therefore, the high variability of the real world requires a corresponding versatility of an automatic biometric recognition system. This can be achieved by purposively choosing the best performing algorithmic solution for a given context. Throughout the paper, the term "context" is to be considered in the widest sense, encompassing all kind of variables (environmental and operational conditions, type of usage, sensor efficiency, motion, etc.) which may have an impact on the application at hand. For example, context awareness may allow a biometric system to trust more the response of those modules which have been tested as best performing under the same context.

Context-awareness and context-aware systems have been extensively described in literature. However, the application to biometrics have been explored only in recent years. According to [1] "*a system is context-aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task*". This concept of context-awareness is often closely related to other issues like *responsiveness* [2], *adaptivity* [3], *reactivity* [4] and *context-sensitiveness* [5]. All these issues imply the capability of detecting the context and of modifying the operation based on that context to achieve the best performance. Considering the current biometric technologies, this may be implemented in several ways. For example, designing a biometric recognition system capable of dynamically selecting the optimal feature extraction method for a given data capturing condition. Another potential implementation of context awareness is to select the best suited feature matching method, balancing speed versus accuracy, according to the operational

- *M. Nappi is with the Department of Informatics, University of Salerno, Fisciano SA, 84084, Italy. E-mail: mnappi@unisa.it*
- *M. Nixon is with the School of Electronics and Computer Science., University of Southampton, Southampton SO17 1BJ, United Kingdom. E-mail: msn@ecs.soton.ac.uk*
- *S. Ricciardi is with the Department of Biosciences, University of Molise, Pesche IS, 84084, Italy. E-mail: stefano.ricciardi@unimol.it*
- *M. Tistarelli is with the Computer Vision Laboratory, University of Sassari, Alghero SS, 07041, Italy, tista@uniss.it*

requirements (high security versus low false rejections). These as well as other context-aware strategies can also be implemented in multi-biometric systems, where multiple identifiers are selectively fused together on the basis of the context.

In the last decade, a few examples of context adaptation strategies and dynamically optimized biometric systems have been proposed in literature. To the best of the authors knowledge, this is the first survey in the field of context-aware biometrics. The proposed perspective is neither limited to a particular technology nor to a specific processing stage.

A simple classification of context-aware biometrics is proposed, along with a comparison of the key features, objectives and performances. A rather comprehensive vision of state of art, even though not exhaustive, is proposed. The main results achieved so far are analyzed, together with the main challenges and the future scenarios for context-aware biometrics.

The reminder of the paper is organized as follows. Section 2 explains the main issues of context-awareness and its relation with biometrics. Section 3 provides an overview and comparison of the main contributions published on context-awareness and biometrics. The results achieved so far, the main challenges and the future directions for context-aware biometrics are discussed in Section 4.

2 Context awareness and context-aware biometrics

While the concept of context-aware for biometric systems is relatively recent, the concept of context awareness in information technology has been firstly introduced in the seminal work by Schilit et al. [6]. According to the authors' vision, a context-aware system "*adapts according to the location of use, the collection of nearby people, hosts, and accessible devices. as well as to changes to such things over time. A system with these capabilities can examine the computing environment and react to changes to the environment*".

This operational definition is further detailed by distinguishing three fundamental aspects of context: "*where you are, who you are with, and what resources are nearby. Context encompasses more than just the user's location, because other things of interest are also mobile and changing. Context includes lighting, noise level, network connectivity, communication costs, communication bandwidth. and even the social situation*".

A more general and application-oriented definition of context is found in [1] where context is "*any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves*".

This paper also highlight that the meaning of term "context-awareness" has been further extended by the diffusion of mobile devices and ubiquitous computing which provide a new dimension to user's mobility: "*The increase in mobility creates situations where the user's context, such as the location of a user and the people and objects around her, is more dynamic. Both handheld and ubiquitous computing have given users the expectation that they can access information services whenever and wherever they are. With a wide range of possible user situations, we need to have a way for the services to adapt appropriately, in order to best support the human–computer interaction*".

Since the capability of evaluating the static or dynamic user's characteristics are required for context-aware systems, physical and behavioral biometrics can possibly enable a more accurate and deep harmonization of the available services to the actual user's. An attempt to determine the added value of context-aware information (integrating biometric data) for ubiquitous computing environments is given in [7]. The authors, investigating about issues and challenges related to context-aware information indexing and retrieval, point out the relevance of biometrics. In particular, behavioral traits are considered the physiological and psychological user conditions, which characterize the context of activity or even the emotional context.

In this paper, the term context is considered in its widest meaning, encompassing all kind of variables (environmental conditions, operative conditions, type of usage, sensor efficiency, subject's motion, etc.) which may possibly impact any biometric applications. Human activities, indeed, are characterized by a number of (often unpredictable) changes in the way they are carried out, partly due to the human factors and partly to external factors.

However, as recent works have shown, context-awareness and biometrics have a twofold-way relationship. Indeed, not only biometric information may be valuable in characterizing user context (e.g. by providing user's physical/behavioral status) but also the opposite is true. Indeed, contextual data (i.e. environmental data, application status, sensors status, operative conditions, etc.) may provide useful information to improve almost any aspect of the authentication/recognition process (i.e. accuracy, reliability, robustness to variable environmental conditions, robustness to low-quality samples, template security, etc.). In other terms, by being aware of any relevant context-related information allows to maximize the performance of either single or multiple biometrics, while improving robustness and security to malevolent attacks. Therefore, context and context-awareness can play a relevant role in many, if not all, applications of biometrics. The capability to detect and understand any contextual change is crucial to adapt biometric sensing, processing and operation to the changing user-status, environmental conditions, security needs or application requirements. Alternatively, by monitoring soft biometric signals (e.g. heart rate, body temperature or thermal distribution, etc.), it is possible to infer user-context status according to a given user-context model, to the aim of adapting systems and services in an optimal way. Figure 1, provides an overall view of the types of context data considered in literature for biometric applications.

3 State of the art of context aware biometrics

The concept of context awareness with relation to biometrics has been explored in a number of research papers with different goals and applicative perspectives. In many cases context awareness is a key for improving performance and usability of biometric system. However, there are also many examples in which biometric technologies are instead exploited to infer the actual context.

In the following subsections, we resume the main approaches and achievements available in literature so far, by organizing them through the following taxonomy, according to their main research focus or field of application:

- *authentication/recognition performance;*
- *ubiquitous computing / mobile devices;*
- *smart environments / ambient intelligence;*
- *security / anti-spoofing.*

We are aware that, due to known cross-relations among these four categories, some of the works selected in this survey could possibly fit in two or more of the general topics listed above. For instance, ubiquitous computing is a key layer of ambient intelligence and within smart environments either security or authentication performance could be relevant. In these cases, the best fitting category (according to authors' main focus) has been chosen. Within each subsection, contributions to the field are presented in ascending chronological order. The section is completed by Table 1 summarizing the works considered along with all the synthetic info required to provide an overall picture of the state of the art.

