Voice and face interaction evaluation of a mobile authentication platform

Oscar Miguel-Hurtado
School of Engineering and Digital Arts
University of Kent
Canterbury, United Kingdom
O.Miguel-Hurtado-98@kent.ac.uk

Richard Guest
School of Engineering and Digital Arts
University of Kent
Canterbury, United Kingdom
R.M.Guest@kent.ac.uk

Chiara Lunerti
School of Engineering and Digital Arts
University of Kent
Canterbury, United Kingdom
C.Lunerti@kent.ac.uk

***Abstract*—Biometric authentication in mobile devices has become a key aspect of application security. However, the use of dedicated sensors such as fingerprint/iris sensors may not always be feasible. As an alternative, the use of face and voice biometrics using the generic sensors integrated in smartphones is gaining momentum. This work applied the HBSI framework to analyise the user's interaction with the mobile PIDaaS platform that integrates voice and face authentication. Our analysis enables a thorough comparison between the user's interaction for these two modalities with the same population.**

Keywords— Biometrics, Evaluation, Interaction, Mobile, Usability, Voice, Face

I. Introduction

Since the introduction of fingerprint sensors in mobile devices, biometric authentication mechanisms have become a must-have feature for high-end smartphones. Alongside deadicated mobile fingerprint sensors some recently released smartphones also incorporate dedicated iris cameras, yet all models include generic sensors such as a frontal camera and microphones, which make face and voice biometrics available on any device. The dedicated biometric sensors generally provide a very fast, accurate and convenient way to perform several operations such as unlocking the smartphone's screen or authorising purchases, however, encrypted user templates from dedicated sensors are stored within the device, the control of which is typically the responsibility of the smartphone owner. Some service providers require more control over the user templates and cannot risk solely relying on the owner responsibility. For this reason, in order to utilise biometric authentication to a particular service, dedicated sensors may not be feasible. Therefore, the use of face and/or voice authentication with the frontal camera and/or the microphone has been adopted by several financial service providers, letting the provider control and supervise the enrolment process, and managing the user's templates. Smartphones are seen by many service providers as an excellent channel to reach many of their users. However, the inherent unconstrained nature of mobile devices and the wide demographic of potential users have also brought new challenges for the biometric community. Mobile devices can be used in many different environments, positions and usage scenarios, which also implies uncontrolled biometric sample acquisition. This creates a complex challenge for the analysis of the interaction between human and smartphones.

Within this context, the Private IDentification as a Service (PIDaaS) [1] EU-funded project aimed to create a multi-factor authentication solution for mobile devices on the cloud that can be easily incorporated to the workflow of third-party applications or service providers. In order to ensure the usability and effective interaction with the final PIDaaS Mobile Application (PMA), the Human-Biometric-Sensor Interaction (HBSI) framework using the integration proposed in our previous work [2] has been applied to a new version of the PMA to analyse how users interact with the different interfaces and enhance both the usability and the biometric performance of the final version of the system. As a continuation of the work presented in the 2016 ICCST Conference [2], the novel and extended HBSI framework proposed has been applied for the evaluation of a multi-modal biometric system, since the new version of the PMA integrates face and voice authentication. This experiment allowed a thorough comparison between face and voice biometric modalities from the same population.

In the following sections the HBSI framework (Section II) and the PIDaaS platform (Section III) are briefly introduced. The methodology used in this work is described in Section IV followed by the results obtained (Section V). Finally, in Section VI the conclusions of this work are discussed.

II. Biometric Interaction Analysis

The HBSI framework [3], devised by Purdue University, provides a set of interaction metrics to reach a thorough understanding of how users interact with biometric system and its impact on the biometric performance. The HBSI model is formed of three elements: human (the participants of this experiment), sensor (either the front camera or the microphone of the smartphone) and biometric system (the PIDaaS platform). We consider their corresponding interactions through ergonomics, usability and sample quality.

The human-sensor interaction is related to how the users present their biometric characteristics to the sensor. The sensor in the PMA is the front-camera and the microphone. The analysis of this interaction allows us to understand how to better guide users in order to obtain biometric samples of sufficient quality. The human-biometric system component establishes how users interact with the PIDaaS Platform, mostly through the PMA interface. In this case the evaluation

allows us to design a better user-centric interface for the final PMA version. The sensor-system interaction is measured through the quality of the biometric captured samples. The HBSI presentation metrics are defined by the type of presentations the users make, and their categorisation depends on whether the user makes a correct or incorrect presentation, whether the presentation was detected by the biometric system and whether the presentation was correctly classified by the biometric system [4]. Taking into account these three factors, the presentations are classified for unsuccessful interactions: Defective Interaction (DI), Failure to Detect (FTD), Concealed Interaction (CI), Failure to Process (FTP), False Interaction (FI); or for successful interactions: Successfully Processed Sample (SPS). This is shown in Figure 1.

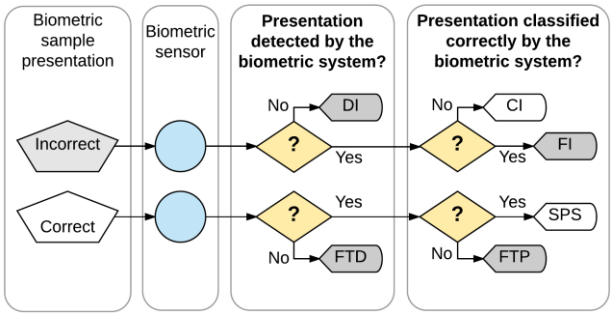

Fig. 1. HBSI presentation metrics

Furthermore, the HBSI framework defines metrics related to usability (satisfaction, eefficiency and effectiveness), cognitive (learnability and memorability), ergonomics (physical conditions) and signal processing (sample quality and processing capabilities) [4] to obtain a holistic view of the user's interaction with the biometric system. For further details about the HBSI please refer to [2-7].

