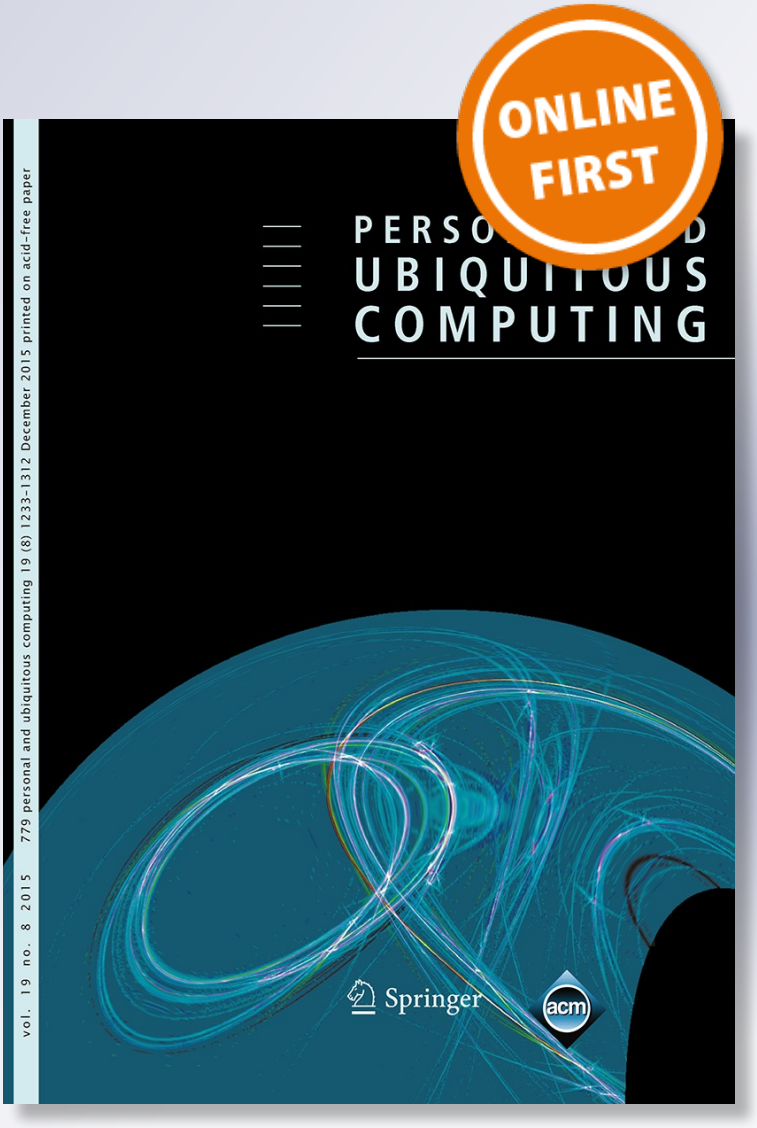
Model for adaptable context-based biometric authentication for mobile devices

Adam Wójtowicz & Krzysztof Joachimiak

Personal and Ubiquitous Computing

ISSN 1617-4909

Pers Ubiquit Comput
DOI 10.1007/s00779-016-0905-0



Springer

Pers Ubiquit Comput
DOI 10.1007/s00779-016-0905-0

ORIGINAL ARTICLE

Model for adaptable context-based biometric authentication for mobile devices

Adam Wójtowicz[1] · **Krzysztof Joachimiak**[2]

Received: 6 April 2015 / Accepted: 5 January 2016

Abstract It becomes possible to take advantage of seamless biometric authentication on mobile devices due to increasing quality and quantity of built-in sensors, increasing processing power of the devices, and wireless connectivity. However, practical effectiveness of the biometric authentication application depends on user's environment conditions that can decrease the accuracy of biometrics recognition or make the acquisition process undesirable for mobile user in a given moment, i.e., effectiveness depends on usage context. In this paper, context-based biometric authentication model for mobile devices is proposed. It enables determining the most accurate authentication method at the moment along with the most accurate form of interacting with a user w.r.t. authentication process. The generic model designed and verified with proof-of-concept implementation constitutes a foundation for building further adaptable and extensible multi-factor context-dependent systems for mobile authentication.

Keywords Adaptable authentication · Adaptable access control · Biometric authentication · Context-based authentication · Mobile authentication · Mobile devices

This research work has been supported by the Polish National Science Centre Grant No. DEC-2012/07/B/ST6/01523.

✉ Adam Wójtowicz
awojtow@kti.ue.poznan.pl

[1] Department of Information Technology, Poznań University of Economics and Business, Al. Niepodległości 10, 61-875 Poznan, Poland

[2] The Faculty of Mathematics and Computer Science, Adam Mickiewicz University, ul. Umultowska 87, 61-614 Poznan, Poland

1 Introduction and motivation

Nowadays, the mobile revolution is observed. Mobile services generate growing data transfer with thousands, if not millions, of mobile applications. They are usually based on BYOD (bring your own device) model which makes secure means of mobile user authentication a necessity. It concerns authentication of users on their mobile devices (e.g., unlocking a device), authentication of mobile users in remote services (e.g., to authorize transactions), and authentication of digital documents (e.g., verifying signature of a message sent to a mobile device). Means of user authentication used so far, such as passwords, PINs, or graphic patterns, are an inadequate choice for the new mobile world for a number of reasons. They are relatively easy to eavesdrop in untrusted environments (e.g., industrial cameras can record mobile users almost everywhere). They are also either uncomfortable for users to input on mobile device due to complexity, or trivial for brute force attacks (in case of short passwords) and for other attacks (graphic patterns for touchscreens). What is even worse, users tend to disable authentication at all, if they are forced to input cryptographically strong passwords with small mobile virtual keyboard [7]. Almost one out of three users does not protect his or her mobile device with a password, and 69 % of Europe citizens have stored or accessed confidential data using mobile devices in 2012 [27]. This is all the more true in case of strong two-factor authentication (combination with one-time passwords or peripheral devices), which is time-consuming, and therefore frequently switched off by the users.

Fortunately, in this area, biometrical authentication techniques seem to be promising for mobile users. They eliminate the problem of memorizing and typing in a number of complicated passwords, and the problem of

Published online: 08 February 2016

carrying and using other identifiers (e.g., credit cards). When properly implemented, authentication with biometrics is natural, seamless, fast, and secure even within untrusted environments. Uniqueness of biometrical features minimizes error rate, and using biometrics combined with other access control means reduces the risk of a successful intrusion. It is worth noting that many of biometric authentication schemes can be easily implemented on mobile devices taking advantage of already existing built-in device sensors such as cameras or microphones, or, as in the case of latest iPhone 6s or Samsung Galaxy S5, built-in fingerprint sensor. Biometrics has appeared on the ground of mass consumer electronics, and it is based on sensors that are cheap and reliable enough. New applications allowing mobile user to be biometrically authenticated not only on her device but also in a remote service or store can be perceived as a trigger for a new m-commerce trend.