3.1 Authentication/recognition performance

A substantial effort in biometric research is aimed at increasing the authentication/recognition accuracy. This is often achieved by designing better performing methods and algorithms for tasks such as pre-processing, feature extraction and matching. Since the best performing technique in a given operating context could be non-optimal in other scenarios, it seems reasonable to gather information about the context to adapt a section or the whole biometric system pipeline to it. This can be done according to different strategies as described in the following lines.

One of the first attempts to implement context-awareness for improving 2D face recognition accuracy under widely variable illumination conditions can be found in [8] and [9]. The authors claim that the benefits of image filtering methods to cope for uneven illumination conditions, are tightly related to the application environments. As an example, retinex filtering allows to improve face recognition performance under bad illumination. However, this filtering method performs poorly under normal illumination, whereas image's histogram equalization provides the best results. This context-dependent performance inspired a strategy in which fusion of retinex, Gabor wavelet and contrast-stretching filters, along with feature representation, is guided by an evolutionary approach based on context-awareness (illumination of input image) to maximize system performance. The fitness function defined for the genetic algorithm to work is the following:

$$\eta(V) = \lambda_1 \eta_S(V) + \lambda_2 \eta_g(V) \qquad (1)$$

where $\eta_S(V)$ accounts for successful recognition rate, $\eta_g(V)$ is the term for class generalization, while λ_1 and λ_2 weights each of the previous terms. Experiments confirm a clear edge for the proposed context-adaptive technique versus non-adaptive methods under uncontrolled illumination conditions.

Contextual information can be valuable for delivering adaptive multi-biometric fusion rules, as shown in [10] on context-aware fusion of face and gait biometrics. Most multi-biometric approaches, indeed, are based on static fusion rules, so they are not able to adapt their response to environmental variations or even to intra-class variations. In proposed work, camera field of view (view angle) and subject-to-camera distance are considered context factors relevant to the optimal fusion of (video captured) gait and face, which is performed through a neural network resulting in the ID of the person in the video clip according to:

$$ID = \underset{p}{arg\,max} \left(\sum_i l_i^p \right) \qquad (2)$$

where l_i^p is the p-th element in the output vector l_i or, in other terms, a vote for person p. Experiments comparing this fusion method to context-aware weighted-sum method and to static rules based methods (sum, product, max e min), confirm a measurable advantage in terms of recognition rate.

Reliable activity recognition, that represents an enabling technology for personal health applications, may also benefit from context awareness inferred by biometric sensors, as proposed in [11]. The authors describe a computationally inexpensive algorithm fusing data gathered from multiple body sensors (accelerometer) and biometric sensors to improve the activity recognition accuracy through a context-based relationship model, correlating inertial data and biometric response. Since biometric information depends on each individual's characteristics, the relationship model has to be derived by means of a training session during which signals gathered from inertial sensor are associated to biometrics (heart rate, blood oxygen level, skin temperature). The proposed method delivers an average activity recognition rate of around 90% for activity duration above thirty seconds. According to authors, this accuracy could be further improved by exploiting machine learning techniques during the system's training phase. The application of context information to the increasingly popular topic of gait recognition is explored in [12]. The authors are particularly interested in addressing recognition rate dropping when only low quality samples are available. To this aim, they propose to extend the dynamic features considered in the matching stage by combining them with behavioral patterns.

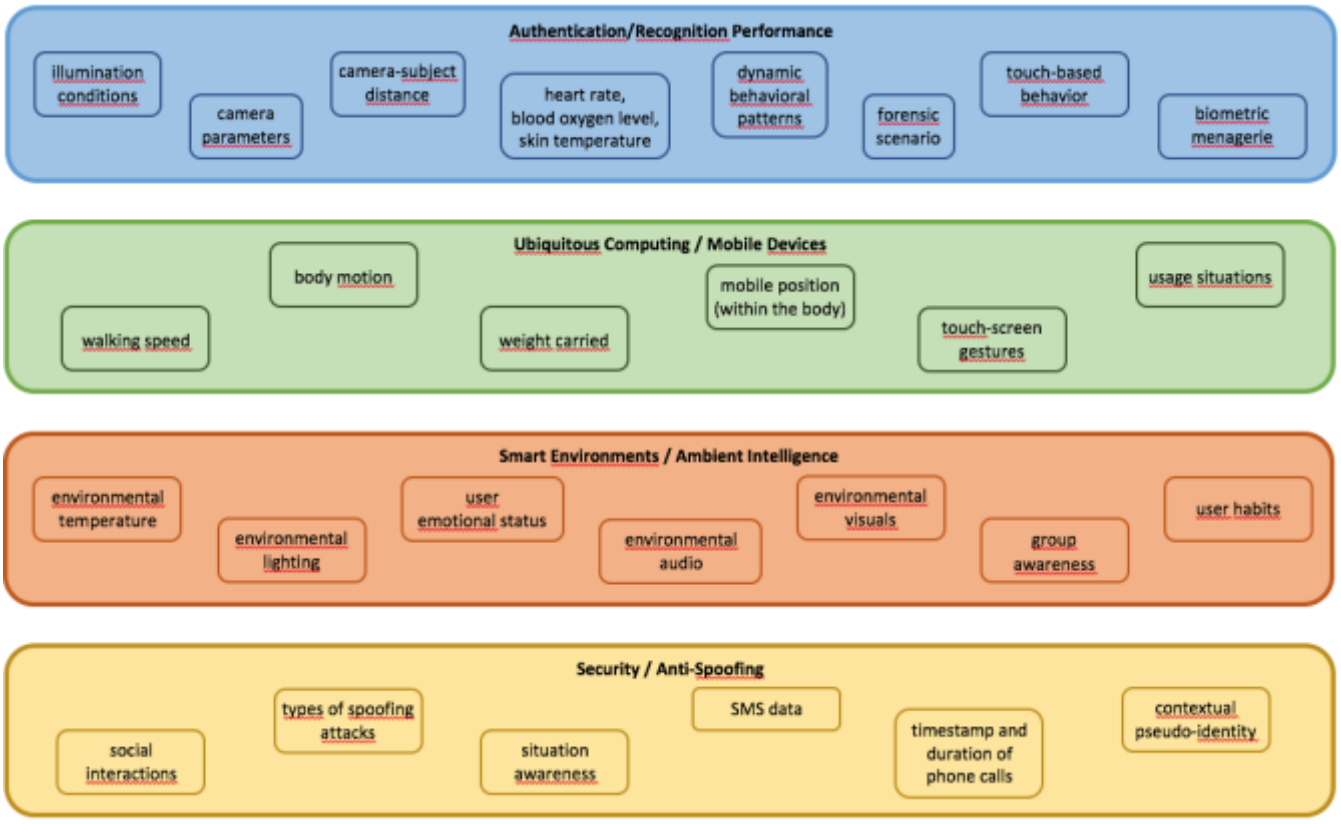

Figure 1. Types of context data exploited for biometric applications according to the state of the art, grouped for area of research/application.

According to experimental results reported, this strategy may considerably improve recognition accuracy with a modest computing cost, with performance improvement depending on the distinctiveness of behavioral patterns, besides than on quality of gait samples.

In [13] the context-awareness concept is moved to the field of digital forensics, working on overlapped latent fingerprints, which often occur at crime scene. Since this kind of fingerprints cannot undergo any processing if not properly separated, the authors propose to retrieve contextual information such as age or chemical composition for enabling a context-based enhanced separation algorithm. The context inferred from the particular forensic scenario is therefore used to optimize algorithm's operating parameters, resulting in an improved equal error rate measured on the two datasets considered for the experiments.

Focusing on mobile device based behavioral biometric solutions, [14] presents an investigation on touch-based biometrics, aimed at objectively assessing the relevance of device's physical (left/right hand, transfer, on table) and application context with regard to user recognition accuracy. Assessment is performed by means of a specifically developed context-aware mobile user recognition approach based on sensor reading normalization (to compensate for different hardware), biometric/behavioral feature extraction and subsequent classification through a Dynamic-Time-Warping based Sequential One-Nearest-Neighbor classifier (DTW-S1NN). Besides known touch-based biometric features, the authors also consider behavioral features such as Swipe-Length and Swipe-Curvature to improve context detection:

$$SL = \frac{\sqrt{(x_{end} - x_{start})^2 + (y_{end} - y_{start})^2}}{\sqrt{(x_{max} - x_{min})^2 + (y_{max} - y_{min})^2}} \quad (3)$$

$$SC = arctan\left(\frac{y_{end} - y_{start}}{x_{end} - x_{start}}\right) \quad (4)$$

Experiments, designed to compare user recognition performance with and without the contribution of contextual behavior information (inferred by gathering motion and touch-screen usage data), resulted in an average accuracy increase of thirty percent when context is considered. According to authors, this figure could be further improved if a finer-granularity context-detection would be achieved.

More recently in [15], a novel context matching algorithm as a part of a comprehensive framework for exploiting contextual behavioral patterns and gait biometrics aimed at automatic person recognition at a distance, is presented. To this purpose, the authors propose a multi-modal approach for reducing the impact of intra-class variations (due to mood, fatigue, illness, shoes worn, age, etc.) typically affecting gait

recognition performance by incorporating social context metadata into the gait recognition algorithm. This supplementary information is extracted by analyzing probe image sequence during preprocessing. Matching extracted contexts to subject's behavioral profiles results in a measurable improvement of recognition rate, as confirmed by experiments conducted on HUmanID Challenge dataset.

In [16], an investigation of music-listening and the presence of images while swiping on a touch-based interface is presented. The relevance of this common contextual activities is assessed by means of experiments aimed at measuring the impact they may have on EERs during touch-based user authentication. Previous works, indeed, have not shown experimentally the impact of other kind of contexts beyond phone orientation on touch-based authentication. The results presented from different testing configuration (combining the presence/absence of both music-listening activity or the presence/absence of images during swiping) confirm that music-listening is a relevant context for touch-based authentication. The authors also provide an analysis of the overall architecture of a music-listening aware touch-based authentication system.

Context may also be represented by a generic and heterogeneous population of users of a biometric system. The seminal work of Doddington et al. [17] suggested the existence of the "Biometric Menagerie" in which users exhibit performance differences within the system. This observation led the authors to the definition of a taxonomy based on several user categories labeled as Sheep, Goats, Lambs, and Wolves. Sheep represent the subset made form users whose feature sets are well separated from other users in the population. The users who are difficult to recognize are called Goats, while those whose biometric feature set overlap significantly with other users are called Lambs. Finally, the Wolves represent subjects capable to spoof the biometric characteristics of other users. Tough the original study has been conducted in the context of a speaker recognition system, the aforementioned categorization can be applied to any kind of biometrics. Starting from this premise, in [18] the authors exploit the "Doddington Zoo" effect to model a customized biometric fusion scheme for iris and fingerprint, according to the category (the context) each user belongs to. The experiments confirm that selective fusion performed only on weak users (Goats and Lambs) may represent a valuable way to improve the overall system performance substantially. Moreover, by considering this kind of context information a good tradeoff between uni-modal and multibiometric systems can be achieved.

3.2 Ubiquitous computing / mobile devices

The worldwide diffusion of mobile devices and wearable technologies (smartphones, tablets, smart watches, fitness/health bands, etc.) has powerfully driven ubiquitous computing, opening a number of applicative scenarios in private and public contexts. As a result, ubiquitous computing is permeating everyday life by gathering, processing and sharing personal data along with surrounding environment information, thus reasonably giving rise to concerns about security issues. Overall, most context-aware approaches to ubiquitous user authentication aim at increasing security level in accessing to mobile applications and services while operating in an implicit and non-intrusive way.

User authentication by gait biometric is particularly suited to operating implicitly, but is affected by intra-class variations possibly due to uncontrolled capturing conditions or constraints related to operating environment. Starting from this premise confirmed by a preliminary performance analysis, the authors of [19] propose a classifier-independent statistical Measure of Similarity (MOS) highlighting high entropy locations within the feature vector. According to the experiment conducted with this metric, the authors remark the sensitiveness of gait biometric to factors beyond walking speed (such as the weight possibly carried or the shoes worn) which could be automatically interpreted to provide context-awareness for ubiquitous computing applications.

On modern smartphones equipped with multiple sensors, gathering of contextual information can be easily performed by measuring a range of environmental aspects. To this regard, an approach for inferring subject-specific context models from contextual data captured in the form of device usage patterns, is presented in [20]. These models are used to train support vector machines for providing a class probability which translates in the number of features to be considered for authentication or, possibly, that authentication can be avoided. The feasibility of proposed classification approach is confirmed by the results of experiments, though large training sets are crucial to build accurate context models.