The need for seamless service usage even in diversified external conditions is the reason why users switch to mobile devices and applications. Context-based approaches applied to the mobile applications are the attempt to address this challenge. They receive and interpret information regarding current environment conditions that compose the context at the given moment in order to make usage of mobile applications more efficient. Users do not have to manually switch between options and preferences, since mobile device automatically specifies both the content to be presented and the form of the presentation. Support for the context dependency seems to be one of the ultimate goals of the ICT for e-society—providing highest possible process automation and intelligence that is able to semantically interpret information coming from external sources.

The approach presented in this article is based on two main groups of techniques mentioned above, i.e., biometrics and context dependency. Having access to several authentication methods, including non-biometric and biometric ones, the mobile device can be equipped with an application adapting itself to constantly changing external conditions. The simplest example scenario would be riding the bicycle or driving a car that makes it hard to authenticate in the device with the regular passwords that absorbs one's attention. The proposed context-based solution can check whether there are such factors at the given moment and, if so, can propose the most accurate authentication method along with the most accurate form of informing the user about the chosen method. The factors that have to be taken into account can be grouped into two categories: the presence of the conditions that decrease the quality of the given biometric signal (e.g., too high noise level for the voice biometrics), or the presence of the conditions that make given biometrics undesirable for user at the moment (e.g., need for discreet device usage during the business meeting, which also eliminates the voice biometrics). The goal of the proposed approach is to design context-based biometric authentication solution assuming that it has to be as easy to implement as possible, take advantage of pre-existing mobile sensors, and be dynamically adaptable to current user profile. The work also concerns identification of the critical points of the system and the future development perspectives.

The initial section of the article contains description of biometric authentication methods and biometric data processing, including context-based authentication, as well as an analysis of the existing works. In the subsequent three sections of the article, the proposed model is elaborated in detail, discussed, and the whole work is concluded.

2 Related work

2.1 Biometric authentication

Biometric authentication (referred to as biometrics) consists of three steps: acquisition of biometric data with the sensor, converting the data to digital template, and comparison of the template to a reference template. This process can be used for user identification (one-to-many model, e.g., to identify mobile user for a remote service) as well as for user verification (one-to-one model, e.g., to verify whether it is the owner who tries to unlock the device).

Biometric data represent biometric features of the human body, which is "something you are" authentication factor, contrary to "something you know" (e.g., password), "something you have" (e.g., token), or "where you are" (specific mobile systems). Biometric features can be divided into two main groups: physiological (e.g., fingerprints, face features, DNA) and behavioral (e.g., typing characteristics, voice, gait). Biometric features have the properties of universality, individuality, permanence, collectability, and performance.

However, it has to be stressed that there is no "ideal biometrics." Application of the given biometry is always a trade-off between security, comfort, invasiveness, and cost [17]. Similar constatation can be made regarding algorithms comparing biometrical sample with the reference template. While password or access card verification works according to Boolean logic, in case of biometry the process is more complex since it is impossible to acquire two identical biometric samples, among others due to environment conditions (or context). False acceptance and false reject errors occur, and corresponding measures are used [29], namely FAR (false acceptance rate) and FRR (false reject rate). CER (crossover error rate) is an error rate (and

sensor sensitivity setting) where FAR and FRR are equal. In the following subsections, biometrics that are or potentially can be used in the mobile devices have been described.

Fingerprints Factors affecting quality of fingerprints acquisition include dirt, humidity, skin tensility, pattern location, and orientation. The following acquisition technologies are used (usually in non-mobile devices): optical sensors, which are cheap but easy to circumvent and dirt sensitive; capacitive sensors, dirt and humidity sensitive; thermal sensors, temperature sensitive; and ultrasonic sensors, expensive but hard to circumvent, since they analyze not only fingerprints but also finger physical properties, such as blood vessels. The example of off-the-shelf fingerprint solutions designed for mobile devices is Tactivo by Precise Biometrics [22]. The biometrical patterns are stored either on a device or in a smart card (the card itself can be used as an additional authentication factor). Another example of similar solution is iFMID by S.I.C. Biometrics [25], where three options for pattern storage are available: on device, on corporate servers, or service provider servers. Both solutions support CAC (common access card) and PIV (personal identity verification) standards.

Face Face biometrics usage is unobtrusive for users due to noninvasiveness and ease to collect the data with a regular camera. Algorithms processing face images can compare either face geometry (geometrical relations between selected details) or vectors describing whole face images. Nowadays, researches on face 3D models are conducted. Such approaches allow for face recognition from different angles and make successful attack much more difficult [1]. Lighting, camera position, glasses, clothes, aging, and other face changes are the factors that impact the quality of face recognition. FastAccess Anywhere is a face recognition application designed for iOS, Android, and Windows OSs [24]. It secures both access to a device and to Web sites and applications. Second authentication factor can be employed optionally. The application can distinguish between a face and a face image. Additionally, multiple devices can be synchronized and used after single authentication. For iOS, FaceVault [21] has been designed which, according to the producer, offers face recognition regardless of glasses or makeup change. Recognition is performed on the server side.

Voice Voice recognition, as in the case of face, is a method that is easy to apply in mobile devices, since software only is required. Authentication can be performed according to one of four schemes, where user has to verbalize fixed phrase, phrase send by the system (each time new), freely chosen phrase, or a conversation which verifies both knowledge and voice characteristics. Factors that affect quality of the voice recognition include background noise, human emotional state, aging, or respiratory diseases. An example of a solution that adapts the preexisting corporate access control to the voice authentication (maintaining password-based authentication if desired) is Mobile VocalPassword by Nuance [20].

Iris Iris image can be acquired with regular camera or near-infrared scan. In the latter case, influence of the external factors, causing, e.g., light reflexes, can be reduced. The structure of the iris is analyzed, not the color (although the color can be an additional aspect). Taking advantage of the fact that eye pupil constantly adapts to changing light conditions, advanced iris-based techniques can distinguish real eye from the its static image used by an attacker.