The idea behind [21], while is still targeted to exploiting context awareness for flexible user authentication, is focused on how modulating the strength of active authentication required for a given level of security, via contextual multi-factor data. In other terms whenever there is a high chance the user is a legitimate user, more acceptable and less reliable active authentication technique (possibly behavioral biometrics) could be used. Conversely, if contextual data convey a low chance that the user is genuine, a more accurate (e.g. physical biometrics), though less acceptable, authentication method is required. The proposed Context-Aware Scalable Authentication model, is based on a probabilistic framework for dynamic selection of active authentication scheme, given passive factors, modeled by:

$$\hat{u}\begin{cases} 1, \alpha P(u=1|s_1,\ldots,s_n) > P(u=-1|s_1,\ldots,s_n) \\ -1, \alpha P(u=1|s_1,\ldots,s_n) \leq P(u=-1|s_1,\ldots,s_n) \end{cases} \quad (5)$$

where α denotes the degree to which user authentication is conservative, $(u=1)$ denotes that the user is legitimate, while $(u=-1)$ denotes the user is not legitimate and s_1 represents the value observed for the *i*-th factor.

Influence of context on body movement patterns captured

through smartphone accelerometer, represents the main focus of [22]. By means of statistical experiments and supervised learning methods, the authors observe that the position in which the phone is held affects user recognition performance. Hence, they propose a two-stages approach to user authentication aimed to detect where the mobile device is, among the four most probable locations (i.e: right hand, left hand, right front pocket, left front pocket), before performing authentication. The experiments confirm the relevance of spatial context-awareness (phone location) for an improved authentication accuracy, particularly in case of in-the-wild application. If context is reliably determined, classification accuracy may increase up to 20% over a context insensitive approach.

In most mobile devices, user authentication is typically performed only in specific situations like the post login stage. In [23] this task is performed implicitly and unobtrusively through a touch based identity protection service. Their approach is based on the continuous analysis of touch screen gestures via an authentication service operating in the background of any running application. In uncontrolled environments, indeed, data generated during touch screen usage tends to result noisier and more unpredictable due to variations related to usage behavior and application context. The implicit and continuous identity verification service, exploits a set of highly salient features extracted by touch screen data, along with a sequential identification algorithm. According to experimental data collected, the proposed method may reach over 90% of recognition accuracy in uncontrolled application environments, with a small computational cost and a reasonable increment of battery usage.

More recently in [24], a generic model for context-based biometric authentication on mobile devices is presented, in which context data enables a dynamic selection of different biometric authentication modality. This selection is performed according to two main criteria: maximizing the quality of biometric samples captured under different environmental conditions and harmonizing the authentication modality to user interaction scheme detected at the moment. The proposed model may exploit any of the sensor info available which, after an initial discretization, is used to define user-contexts (i.e. usage situations) represented through a vector of criteria values. Additionally, a ranking of user preferences concerning authentication and communication modalities is also required by the approach to the aim of interpreting context data and making final decision. In the proposed model, the maximum number of possible situations is given by:

$$\left(\prod_{i=1}^{k} x_k\right) \times p_1! \times p_2! \qquad (6)$$

where k is criteria number, x_k denotes the number of values for criterion k, p_1 denotes the number of authentication methods, and p_2 denotes the number of communication methods. Proposed model has been validated via a proof-of-concept software prototype. Nevertheless, when time interval between sensors samples is too long, there is a chance that a non-optimal authentication modality could be erroneously selected according to inaccurate sample data.

3.3 Smart environments / Ambient intelligence

Ambient intelligence (AmI) environments and more generally smart environments, which promise enhanced services customization, natural interaction and ubiquitous information communication, are typically context-aware by design. Nevertheless, they may benefit in many ways from context detection methods exploiting physical and/or behavioral biometrics combined to environmental sensors [25], possibly providing a greater understanding of user's status and activity.

To this regard in [26] the authors describe an experimental home automation framework to capture user's behavior and environment status to adaptively control customized services and domestic devices. The proposed approach exploits Fuzzy Markup Language (FML) derived from XML to implement the control network layer responsible of interconnecting control devices required to enable ubiquitous communication. System adaptivity to contextual data (environmental sensors or face biometrics) is achieved via an agent based core middleware based on an evolutionary mechanism to customize available services. Besides regulating access to the AmI environment, face biometrics are used to adapt system response to the specific preferences and requirements associated to each user profile. This approach is further extended in [27], where context data are enriched by physical and emotional user status captured from a set of biometric features and modeled by means of both previously mentioned FML and H2ML another XML based language modeling human information usable at different abstraction levels inside the AmI architecture. so as to reach transparency, uniformity, and abstractness in bridging multiple sensors properties to flexible and personalized actuators. and to exploit distribution and concurrent computation in order to gain real-time performances.

Smart indoor environments also represent the main application scenario in [28]. The proposed abstract framework is based on the unobtrusive monitoring of occupants through multiple biometrics data to the aim of tracking their position and activity within the environment. Info gathered by the sensors network may trigger environment changes according to a state transition based abstraction model. Any type of biometric sensor may be handled by this model in which a biometric recognition step represents an event, while the reasoning and decisional activity involved in state transition is represented by transition function. According to experiments, the proposed state transition model provides a flexible and effective abstraction of biometrics-based context-aware smart environments.

Speaker diarization, a task typically aimed at associating temporal regions to a set of speakers based on a single-

channel audio content, is exploited in [29] to adapt applications response in smart-environments. In this approach, context information derives from two types of biometrics, face and speech, respectively captured by means of a single pan/tilt/zoom video camera and by multiple microphones arrays, and conveyed as an audio-visual signal. According to this operating paradigm, user localization via acoustic position and face identification is used as an additional context source for the diarization task. This additional information is combined to a speaker change detection probability through a Hidden Markov Model, resulting in a reduced diarization error. The face identification component accounts for up to fifty percent of the overall error reduction performance.

A different take on using multiple-biometrics for the enhancement of AmI environments is represented in [30], where the main focus is on the improved user identification capability by exploiting a multi-agent based architecture. Here the term multiple biometrics refers to multiple face recognition modalities, though the proposed architecture is designed to support any kind of biometric identifier in any combination. Each biometric module of the framework implements an autonomous agent able to handle its own recognition task. A specific metric named System Response Reliability is a key component of the data-fusion strategy, by assessing single-response reliability through:

$$SSR = |\varphi(p) - \varphi_k| / S(\varphi(p), \varphi_k) \qquad (7)$$

where:

$$S(\varphi(p), \varphi_k) = \begin{cases} 1 - \varphi_k & if \quad \varphi(p) > \varphi_k \\ \varphi_k & otherwise \end{cases} \qquad (8)$$

is the distance from φ_k to the proper extreme of range [1,0) of feasible values, based on the comparison of $\varphi(p)$ and φ_k, where the former is the density ratio and the latter is a characteristic (experimentally defined) of a biometric agent, related to its ability in separating genuine subjects from imposters. Inter-agent communications among different classifier-agents is based on the N-Cross Testing Protocol, while final (combined) recognition decision is delivered by a different agent type acting as supervisor module, which frees the proposed architecture from the parameter invariance limiting most other multi-biometric approaches.

The proposal of a cognitive sensing framework exploiting low cost, low power, distributed devices providing a variety of behavioral biometrics, is found in [31]. By exploiting a network of heterogeneous sensors, sparse behavioral biometric data can be gathered and rapidly analyzed, resulting in situation understanding, cross-layer adaptation and behavior-based collaboration leveraged by a multi-agent architecture. Context awareness, group awareness and spatial data contribute to implementing a cognitive sensing intelligence possibly able to address some of the issues often affecting usage of soft biometrics, such as presence of crowd and long capture distance. Finally, the application of multimodal biometrics to cloud computing is investigated in [32]. In information technology services hosted by cloud computing, privacy and security represents crucial aspects only in part addressed. High security approaches, indeed, typically involves computationally expensive solutions which are unlikely to result acceptable by most users. To this regard, the authors propose a framework aimed at authenticating cloud users through a multi-factor authentication-multi-modal biometrics approach based on class-association rules and a novel metric measuring user experience.

According to this scheme, for a given user, the most expected authentication modality is inferred by exploiting class-association rules along with user's authentication habits derived from her/his authentication history, to the aim of progressively improving the experience. As a side-effect, the use of class association rules results in the possibility to understand user's actual operating context which, in turn, allow to select the biometrics most suited to it.

3.4 Security / anti-spoofing.

Context awareness and biometrics are both tightly related to the topic of security, the former due to its relevance for threat prevention and detection and the latter for representing one of the possibly most effective means for separating genuine/authorized subject from impostor/unauthorized ones. Consequently, it is reasonable and convenient to combine both aspects in a context-aware biometric-based strategy to effectively addressing security, privacy and spoofing issues.

To this regard, in [33], "Cerberus" a security approach suited to "smart spaces" is presented. Smart spaces, are sentient and information-rich environments extending the physical space through embedded devices and sensors able to detect context changes and to adapt to them. High-level architecture of Cerberus is based on four main components: the security service, the context infrastructure, various security policies represented in the knowledge base, and an automated reasoning capability provided by an inference engine, that enforces the security policies. Within a smart space, adaptable security policies are associated to dynamic and frequently changing contexts. Any available biometric feature contributes to the confidence level of a credential associated to each identity. First order logic is used as logical model for context, providing required abstraction level.

With regard to types of context data potentially relevant for security related applications, is worth noting that even social interaction contains distinguishable context data which can be used, possibly together with biometric information for user authentication in low security application contexts. This "socially-aware" security scheme, whose feasibility is discussed in [34], is not based on direct observation of user's social interaction but rather on its indirect evaluation by means of social interaction recordings made via today ubiquitous bluetooth-capable mobile phones. This social security model works well in conjuction with additional behaviometric models based on soft biometrics and providing the "someone you are" factor.

TABLE 1

Resume table of works described in section 3. Contributions are listed in descending alphabetic order.

#	Authors, Year, Reference	Biometrics	Types of Context Data	Aim	Approach
1	Abate et al., 2011 [30]	face	multi-biometric data	AmI environment control	multi-agent based architecture
2	Acampora et al., 2005 [26]	face	indoor environmental data, user biometrics	AmI environment control	intelligent agents based framework, adaptive fuzzy control strategy
3	Acampora et al., 2007 [27]	face, gait, body temperature, etc.	environmental data, user status	AmI environment control	H2ML (Human to Markup Language) + FML (Fuzzy Markup Language) based framework
4	Al Mouthadi et al., 2003 [33]	any	situational information conveyed by "smart spaces"	improving security of smart spaces	first-order-logic based context model, inference engine
5	Bächlin et al., 2009 [19]	gait	walking dynamics, weight carried, shoes worn	context-detection	classifier-independent statistical Measure of Similarity (MOS)
6	Bazazian and Gavrilova, 2012 [12]	gait	behavioral patterns	improving recognition accuracy	matching algorithm evaluating combination of dynamic features and behavioral patterns
7	Bazazian and Gavrilova, 2015 [15]	gait	behavioral patterns	automatic person recognition at a distance	matching algorithm evaluating social context metadata and subject's behavioral profiles
8	Buhan et al., 2010 [38]	any	context-dependent input	improving disposability and renewability of biometric tokens	algorithm for generating contextual pseudo-identity through an extended fuzzy embedder
9	Feng et al., 2014 [23]	touch-based gestures	application context	implicit and continuous authentication	continuous identity verification running in background of other apps
10	Feng et al., 2015 [14]	touch	mobile device's physical and application context	improving recognition accuracy	behavioral/biometric feature extraction and dynamic-time-warping based feature matching via Sequential One-Nearest-Neighbor classifier
11	Frankel and Maheswaran, 2009 [34]	behavioral biometrics	user's social context	implicit authentication	socially aware security scheme
12	Geng et al., 2010 [10]	face + gait	camera field of view, camera-to-subject distance	improving recognition accuracy	context-aware fusion based on neural network
13	Hao et al., 2013 [31]	multiple behavioral biometrics	spatial, data, context, and group awareness	tracking and identification	cognitive sensing framework based on multi-agent architecture
14	Hayashi et al., 2013 [21]	behavioral	user's location, time since last login	balancing authentication security and usability	probabilistic framework for dynamic selection of active authentication scheme given passive factors

15	Kantarci et al., 2015 [37]	fingerprints	user's location, wifi data, numbe and duration of phone calls and SMSs	unauthorized access prevention, fraud detection	cloud-centric, context-aware knowledge-based architecture
16	Komulainen et al., 2013 [35]	face	video content	spoofing attack detection	cascade configuration of HOG and linear SVM based detectors
17	Mansour et al., 2016 [32]	any	time, place, device	improving security/privacy in cloud computing	multi-factor authentication based on multimodal biometrics and class-association rules
18	Martin et al., 2011 [11]	body dynamics, heart rate, blood oxygen level, skin temperature	context-based relationship model, correlating inertial data and biometric response	improving activity recognition accuracy	fusion of multiple body inertial data and biometric sensors through a customized correlation-model
19	Menon et al., 2008 [28]	face, voice	user's location and activity	smart-environment control	state transition based abstraction model
20	Nam et al., 2007 [9]	face	illumination conditions of application environment	improving recognition accuracy	fusion of retinex, Gabor wavelet and contrast-stretching filters guided by genetic algorithm
21	Paul et al., 2014 [36]	face+ear	situation awareness	template protection	random fusion, projection and selection of multiple biometric traits
22	Primo et al., 2014 [22]	gait	phone location	implicit authentication	two-stage authentication process based on phone location detection
23	Primo and Phoha, 2015 [16]	touch-based gestures	music listening, during authentication	improving recognition accuracy	music-presence sensitive, touch-based gestures matching
24	Qian et al., 2014 [13]	latent fingerprints	forensic scenario analysis	overlapped fingerprints separation	separation algorithm optimization based on forensic context
25	Ross et al. [18]	any	user population	improving performance stability	selective fusion scheme based on user categorization
26	Schmalenstroeer and Haeb-Umbach, 2010 [29]	face, voice	user's location and identity	smart-environment control	speaker diarization based service-oriented middleware
27	Witte et al., 2013 [20]	mobile device embedded sensors' data	device usage-patterns	user friedly authentication	support vector machines trained by subject-specific context models
28	Wójtowicz and Joachimiak, 2016 [24]	mobile device embedded sensors' data	multi-factor usage situations	selection of best quality biometric sample in a given context	generalized model
#	**Authors, Year, Reference**	**Biometrics**	**Types of Context Data**	**Aim**	**Approach**