Finger veins Finger/palm veins recognition is one of the most accurate biometric authentication methods. The examples include touchless Fujitsu system, PalmSecure [10], or Hitachi, VeinID [15]. Vascular technology is considered the least privacy intrusive, since it is hard to collect samples without ones acceptance. Also data acquisition speed, recognition reliability, pattern persistence during lifetime, and high security (it is impossible to use even cut off finger to break access control) are the advantages of the technology. The accuracy of the scanning process can be decreased by light sources, specific kind of dirt, and finger position [28].

Facial thermography Face thermogram is, contrary to regular face image, resistant to variable lighting conditions or other face image changes [5]. However, specific camera has to be used, having thermal imaging sensor. Other difficulties related to recognition process include variable nose and mouth temperatures caused by respiration, or glasses blocking thermal imaging. Also thermal face image is dependent on intensive physical activity, or eating [4].

Electrical properties of human body Touchscreen recognizing user based on his or her electrical properties has been constructed [13]. The method needs subsequent work that would reduce the impact of the environment on the collected data; therefore, nowadays it could be applied as a supporting biometric factor only.

Touchscreen gestures Users can be identified based on the way how they use touchscreen. In the research experiments [9], touchscreen gestures profile were defined based on 53 distinct features (e.g., position of the trace, movement direction and speed, pressure, distance between points).

2.2 Combining biometrics

If authentication with a single biometrics is not secure enough for the given application, it can be combined with

second authentication factor (biometric or other group, i.e., possession, knowledge, location). Biometrics combinations are performed according to 6 different models [5]:

- different biometrics,
- multiple use of one biometrics (e.g., acquisition of the data from many fingers, or from the second eye),
- multiple sampling of one biometrics,
- multiple sampling with different sensors,
- multiple comparators,
- multi-factor authentication.

Loose coupling and tight coupling of different biometrics can be distinguished [5]. In loose-coupled approach, a process of comparing of biometric sample with template is performed for different biometrics separately. Final authentication decision is a conjunction/disjunction of independent subdecisions. In turn, in tight-coupled approach biometric samples are set together in a common vector, which is a base for the final decision.

A protocol for the factors acquisition is not always static, since it can be based on dynamic requests generated exclusively for a given user. An example of such approach is authentication based on voice responses, which is a combination of biometric feature and a confidential knowledge factor. As the number of responses increases, the analyzed sample gets larger; thus, the probability of right authentication decision increases.

2.3 Continuous authentication

In the standard access control models, authentication is performed once, in the logging phase. Since in the mobile scenarios devices are not physically separated from the intruders, standard models can be insufficient for the effective security. Applying biometrics for mobile access control allows for continuous authentication during the session, without additional interactions with a user. Frequently repetitive face or iris verifications [26], electrocardiogram monitoring, or behavioral biometrics can be a base of continuous verification. In this context, the set of all biometrics containing only "hard" factors is extended to include also "soft" factors (e.g., color of clothing). They have high error rate, but are useful in continuous authentication schemes. In the mobile scenarios, low FRR is significant for the unobtrusiveness of the process [19]. Even if at the same time FAR is higher, it is neutralized by the fact of frequent verifications.

An example of commercially available mobile device with continuous authentication is Nymi by Bionym [11]. It employs an electronic bracelet connected wirelessly to the mobile device, collecting continuously user's electrocardiogram data used for authentication. Authentication takes into account current bracelet–device distance. Additionally, it allows for defining gesture-based custom interactions using bracelet built-in gyroscope and accelerometer. Another example, resulting from research community efforts, encompasses continuous authentication in medical system environment [2]. Hospital workstations have been integrated through servers with portable staff's smart cards. Card holders moving away from workstations are instantly logged out.

2.4 Context-based biometric authentication on mobile devices

A number of research works on biometric authentication on mobile devices exist, e.g., [3, 31]; however, only few of them tackle the issues of context sensitivity and adaptation. In the existing articles that focus on context-based methods for mobile devices, authors divide sensors that are data sources for the context into the classes of physical (related to device location and environment) and logical (describing device's state), as well as into the classes of active (activated sensor sends data) and passive (requiring user actions to send data) [30]. Also biometric authentication itself can be either passive (working in the background) or active (requiring user actions to authenticate). Therefore, the context notion and its practical usage with biometry is considered in various ways.

In some approaches, context is used to improve efficiency of systems that are composed of not only one handheld device, but many diverse and interoperable devices (cf. the idea of Internet of Things). For example, in [12, 16] a healthcare supporting system decides which sensor/device is chosen to collect data and considers sensor limitations (e.g., lack of Internet connection). However, in these works the factors that impact the user authentication are predefined, and the process of choosing authentication method does not depend on environmental conditions; just the continuous multi-factor authentication is applied. The authors only suggest that context could impact the quality of stored and acquired credential patterns matching.

In other approaches, the relation between environment conditions and authentication method to be applied is defined in a different way, i.e., context itself is treated as a passive authentication factor. At the same time, context can be used to determine a security level which indicates the strength of an active factor required to successfully log in or unlock the device. Such approach, presented in [14], is focused on combining a passive factor (or a set of passive factors) with a dynamically chosen active factor. The selection of the latter depends on security level. If the context pattern indicates the security level is high, a "weaker" method is selected as the second factor. In this work, biometric active factors have not been used (just PIN and passwords). Other limitation of this work concerns the

fact that its validation has been performed on a simple model assuming user location as a single passive authentication factor. An approach based on similar assumptions has been presented in [23]. The research is focused on dynamic selection of authentication time and applications for which authentication is required. The active authentication method is PIN only. As for biometric features, they are treated as a passive factor, and only voice is collected using the mobile device sensor (face signal is used as well, but using stationary camera).

Also self-adapting approaches have been proposed. For instance, in [30] a classifier has been taught to detect sets of conditions reflecting typical usage schemes of eligible users. Within this work, context data are used to form a behavioral pattern perceived as biometric features, and as such, they support the authentication process. Emphasis is put on the authentication based on context data only, which is a controversial approach since attack schemes based on "soft" behavioral biometry can be easily conducted. Similarly in [18] continuous authentication model measuring confidence based on comprehensive user behavior sets has been proposed, taking into account also disabilities specificity.

It can be noted that in some research similar input as in the above-mentioned papers is used to solve different problems. For example, in [6] the authors combine context and biometric data, not to choose optimal method nor to authenticate user passively on mobile device. Instead, their goal is to process biometric sample using the context data to produce cryptographic contextual pseudo-identities that facilitate authentication in ubiquitous services.