Security of biometric authentication systems, besides depending from the verification approaches adopted, also relies on system's capacity to resist to spoofing attack of various genre. Since, reasonably, no generic anti-spoofing technique could successfully respond to every attack scenario, in [35] the authors propose to break down the problem into a variety of attack specific sub-problems which can be solved by specific countermeasures. This is possible by exploiting a network of attack-specific spoofing detectors which resembles how humans perform spoofing detection by analyzing scene and context. This strategy is implemented by a cascade configuration of detectors, specialized in detecting upper-body and spoofing medium. Both types of detectors are based on histogram of oriented gradients descriptors and linear support vector machines. The detection pipeline analyzes each frame within a captured video sequence so that longer footage possibly increase detection accuracy but also increase computing load. Cross-database evaluation results confirm the effectiveness of proposed cascade detection architecture that is designed to be easily expandable to address a larger number of attack modalities.

Biometric systems security greatly depends from template protection. Cancelable biometrics represent one of the most regarded way to protect templates by transforming original biometric features into an alternative data form hard to be misused by an attacker and subject to be revoked if compromised. In [36] the authors describe a method for cancelable template generation exploiting situation awareness via a random cross-folding method involving random fusion, projection and selection of multiple biometric traits. Method validation, carried out on a bimodal face+ear virtual dataset, confirm the efficacy of the approach in terms of increased template protection.

The increasing diffusion of Internet of Things through a vast number of devices and hardware architectures involves an increased risk of attack and new kinds of threats. Indeed, connected user devices along with the (usually large) number of mobile apps running on them, are prone to security vulnerabilities as a result of unauthorized access. These potential menaces represent the scenario in which the authors of [37] propose their concept of Internet of Biometric Things, a cloud-centric biometric identification architecture consisting of connected devices requiring biometric authentication. This cloud-centric authentication approach take advantage from biometrics and context-awareness to improve security of mobile applications to prevent malicious users to gain unauthorized access. According to this strategy, cloud-centric knowledge-based abstraction provide contextual data such as position, WiFi data, mobile's data or even number, timestamp and duration of received/placed calls and SMSs, reinforcing local password and fingerprint based authentication. Additionally, by exploiting the same kind of data, even frauds can possibly be detected.

Finally, in [38] the concept of contextual pseudo identity, a soft identity token assembled from both a user's biometric and the context, is introduced. Contextual pseudo identity offers enhanced tokens' disposability and renewability compared to traditional biometrics-based identity tokens. These two essential properties for protecting user's real identity may provide better security in challenging (security-wise) application contexts like ubiquitous computing. Contextual pseudo identities are generated by an algorithm based on the extension of a Fuzzy Embedder so that it accepts both biometric and context-dependent input while preserving its intrinsic security and reliability properties.

4 DISCUSSION AND CONCLUSIONS

From the analysis of the state of the art resumed in the previous section, the overall emerging picture suggests that context-awareness in biometrics (or possibly biometrics in context-awareness) represent a field explored only in the surface, with a vast potential still unexploited.

The variety of approaches somehow combining context and biometrics presented so far, show that a first group of strategies privilege performance improvement in its various declinations (recognition accuracy, resistance to attacks, template security). This result is perhaps predictable, since performance enhancement typically represents one of the strongest research motivation.

A second group of contributions is specifically targeted at smart-spaces / ambient-intelligence environments, which naturally stem from the concept of context-awareness and already exploited biometrics information, though in a less organic way.

Finally, a third smaller, yet promising, group of works tries to explore more novel aspects, such as implicit/continuous authentication, definition of new "biometric-relevant" contexts, customized context-biometrics correlation models.

It is worth to note that there is tangible potential even for industrial applications, as highlighted by a number of international patent applications [39] [40] [41] [42] registered so far and concerning the topic.

Another consideration due is that none of the approaches reported (neither those concerning the same general topic) share the same experimental methodology or the same reference database, even because contextual-data are typically approach-dependent. As a consequence of this fact, it is practically impossible to objectively evaluate the results achieved by the algorithms and methods behind these works through a fair comparative analysis. Though the difficulty in building a comprehensive contextual database is clearly understandable, due to the generality of the term "context", it would perhaps be more reasonable to build an application-context specific database (e.g. for indoor environment, for mobile-ubiquitous usage, etc.) in which all the data produced by environmental sensors, mobile-device sensors, biometric sensors, etc. are gathered as time series, to make possible delivering an objective evaluation framework.

Nevertheless, there is still ample room for deepening the inter-relationship between context-awareness and biometrics. To this regard, future directions of research could possibly explore this territory with three levels of granularity.

The first level may concern more general topics related to context-awareness in biometrics, such as:

- *temporal dimension of context awareness;*
- *general correlation model;*
- *social context driven biometrics;*
- *privacy aspects.*

Context awareness is the result of meaningfully combining different pieces of contextual information. However, instant context sampling may not always be the best choice for a given application whilst a properly defined observation window could be applied. Activity timestamps or even biometric signals time series could be analyzed, possibly via machine learning methods, to improve context inference. Adaptive context-sampling algorithms could also be exploited to optimize time resolution versus current user and environment status.

While a few authors have proposed a model for representing [43] and correlating [44] biometric information and context data in selected application contexts, the lack of a more general approach to the modeling of relations among activity patterns, raw biometrics and contextual data, requires further investigation.

Social context has already been considered as a possibly key aspect of context-awareness, but the role of biometrics in this regard has not been fully deepened. The vast diffusion of ubiquitous multi-sensors equipped mobile devices enables the monitoring of social dynamics and their inclusion in more refined context detection methods, with possible advantages in term of improved service-to-context adaptation.

Privacy and legal requirements for developing biometric context-based applications should also be carefully considered. To this regard, according to [45] and [46], "social guarantees should be built into context-based systems for private relations (between private user and private services) and public relations (between private/public users and public services)".

The second level may investigate the following more specific topics:

- *context-based sensor operation optimization;*
- *context-based thresholding;*
- *context-based template matching strategy;*
- *context-adaptive weighting of multiple-biometrics.*

Biometric sensors are characterized by a variable number of operating parameters (e.g.: field-of-view, sensibility, orientation, sampling frequency, sample quantization, frame-rate, resolution, etc.) which in many cases could be procedurally controlled to adapt the sensor's response to the current context (operating conditions, operating modalities, etc.). Though some kind of control is already present in many actual biometric systems, a generalized adaptive operating model could be beneficial to context-aware biometric applications.

Similarly, context-based strategies should be explored with regard to each of the main processing stages of a biometric system. Context-awareness related topics worth further investigation include tasks such as setting the decision threshold, selection of a particular matching algorithm or weighting of each biometric within a multi-biometrics fusion scheme, which could all be adapted to operating conditions (e.g. low-to-high security, in-the-wild operations, good/poor sample quality, etc.)

Finally, there are a few application fields which should be regarded with particular attention with regard to context-aware biometric systems and methods:

- *health;*
- *automotive;*
- *aviation;*

In the healthcare industry, there is a specific need for flexible, on-demand authentication, extensible context-aware access control, and dynamic authorization enforcement. On-demand authentication procedures, allow users to be authenticated based on their task-specific situations. Within this scenario, context-aware access control could enable more precise and fine-grain authorization polices for any application [47]. Pervasive healthcare can take advantage by context-aware security approaches too, by gathering physiological, environmental and personal information to generate user context for authenticating a specific patient [48].

In the automotive industry, there is a strong commitment in designing and developing active vehicle safety (AVS) systems to possibly reduce the number and the severity of accidents. The proposal of context and driver aware AVS systems associating behavioral biometric data with the external (road context) and internal (car context) contextual data represent an interesting and line of research with the remarkable potential of saving human lives [49]. Human factor is crucial also in air traffic control, since "*diminished vigilance caused by fatigue, stress, and excessive mental load have been cited as a major cause for most aviation accidents*" [50]. Context-aware approaches combining user's biometric data (e.g. pupillometric indices of cognitive load), time, location and environmental analysis may prove valuable to detect sleepy or reduced functionality in air traffic controllers during their critical work sessions.

In the end, the aforementioned cues are only a few of the possible research topics still open, but the advantages of associating context detection to biometrics, though already clear, are still to be fully exploited.

REFERENCES

[1] Abowd, G. D., Dey, A. K., Brown, P. J., Davies, N., Smith, M., & Steggles, P. (1999, September). Towards a better understanding of context and context-awareness. In International Symposium on Handheld and Ubiquitous Computing (pp. 304-307). Springer Berlin Heidelberg.

[2] Elrod, S., Hall, G., Costanza, R., Dixon, M., & Des Rivieres, J. (1993). Responsive office environments. Communications of the ACM, 36(7), 84-85.

[3] Brown, M. G. (1996). Supporting user mobility. In Mobile Communications (pp. 69-77). Springer US.

[4] Cooperstock, J. R., Tanikoshi, K., Beirne, G., Narine, T., & Buxton, W. A. (1995, May). Evolution of a reactive environment. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 170-177). ACM Press/Addison-Wesley Publishing Co..

[5] Rekimoto, J., Ayatsuka, Y., & Hayashi, K. (1998, October). Augment-able reality: Situated communication through physical and digital spaces. In Wearable Computers, 1998. Digest of Papers. Second International Symposium on (pp. 68-75). IEEE.

[6] Schilit, B., Adams, N., & Want, R. (1994, December). Context-aware computing applications. In Mobile Computing Systems and Applications, 1994. WMCSA 1994. First Workshop on (pp. 85-90). IEEE.

[7] Jones, G. J. (2005, April). Challenges and opportunities of context-aware information access. In Ubiquitous Data Management, 2005. UDM 2005. International Workshop on (pp. 53-60). IEEE.

[8] Young, N., Bashar, M., & Rhee, P. (2006). Adaptive context-aware filter fusion for face recognition on bad illumination. In Knowledge-Based Intelligent Information and Engineering Systems (pp. 532-541). Springer Berlin/Heidelberg.

[9] Nam, M. Y., Bashar, R., & Rhee, P. K. (2007). Adaptive feature representation for robust face recognition using context-aware approach. Neurocomputing, 70(4), 648-656.

[10] Geng, X., Smith-Miles, K., Wang, L., Li, M., & Wu, Q. (2010). Context-aware fusion: A case study on fusion of gait and face for human identification in video. Pattern Recognition, 43(10), 3660-3673

[11] Martín, H., Bernardos, A. M., Tarrío, P., & Casar, J. R. (2011, July). Enhancing activity recognition by fusing inertial and biometric information. In Information Fusion (FUSION), 2011 Proceedings of the 14th International Conference on (pp. 1-8). IEEE.

[12] Bazazian, S., & Gavrilova, M. (2012, May). Context based gait recognition. In SPIE Defense, Security, and Sensing (pp. 84070J-84070J). International Society for Optics and Photonics.

[13] Qian, K., Schott, M., Zheng, W., & Dittmann, J. (2014). Context-based approach of separating contactless captured high-resolution overlapped latent fingerprints. IET biometrics, 3(2), 101-112.

[14] Feng, T., Zhao, X., DeSalvo, N., Liu, T. H., Gao, Z., Wang, X., & Shi, W. (2015, April). An investigation on touch biometrics: Behavioral factors on screen size, physical context and application context. In Technologies for Homeland Security (HST), 2015 IEEE International Symposium on (pp. 1-6). IEEE.

[15] Bazazian, S., & Gavrilova, M. (2015). A hybrid method for context-based gait recognition based on behavioral and social traits. In Transactions on Computational Science XXV (pp. 115-134). Springer Berlin Heidelberg.

[16] Primo, A., & Phoha, V. V. (2015, September). Music and images as contexts in a context-aware touch-based authentication system. In Biometrics Theory, Applications and Systems (BTAS), 2015 IEEE 7th International Conference on(pp. 1-7). IEEE.

[17] Doddington, G., Liggett, W., Martin, A., Przybocki, M., & Reynolds, D. (1998). Sheep, goats, lambs and wolves: A statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation. National Inst Of Standards And Technology Gaithersburg Md.

[18] Ross, A., Rattani, A., & Tistarelli, M. (2009, September). Exploiting the "doddington zoo" effect in biometric fusion. In Biometrics: Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on (pp. 1-7). IEEE.

[19] Bächlin, M., Schumm, J., Roggen, D., & Töster, G. (2009, June). Quantifying gait similarity: User authentication and real-world challenge. In International Conference on Biometrics (pp. 1040-1049). Springer Berlin Heidelberg

[20] Witte, H., Rathgeb, C., & Busch, C. (2013, September). Context-aware mobile biometric authentication based on support vector machines. In Emerging Security Technologies (EST), 2013 Fourth International Conference on (pp. 29-32). IEEE.