In any of these works, the problem of context impact on the quality of the biometric samples (for various biometric features) acquired under changing environmental conditions in the process of active authentication is not addressed. Also the possibility of determining, based on the context data, user's intended interaction scheme during authentication is not explored. Moreover, in context-based biometric authentication systems, after one biometric method is chosen, a user has to be informed (and react accordingly) about the choice with appropriate modality, that also has to be chosen taking into account the current context limitations. Existing models do not adapt user interactions process related to the authentication to the limitations of the context.

3 Model for context-based biometric authentication for mobile devices

3.1 Assumptions

The goal of this work is to propose a system for mobile devices that, based on context data (e.g., location, noise, usage mode), chooses the optimal biometrics for authentication along with optimal communication method to inform the user about the choice and interact with him. Sample context-dependent factors that impact the biometrics are depicted in Fig. 1.

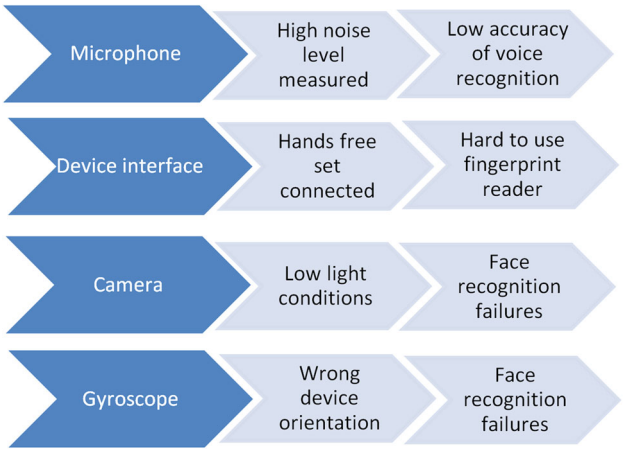


Fig. 1 Example of the factors impacting effectiveness of biometry usage

The proposed system can be applied in the following usage scenarios:

- mobile device unlocking;
- authentication in remote services or mobile applications assuming one-factor authentication;
- choosing biometric method that is the second one in two-factor authentication (e.g., in financial transaction authentication/authorization schemes).

The system can be extended in order to:

- support choosing more than one biometry;
- support choosing non-biometric authentication methods.

Sensors in mobile devices When designing context-based solution, one has to start with identification of accessible types of information that can be acquired to build a context. Not all built-in sensors provide data that can be interpreted to form a useful knowledge about the context. The most popular mobile sensors set with the results of usefulness analysis for biometrical authentication is presented in Table 1.

Finally, for the purpose of the proposed model it has been assumed that devices are equipped with the following sensors providing context data:

- camera,
- microphone,
- movement sensor,
- thermometer,
- accelerometer/gyroscope.

Table 1 Usefulness of the mobile device sensor's data for biometrical authentication

Sensor	Data type	Usefulness
Camera	Images	Useful. Image processing can be used to low-/high-lighting assessment
Microphone	Sound	Useful. Sound signal analysis can be used to noise level and noise type assessment
Accelerometer/gyroscope	Linear acceleration/angular position	Useful. To identify type of shakes or user movement
Barometer	Pressure/altitude	Low usefulness
Hygrometer	Humidity	Low usefulness
Thermometer	Temperature	Useful
GPS module	Location, movement speed	Useful
Gesture sensor	Information about using the gestures for touchless interactions	Useful
Magnetometer	Direction and magnitude of magnetic field (works as a compass)	Not useful
Proximity sensor	Centimeters or Boolean values (depending on the sensor, e.g., Apple's use NEAR/FAR)	Useful as a supporting sensor. Usually range is limited to up to 5 cm
Hall sensor	Magnetic field magnitude	Can be useful to check whether device is inserted in a case (e.g., to wake up device automatically)
Light sensor (RGB)	Intensity of RGB colors	Useful, but camera can be used as well

Authentication and interaction methods In Sect. 2, biometrical authentication methods that either are used or are subject of research have been described. The most robust ones include fingerprints, face, and voice recognition. These three authentication methods are applied to the proposed model. Regarding methods of user interaction for the optimal way of informing a user about the chosen authentication, also three methods are applied: screen interaction (text message, touch reaction), voice interaction (voice sentences or signals and voice reaction), vibration interaction (different kinds of vibrations and shaking reaction).

Sensor data discretization Each result of sensor measurement is discretized before it is passed to the decision process. For example, temperature scale is divided into two ranges (less than and more than 0 °C), based on a priori knowledge regarding device usability and user limitation (gloves) in the subzero temperatures. However, the initial discretization ranges are only the starting point for the self-adapting process, which will be elaborated in the further sections.

Authentication and presentation constraints Predefined constraints constitute a starting point for the self-adapting process. They are based on:

- The knowledge regarding efficiency of the given biometrics w.r.t. the set of external conditions, e.g., high FRR in case of low-light conditions for face recognition.
- The knowledge regarding typical user behavior and his or her limitation in certain situations, e.g., smartphone muting is interpreted as silent usage user intention and therefore voice authentication is excluded.

Constraints resulting from typical user behaviors can be replaced with constraints resulting from initial learning phase. In such case, when biometric authentication is needed, all the biometric methods are activated, and the fact that one of them is used is recorded as the choice for the given set of environment conditions. The constraints are adjusted iteratively, as it is described in the further sections. The learning can be performed locally in the device, or remotely in the service collecting the usage data from a number of devices.

3.2 Decision process

Defining a user situation based on criteria values According to the criteria listed in Table 2, every usage situation is represented by a vector of criteria values. Each criterion value is an integer from 1 to t (where $t \geq 2$). Examples of vectors have been presented in Table 3. They reflect the following situations:

1. A user walks in a street in the summer. Speed is low, lighting is good, noise level is low. The user has not muted her phone.
2. A user drives a car late night in the winter. Speakerphone is plugged in.
3. A user walks through the passenger coach in the train.
4. A device is lying on the table, and a user interacts with it with her gestures.