[21] Hayashi, E., Das, S., Amini, S., Hong, J., & Oakley, I. (2013, July). CASA: context-aware scalable authentication. In Proceedings of the Ninth Symposium on Usable Privacy and Security (p. 3). ACM.

[22] Primo, A., Phoha, V. V., Kumar, R., & Serwadda, A. (2014). Context-aware active authentication using smartphone accelerometer measurements. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 98-105).

[23] Feng, T., Yang, J., Yan, Z., Tapia, E. M., & Shi, W. (2014, February). Tips: Context-aware implicit user identification using touch screen in uncontrolled environments. In Proceedings of the 15th Workshop on Mobile Computing Systems and Applications (p. 9). ACM.

[24] Wójtowicz, A., & Joachimiak, K. (2016). Model for adaptable context-based biometric authentication for mobile devices. Personal and Ubiquitous Computing, 20(2), 195-207.

[25] Tistarelli, M., & Schouten, B. (2011). Biometrics in ambient intelligence. Journal of Ambient Intelligence and Humanized Computing, 2(2), 113-126.

[26] Acampora, G., Loia, V., Nappi, M., & Ricciardi, S. (2005, July). Ambient intelligence framework for context aware adaptive applications. In Computer Architecture for Machine Perception, 2005. CAMP 2005. Proceedings. Seventh International Workshop on (pp. 327-332). IEEE.

[27] Acampora, G., Loia, V., Nappi, M., & Ricciardi, S. (2007). Human-Based. Models. for. Ambient. Intelligence. Environments. In Artificial Intelligence and Integrated Intelligent Information Systems: Emerging Technologies and Applications (pp. 1-17). IGI Global.

[28] Menon, V., Jayaraman, B., & Govindaraju, V. (2008, June). Biometrics driven smart environments: Abstract framework and evaluation. In International Conference on Ubiquitous Intelligence and Computing (pp. 75-89). Springer Berlin Heidelberg.

[29] Schmalenstroeer, J., & Haeb-Umbach, R. (2010). Online diarization of streaming audio-visual data for smart environments. IEEE Journal of Selected Topics in Signal Processing, 4(5), 845-856.

[30] Abate, A. F., De Marsico, M., Riccio, D., & Tortora, G. (2011). MUBAI: multiagent biometrics for ambient intelligence. Journal of Ambient Intelligence and Humanized Computing, 2(2), 81-89.

[31] Hao, Q. (2013, February). Cognitive sensing for distributed behavioral biometrics. In Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2013 IEEE International Multi-Disciplinary Conference on (pp. 98-101). IEEE.

[32] Mansour, A., Sadik, M., Sabir, E., & Azmi, M. (2016, October). A context-aware Multimodal Biometric Authentication for cloud-empowered systems. In Wireless Networks and Mobile Communications (WINCOM), 2016 International Conference on (pp. 278-285). IEEE.

[33] Al-Muhtadi, J., Ranganathan, A., Campbell, R., & Mickunas, M. D. (2003, March). Cerberus: a context-aware security scheme for smart spaces. In Pervasive Computing and Communications, 2003.(PerCom 2003). Proceedings of the First IEEE International Conference on (pp. 489-496).

[34] Frankel, A. D., & Maheswaran, M. (2009, January). Feasibility of a socially aware authentication scheme. In Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE (pp. 1-6). IEEE.

[35] Komulainen, J., Hadid, A., & Pietikainen, M. (2013, September). Context based face anti-spoofing. In Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on (pp. 1-8). IEEE.

[36] Paul, P. P., Gavrilova, M., & Klimenko, S. (2014). Situation awareness of cancellable biometric system. The Visual Computer, 30(9), 1059-1067.

[37] Kantarci, B., Erol-Kantarci, M., & Schuckers, S. (2015, October). Towards secure cloud-centric internet of biometric things. In Cloud Networking (CloudNet), 2015 IEEE 4th International Conference on (pp. 81-83). IEEE.

[38] Buhan, I., Lenzini, G., & Radomirović, S. (2010, October). Contextual biometric-based authentication for ubiquitous services. In International Conference on Ubiquitous Intelligence and Computing (pp. 680-693). Springer Berlin Heidelberg.

[39] Li, Y. L., & Ramadas, P. (2012). "Context aware biometric authentication", U.S. Patent No. 8,255,698. Washington, DC: U.S. Patent and Trademark Office.

[40] Guralnik, Valerie, Saad J. Bedros, and Isaac Cohen. "System and method for multi-modal biometrics." U.S. Patent Application No. 12/715,520 (2010)
[41] Li, Yuk L., and Padmaja Ramadas. "Biometric authentication based upon usage history." U.S. Patent Application No. 12/342,621 (2010)
[42] Song, Zhexuan, and Jesus Molina. "Method and apparatus for context-aware authentication." U.S. Patent Application No. 12/816,966 (2011)
[43] Andronikou, V., Xefteris, S., & Varvarigou, T. (2012, September). A novel, algorithm metadata-aware architecture for biometric systems. In Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2012 IEEE Workshop on (pp. 1-6). IEEE.
[44] Basu, A., Xu, R., Rahman, M. S., & Kiyomto, S. (2016, December). User-in-a-context: A blueprint for context-aware identification. In Privacy, Security and Trust (PST), 2016 14th Annual Conference on (pp. 329-334). IEEE.
[45] Pedraza, J., Patricio, M. A., De Asís, A., & Molina, J. M. (2013). Privacy-by-design rules in face recognition system. Neurocomputing, 109, 49-55.
[46] Pedraza, J., Patricio, M. A., de Asís, A., & Molina, J. M. (2010). Privacy and legal requirements for developing biometric identification software in context-based applications. International Journal of Bio-Science and Bio-Technology, 2(1), 13-24
[47] Hu, J., & Weaver, A. C. (2004, August). A dynamic, context-aware security infrastructure for distributed healthcare applications. In Proceedings of the first workshop on pervasive privacy security, privacy, and trust (pp. 1-8).
[48] Chowdhury, M. A., & Light, J. (2009, August). Context-Aware Data Association and Authenticity in Pervasive Healthcare. In Privacy, Security, Trust and the Management of e-Business, 2009. CONGRESS'09. World Congress on (pp. 227-230). IEEE.
[49] Sathyanarayana, A., Boyraz, P., & Hansen, J. H. (2011). Information fusion for robust 'context and driver aware'active vehicle safety systems. Information Fusion, 12(4), 293-303.
[50] Rafiqi, S., Nair, S., & Fernandez, E. (2014, May). Cognitive and context-aware applications. In Proceedings of the 7th International Conference on PErvasive Technologies Related to Assistive Environments (p. 23). ACM.