Table 2 Criteria used in the model

	Criterion	Description	Values	Example of how criterion value impacts the context
1.	Sound	User profile settings: sound on or off	1—sound is off 2—sound is on	Sound disabled implies silence requirement; voice authentication is avoided
2.	Vibrations	User profile settings: vibrations on or off	1—vibrations are off 2—vibrations are on	Vibrations disabled implies they are not used to inform the user about chosen authentication method
3.	Type of shakes	Type of shakes registered by the device. Based on shakes characteristics, it is possible to determine whether a user is walking or not	1—walking 2—device is not moving 3—shakes caused by a non-walking movement	Shakes typical for walking in conjunction with moving speed registered imply avoiding face recognition method
4.	Movement speed	Movement speed registered based on GPS module data	1—0 km/h; 2—low speed (walking), <3 km/h 3—high human speed, 3-30 km/h 4—high-speed vehicles, >30 km/h	Vehicle speed in conjunction with speakerphone connected implies avoiding fingerprint authentication
5.	Lighting	Light intensity measured with camera or built-in light sensor	1—light intensity too low 2—optimal light intensity 3—light intensity too high	Too high light intensity decreases display visibility. Information regarding the chosen method of authentication has to be passed using voice or vibrations
6.	Noise level	Noise level (measured in dB). Noise level right before authentication impacts SNR	1—acceptable level 2—noise level too high	Too high noise level disturbs voice authentication process
7.	Type of noise	Dominating type of noise. It is an element building the usage context. Also it influences the algorithm choice. The effectiveness of the recognition depends on type of noise	1—voices, talks 2—street 3—music 4—other	If human voice noise is present and, at the same time, voice is not preferred in the ranking, voice biometrics is excluded from the usage
8.	Temperature	Temperature measured by the mobile device. Alternatively, temperature value can be received from the weather forecast service (less accurate because of lack on indoor/outdoor location information)	1—<0 °C 2—≥0 °C	Temperature <0 °C increases probability that user has limited ability to use fingerprint authentication
9.	Move sensor	Move sensor that allows for touchless information transfer	1—move sensor used 2—move sensor not used	If move sensor is used, fingerprint authentication is excluded
10.	Peripheral device	Peripheral devices in use, or built-in speakerphone in use	1—no peripherals 2—speakerphone 3—headphones	Speakerphone connected or turned on excludes authentication with fingerprints

Table 3 Examples of situations—vectors of criteria values

	Sound	Vibration	Type of shakes	Movement speed	Lighting	Noise level	Type of noise	Temperature	Move sensor	Peripheral device
1.	1	1	1	2	2	1	2	2	2	1
2.	2	2	2	4	2	1	4	2	2	2
3.	2	2	1	4	1	2	4	2	2	1
4.	2	2	2	1	1	1	4	2	1	1
5.	2	2	2	3	1	1	2	1	2	1

Table 4 Sample authentication and communication preference rankings

Rank	Authentication method	Rank	Communication method
1.	Face recognition	1.	Screen communication
2.	Fingerprints	2.	Vibrations
3.	Voice recognition	3.	Voice message

5. A user moves in a hurry. It is winter, acceptable lighting.

According to the proposed approach, a user has to define a complete ranking of the preferences regarding authentication and presentation methods. Therefore, taking into account vector values and user preferences, the system always has enough information to:

- Interpret context data with respect to user preferences. Some criteria values combinations are significant only in conjunction with specific preference combinations.
- Make final choice—if there are more than one authentication/presentation methods allowed after the first phase of the decision process.

Sample representation of authentication/communication preference rankings is illustrated in Table 4. Both rankings have to be complete.

Total number of theoretically possible situations within the proposed model can be expressed by the following formula:

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

where k is criteria number, x_k number of values for criterion k, p_1 number of authentication methods, and p_2 number of communication methods.

Excluding criteria that cannot be used Next step is specifying which criteria cannot be used in a given situation. Majority of constraints are complex, i.e., caused by coexistence of several criteria values at the same time. There are also few simple constraints related to existence of one criteria value.

Criteria and preferences constraints In the proposed model, the subsequent phase is called *Criteria and preferences constraints* (Fig. 2). This phase is required since for some criteria combinations it has to be taken into account on which absolute (e.g., fingerprints ranked third) or relative (e.g., face recognition before voice recognition) position an authentication method is situated. *Criteria and preferences constrains* are predefined or defined during an initial learning phase. For example, for the lighting criterion the minimal value 1 means insufficient lighting and maximal value 6 means excessive lighting making screen usage arduous. Value 3 reflects lighting which is sufficient but slightly decreasing recognition efficiency (measured with CER). Therefore, constraint rules can be defined such as if value 3 on the lighting criterion appears and, at the same time, face recognition is ranked 2 or 3, then face recognition is excluded from the authentication.

Final authentication method choice The choice of one biometrical authentication method is held through:

- elimination—finally a method that has not been excluded is chosen;
- preferences analysis—applied if after elimination there is more than one method chosen or none of them is chosen.

In the proposed approach, each time when authentication method in chosen by the system, the user can override the choice manually. In such case, his or her decision is registered along with complete situation vector and later used as a part of a learning set.

3.3 Learning phase

Initial learning phase In the initial learning phase, when the mobile device user has to be authenticated, all biometrical sensors are activated. The user is authenticated with the method that is used successfully as the first one, e.g., putting his/her finger on a fingerprint scanner is equivalent to choosing the fingerprint biometrics. After a learning set is gathered, constraint rules are induced. To shorten the time of the learning phase, subsets of the rules are predefined.

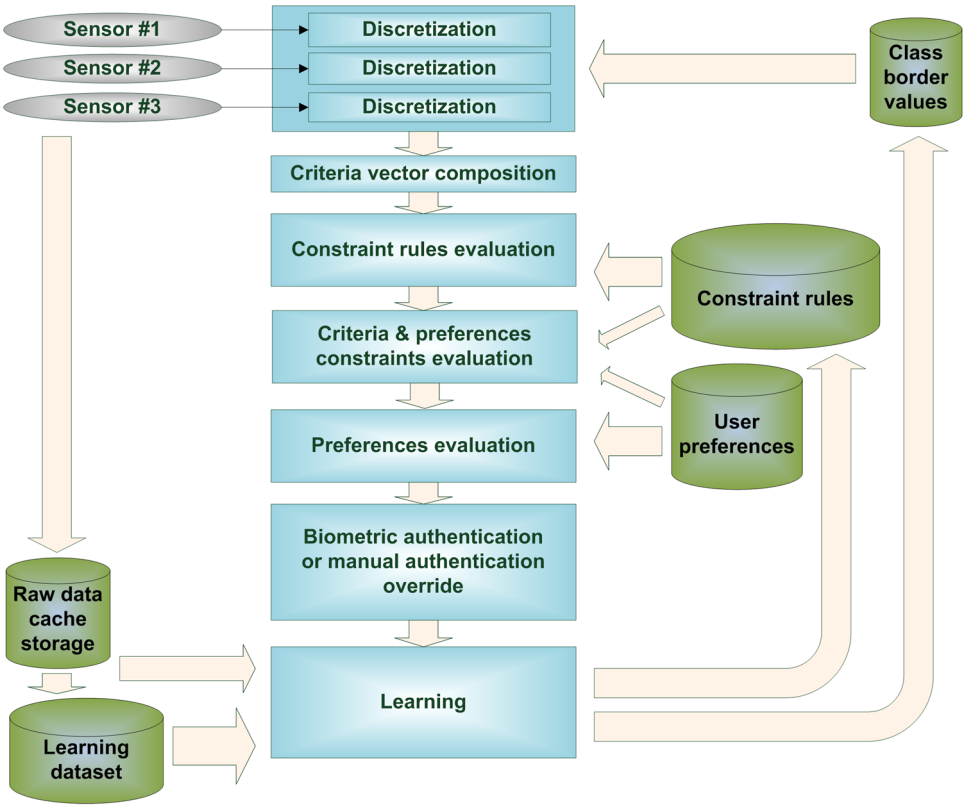


Fig. 2 Decision process in the context-based biometric authentication

Changing context criteria classes In the first phase, sensor data are discretized into integer values corresponding to distinct situations. In the learning phase, as the learning progresses, initial discretization can be modified by:

- Adding/removing classes.
  For example, initially, lighting values are discretized into 3 classes: 1—"too dark," 2—"optimal," 3—"too bright." During the learning phase, this discretization can be modified into, e.g., 1—"too dark," 2—"indoor," 3—"outdoor," 4—"too bright."
- Moving the borders of the existing classes.
  For example, during the learning phase it turns out that in the temperature 5 °C a user still does not use fingerprint authentication (because of gloves). Then, the value of the border between classes 1 and 2 is increased.

Constraint rules modification Constraint rules set is improved by:

- Rule removal.
  For example, assume that the user has overridden the chosen biometrics with face recognition several times (that has been earlier excluded by constraint rules). The constraint rules can overlap each other, that is several constraint rules can exclude common biometric method at the same time. For example, overridden choices in situations s_1, s_2, s_3 have been made because of the constraints $s_1 = \{c_1, c_2, c_3\}$, $s_2 = \{c_2, c_3\}$, $s_3 = \{c_1, c_2\}$. Therefore, the constraint $c2$ will be removed.
- Rules adding suggestion.
  Rules adding suggestion is performed when more than one authentication method is allowed after applying the constraint rules, and the subsequent system's choice is based on user's preferences, but the user has overridden the choice. It means that initially too many methods have been accepted.

Indoor/outdoor classification The efficiency of using the criteria for proper context description depends strongly on the fact whether user position is outdoor or indoor (inside a building or a vehicle). For example, taking into account the time of the day and the season does impact the context only if the user is in an outdoor location, where the influence of the weather, lighting, transport, and noise can be significant. Indoor/outdoor distinction is usually not possible, even based on digital maps containing the building placement data. However, the system can be taught how to determine the indoor/outdoor value based on combinations of different criteria.

- Verification with Web service. Comparing the sensor-collected temperature to a value of a weather parameter provided by a Web service. If the difference is significant, the indoor/outdoor value can be set ad hoc. In cases when the values are similar, indoor/outdoor value can be still determined using earlier measurements that are geotagged.
- Noise amplitude. Works in some large cities.
- Noise type. Indoor noise type is different than outdoor noise type.
- Lighting conditions inadequate to a daytime and to a season. If the light intensity is not adequate to given daytime and season, then probability of an indoor location is increased.
- Shakes/movement speed. If the device is not moved for a longer period of time, then probability of an indoor location is increased.

False situation identity Assume that two following situation vectors are given:

$$s_1 = [2, 2, 1, 3, 1, 2, 2, 2, 2, 1]$$
$$s_2 = [2, 2, 1, 3, 1, 2, 2, 2, 2, 3]$$

Also a constraint rule is given that makes it impossible for the user to authenticate with his face in the situation when he walks in a hurry in a street:

$$c_1 = [-, -, 1, 3, -, -, -, -, -, -]$$

However, there might appear such a combination of the other criteria values that cancels the constraint. Theoretically, it is possible that vectors s_1, s_2 do not reflect the situation that is intended to be constrained by c_1 (fast walk). For example, a user may be on board the slowly moving vehicle such as ferry—the speed measured by the GPS is absolute, and the relative walking speed is lower. In such case, the constraint rule c_1 would exclude the authentication method that is in fact applicable. The learning systems is designed to solve such problems by adding an additional criterion, or by extending the model with additional criterion values.

3.4 Model evaluation

The core of the presented model, i.e., the decision process, has been evaluated with proof-of-concept software prototype. The implemented VBA application applies rule-based authentication and presentation constraints to situations (contexts) represented by criteria value vectors and produces authentication and presentation decision. The evaluation has been performed in two phases. The goal of the first phase was to confirm that for every possible context unambiguous decisions are obtained. The goal of the second phase was to verify whether obtained decisions are consistent with the semantics of the constraints. For both phases, authentication constraints explained in Table 5 and presentation constraints explained in Table 6 have been used.

In the first phase of the evaluation, the prototype system has been run for every vector value combination. Formula (1) presented in the previous section expresses the total number of theoretically possible situations. As a result, unambiguous authentication and presentation decisions have been obtained for every possible context.

In the second phase of the evaluation, all the vector values along with calculated decisions have constituted input dataset for decision trees induction, that have been intended for human interpretation of the decision process. Total number of situation expressed by Formula (1)

Table 5 Authentication constraints used for the evaluation

	Constraints vector	Semantics	Authentication method excluded
1.	[1 1 2 1 0 0 0 0 0 0]	Sound and vibration turned off, user is not moving	Voice recognition
2.	[1 1 1 1 0 0 0 0 0 1]	Sound and vibration turned off, user walks, no peripherals	Voice recognition
3.	[0 0 0 0 0 2 0 0 0 0]	Noise too high	Voice recognition
4.	[0 0 0 0 0 0 1 0 0 0]	Noise type: conversation	Voice recognition
5.	[0 0 0 0 0 0 3 0 0 0]	Noise type: music	Voice recognition
6.	[0 0 0 0 0 0 0 0 1 0]	Move sensor active	Fingerprints
7.	[0 0 0 0 0 0 0 1 0 0]	Temperature below 0 °C	Fingerprints
8.	[0 0 2 1 0 0 0 0 0 2]	User is not moving, speakerphone is connected	Fingerprints
9.	[0 0 3 4 0 0 0 0 0 2]	User is moving with vehicle, speakerphone is connected	Fingerprints
10.	[0 0 0 0 1 0 0 0 0 0]	Lighting too low (too dark)	Face recognition
11.	[0 0 1 3 0 0 2 0 0 0]	User walks fast (hurry)	Face recognition
12.	[0 0 1 0 0 0 0 0 0 3]	User walks, headphones in use	Face recognition

Table 6 Constraints for user interactions

	Constraints vector	Semantics	Interaction method excluded
1.	[1 0 0 0 0 0 0 0 0 0]	Sound turned off	Voice message
2.	[0 1 0 0 0 0 0 0 0 0]	Vibrations turned off	Vibration-based information
3.	[0 0 0 0 0 2 0 0 0 0]	Noise too high	Voice message
4.	[0 0 0 0 0 0 0 0 0 0]	Speakerphone is connected	Screen message
5.	[0 0 0 0 0 0 0 0 1 0]	Move sensor active	Vibration-based information
6.	[0 0 0 0 3 0 0 0 0 0]	Lighting too high	Screen message

includes also combinations for authentication and presentation preferences. However, in order to make the decision tree clear, the number of situations used for the trees generation does not include user preferences and thus is expressed by Formula (2):

$$\prod_{i=1}^{k} x_k \tag{2}$$

where k is criteria number, x_k number of values for criterion k.

Based on 9216 possible contexts (vector value combination), two trees have been induced: the first one that is used for authentication method selection and the second one for presentation method selection. Since the resulting trees have more than 100 nodes, only a fragment of one of the trees is illustrated in Fig. 3. Weka 3.6 application [8] implementing C4.5 (j48) algorithm has been used (top-down induction). The obtained decision trees, due to their completeness and "positive" outcome representation (as opposed to "negative" constraints), have allowed human expert to verify consistency of the calculated decisions with the intended semantics of the constraints.

```
J48 pruned tree
------------------

Lightining = a
|   Noise level = a
|   |   Temperature = a
|   |   |   Type of noise = a: nnn (192.0)
|   |   |   Type of noise = b
|   |   |   |   Sound = a
|   |   |   |   |   Vibrations = a
|   |   |   |   |   |   Type of shakes = a
|   |   |   |   |   |   |   Peripherial device = a: nnn (8.0)
|   |   |   |   |   |   |   Peripherial device = b: nnt (8.0)
|   |   |   |   |   |   |   Peripherial device = c: nnt (8.0)
|   |   |   |   |   |   Type of shakes = b: nnn (24.0)
|   |   |   |   |   Vibrations = b: nnt (48.0)
|   |   |   |   Sound = b: nnt (96.0)
|   |   |   Type of noise = c
|   |   |   |   Type of shakes = a: nnn (96.0)
|   |   |   |   Type of shakes = b
|   |   |   |   |   Sound = a
|   |   |   |   |   |   Vibrations = a: nnn (24.0)
|   |   |   |   |   |   Vibrations = b: nnt (24.0)
|   |   |   |   |   Sound = b: nnt (48.0)
|   |   |   Type of noise = d
|   |   |   |   Sound = a
|   |   |   |   |   Vibrations = a
|   |   |   |   |   |   Type of shakes = a
|   |   |   |   |   |   |   Peripherial device = a: nnn (8.0)
|   |   |   |   |   |   |   Peripherial device = b: nnt (8.0)
|   |   |   |   |   |   |   Peripherial device = c: nnt (8.0)
|   |   |   |   |   |   Type of shakes = b: nnn (24.0)
|   |   |   |   |   Vibrations = b: nnt (48.0)
```

Fig. 3 Fragment of the decision tree generated from the model data

4 Discussion

4.1 Delayed sensor data

If time interval between measurements is too high, there is a risk that the system chooses the authentication method based on inaccurate noise type and level, lighting level, or temperature. The usual real-life reason for this type of the measurement inaccuracy is the fact that right before authentication the mobile device is carried in the pocket, or briefcase, where the conditions are different from the environment. Possible solutions include:

- Adding *proximity sensor* criterion and modifying the constraint rules according to it.
- Adding environment conditions criteria, estimated based on daytime, year season, and weather conditions received from a Web service.
- Forcing the aquisition of the most current data from the sensors in the moment of taking the device out (checked with proximity sensor, Hall sensor, or both).

4.2 Two-factor authentication

Assuming m-banking application field of the proposed model, two-factor authentication for sensitive transaction protection is a necessity. Conforming to classical two-factor requirement, authentication process is composed of one of the "something user is" factors (face, fingerprints, voice) plus one of the "something user knows" factors. Examples of such combinations include confidential pass-phrase spoken by the user and recognized after user voice recognition or confidential sequence of fingerprints of several fingers. In the less security-sensitive scenarios, the authentication process can be composed of two factors of

the same category (e.g., "something user is"—face + fingerprints).

In order to extend the proposed model to the two-factor requirements, the following modifications have to be made:

1. Increasing the number of values for authentication method criterion. To the set of values that correspond to basic methods, pairs are added—two-element combinations.
2. Adding a new criterion: *Auth factors number*. Allowed values: 1 or 2.
3. Adding new constraints. The most important constraints to be added are ones that forbid one-factor methods if *Auth factors number* equals 2.

In case when biometric authentication methods are characterized by diversified FAR, FRR, or CER values, additional *Security sensitivity* criterion can be added, as well as constraints using it. Values of this criterion would correspond to the current authentication accuracy requirement (required by the active mobile application), e.g., m-banking application would require higher accuracy (in terms of FAR, FRR, or CER) than, for instance, device unlocking.

4.3 Authentication choice as user authorization for an application

Apart from the proposed context-based authentication choice model, a complementary model could be developed based on it. The idea is to use authentication choice as means of user authorization for a given application. It is based on the same approach as in the initial learning phase of the proposed model—after the device is activated, all biometrical sensors are activated at the same time (camera, microphone, fingerprint scanner, and potentially other). A user can authenticate himself or herself with a randomly chosen method. Depending on the choice, after successful authentication, the user is authorized to use resources of the given mobile or Web application and is redirected to it automatically. For instance, m-banking application can be bond to the stronger fingerprint biometrics, while augmented reality application—to the face recognition biometrics.

5 Conclusions

The main contribution of this work is creating a generic model for context-based biometric authentication for mobile devices and, on this basis, designing a system to be implemented on mobile devices in the actual stage of their technological development. Contrary to earlier works, context data are used in the process of active authentication to dynamically select biometric authentication method which results in two main features. The first one is the best possible quality of the biometric samples acquired under changing environmental conditions for various biometrics. The second one is the conformance of the selected authentication method with user's intended interaction scheme at the moment. What is more, not only the most accurate authentication method, but also the proper modality for informing the user about the choice and further interactions with him or her is determined by the system. The knowledge regarding context impact on quality of biometric sample acquisition and on intended usage scheme is stored in the adaptable knowledge base. As it has been intended, the presented model is easy to implement and in every possible context it is able to make an unambiguous choice.

The model has been verified by prototyping—the proof-of-concept software implementation has been developed. The system is extensible: The criteria and possible values can be seamlessly adjusted to major environments changes. Discreet, vector-based representation of the context situations is human interpretable; thus, semantic subclasses of the situation building the context can be easily distinguished (e.g., walking, street noise, freezing cold). Therefore, predefining or auditing the initial constraints is straightforward. As the system works, it could learn from the feedback (recorded context situations and user manual choices), and then the initial set of constraints could be adjusted. Finally, the system evaluation, as it has been intended, has allowed for identifying major conceptual obstacles that have to be faced by the designers and developers of such system.

Generally, the further development of biometric technologies and its applications in mobile devices will progress due to technological (faster authentication, better resilience to attacks) and business (cost reduction, scale effect, competitive advantage, users' fad) reasons. However, a real synergy effect can be obtained through integrating various biometric methods with each other and with context data. Therefore, the main idea for future development of the presented model and the system is to enable them to exchange anonymized learning sets between different users to accelerate learning phase and to increase its adaptability.

References

1. Abate AF, Nappi M, Riccio D, Sabatino G (2007) 2d and 3d face recognition: a survey. Pattern Recogn Lett 28:1885–1906
2. Bardram JE, Kjaer RE, Pedersem MO (2003) Context-aware user authentication—supporting proximity-based login in pervasive computing. UbiComp 2003 Ubiquitous Comput 2864:107–123
3. Bargal SA, Welles A, Chan CR, Howes S, Sclaroff S, Ragan E, Johnson C, Gill C (2015) Image-based ear biometric smartphone app for patient identification in field settings. In: Proceedings of the 10th international conference on computer vision theory and applications (VISIGRAPP 2015), pp 171–179
4. Bhowmik MK, Saha K, Majumder S, Majumder G, Saha A, Sarma AN, Bhattacharjee D, Basu DK, Nasipuri M (2011) Thermal infrared face recognition—a biometric identification technique for robust security system. In: Corcoran P (ed) Reviews, refinements and new ideas in face recognition. InTech, Rijeka, Croatia, pp 113–138
5. Bolle RM, Connel JH, Pankanti S, Ratha NK, Senior AW (2004) Guide to biometrics. Springer, Berlin
6. Buhan I, Lenzini G, Radomirovi S (2010) Contextual biometric-based authentication for ubiquitous services. Springer, Berlin
7. Confident Technologies (2011) Survey shows smartphone users choose convenience over security. http://confidenttechnologies.com/news_events/survey-shows-smartphone-users-choose-convenience-over-security. Accessed 16 May 2014
8. Drazin S, Montag M (2013) Decision tree analysis using weka. Machine learning-project II. University of Miami
9. Feng T, Liu Z, Kwon KA, Shi W, Carbunar B, Jiang Y, Nguyen N (2012) Continuous mobile authentication using touchscreen gestures. Institute of Electrical and Electronics Engineers, Waltham
10. Fujitsu (2011) Fujitsu palmsecure. http://www.fujitsu.com/global/solutions/business-technology/security/biometrics/. Accessed 20 June 2014
11. Goode A (2014) Bring your own finger—how mobile is bringing biometrics to consumers. Biometric Technology Today. Oxford, UK
12. Habib K, Torjusen A, Leister W (2014) A novel authentication framework based on biometric and radio fingerprinting. IARIA, Paris
13. Harrison C, Sato M, Poupyrev I (2012) Capacitive fingerprinting: exploring user differentiation by sensing electrical properties of the human body. Association for Computing Machinery, New York
14. Hayashi E, Das S, Amini S, Hong J, Oakley I (2013) Casa: context-aware scalable authentication. In: Proceedings of the ninth symposium on usable privacy and security (SOUPS '13). ACM, New York
15. Hitachi (2007) Hitachi veinid. http://www.hitachi.eu/veinid/. Accessed 20 June 2014
16. Leister W, Hamdi M, Abie H, Posland S (2014) An evaluation scenario for adaptive security in ehealth. IARIA, Nice
17. Martin L (2009) Biometrics. Morgan Kaufmann Publishers, Burlington, pp 645–659
18. Mhamed A, Zerkouk M, Husseini AE, Messabih B, Hassan BE (2013) Towards a context aware modeling of trust and access control based on the user behavior and capabilities. Springer, Berlin, Heidelberg
19. Niinuma K, Park U, Jain AK (2010) Soft biometric traits for continuous user. IEEE Trans Inf Forensics Secur IEEE Biom Compend 5:771–780
20. Nuance Communications (2014) Nuance voice biometrics. http://www.nuance.com/landing-pages/products/voicebiometrics/. Accessed 26 Feb 2014
21. Paul S (2012) Mashable. http://mashable.com/2012/04/27/facevault-app-facial-recognition/. Accessed 05-03-2014
22. Precise Biometrics (2013) Precise biometrics. http://www.precisebiometrics.com/. Accessed 26 Feb 2014
23. Riva O, Qin C, Strauss K, Lymberopoulos D (2012) Progressive authentication: deciding when to authenticate on mobile phones. In: Proceedings of the 21st USENIX conference on security symposium (Security'12), USENIX Association, Berkeley, p 15
24. Sensible Vision (2014) Fastaccess anywhere overview. http://www.sensiblevision.com/en-us/fastaccessanywhere/overview.aspx. Accessed 05 Mar 2014
25. S.I.C. Biometrics (2013) S.i.c. biometrics. http://www.sic.ca/. Accessed 26 Feb 2014
26. Sudarvizhi S, Sumathi S (2013) A review on continuous authentication using multimodal biometrics. Int J Emerg Technol Adv Eng 3:192–196
27. Symantec (2012) European mobile insights. Norton cybercrime report. Tech Rep. http://now-static.norton.com/now/en/pu/images/Promotions/2013/PDFs/NCR%20-%20%20Mobile%20-%20Europe%20FINAL%20FINAL.pdf. Accessed 26 Feb 2014
28. Vallabh H (2012) Authentication using finger-vein recognition. Univeristy of Johannesburg, Johannesburg
29. Whitman Me, Matford HJ (2010) Course technology. Cengage Learning, Boston, pp 344–345
30. Witte H, Rathgeb C, Busch C (2013) Context-aware mobile biometric authentication based on support vector machines. Institute of Electrical and Electronics Engineers, Cambridge
31. Yildirim N, Varol A (2015) Android based mobile application development for web login authentication using fingerprint recognition feature. In: Signal processing and communications applications conference (SIU), pp 2662–2665