This framework has been tested for a number of different modalities: hand geometry [5], fingerprint [4] and face [6]. The HBSI has also been applied to mobile implementations for dynamic signature [7]. A novel and extended implementation was proposed in our previous work [2,8] which incorporates mobile analytic tools and server logs to ensure sufficient data is captured.

III. The PIDaaS Platform

The PIDaaS platform provides an innovative identity management service relying on three main components: a) Biometric Template Protection Schemes, b) Life Management Platform and c) PIDaaS backend. The main user interface for the PIDaaS pplatform is the PMA. The new version analysed in this work integrates both face and voice biometrics (previous version only used voice). The PMA will be used to both register to the PIDaaS platform and perform authentication request from service providers. The face and the voice acquisition interfaces are shared for both enrolment and authentication processes. The users are presented with a voice introduction screen where they will be given instruction on how to provide voice samples. The user must repeat 6 times a random sequence of 5 numbers that appear on the screen. Every time a voice sample is recorded, a quality check module named Voice Activation Detection (VAD) analyses and classifies the samples as either correct or incorrect. The same procedure is followed for face registration where the users have to provide 3 face samples and a Face Activation Detection module (FAD) analyses and classifies them as either correct or incorrect. Once the biometrics samples are acquired, the user's templates are generated and stored.

IV. Experiment Methodology

A. Evaluation crew

The evaluation crew was recruited at two locations: the University of Kent in the United Kingdom; and the Norwegian University of Science and Technology in Norway. The only requirement to participate was to be at least 18 years old and be able to communicate in English. A total of 48 participants collaborated in the evaluation, with 24 participants from each location. All participants spoke in English, although they were originally from 19 different countries. The participants' age range was from 18 years old to 45. Figure 2 depicts the age and gender distributions of the evaluation crew.

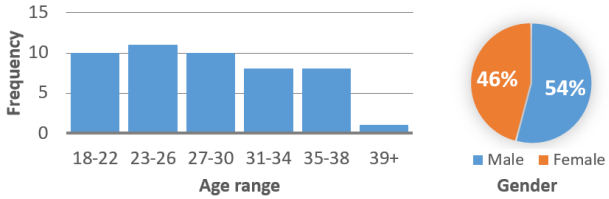

Fig. 2. Evaluation crew age histogram and gender distribution

B. Scenario settings and devices used

The experimental scenario set-up is based on our previous experiment [2] and the implementation lessons learnt. The main aim of the set-up is to recreate realistically an office environment. In our previous experiment, two video-cameras and two web-cameras were used to record the participant's interaction. In this work, the two video-cameras at the back of the participants have been removed as they made the participants feel uncomfortable. Webcams are less visible, participants are more used to them and feel more comfortable in their presence. Moreover, in our previous experiment it was also noticeable that users could not behave as if they were alone with the operator standing next to them. In this work, the operator was separated from the participants using a desk divider, to simulate more realistically the ideal scenario of being alone when using the app for the first time. The final scenario set-up is shown in Figure 3.

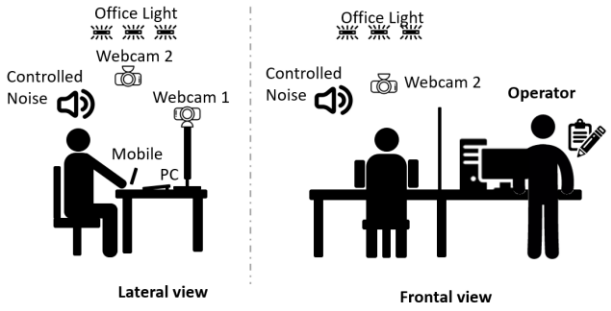

Fig. 3. Scenario settings

A realistic office environment has a background noise level ranging from a quiet office (~40dB) to a large office (~50dB) [10]. In order to simulate a large office environment, a background noise audio file was played and the volume adjusted to meet 50dB. The data collection room was windowless with light provided by fluorescent tubes located in the ceiling. As in our previous experiment, the smartphone used for the evaluation was an iPhone 5S.

C. User guidance and training

One of the main aims of the experiment was to understand and measure the participants' experience with their first contact with the PMA. The learnability (defined as "How easy is it for users to accomplish basic tasks the first time they encounter the design?" [10]) and memorability (when users return to the PMA after a period of not using it, how easily can they re-establish proficiency? [10]) of the biometric interfaces are key factors for user satisfaction. Therefore, user guidance and training was kept to a minimum – guidance was mostly provided by the participant information sheet. Participants were asked to behave as if the operator was not present in the room and to only ask for assistance when they did not know how to proceed when interacting with the PMA. A brief PMA manual was provided to the participants who decided as and when to consult the document.

The experiment was split into three sessions in different weeks. In the first session, the participants registered on the PIDaaS platform and created their voice and face templates. After registration, the participant was requested to reply 5 questions at the desktop PC using a bespoke software. These questions were intended to distract users between consecutive authentication requests in order to avoid simple repetition and therefore simulate a more realistic data collection. In order to submit the answer to each question, the participant needed to verify his/her identity using the PIDaaS platform, which triggered a push notification request in the mobile device. The participant then authenticates him/herself using the PMA. During the second and the third sessions, participants were asked to log in to the PIDaaS platform using the PMA, answer 10 questions, renew their voice and face templates and answer another 10 questions. Three of the last 5 authentications requests were carried out within noisy office environmental conditions. Upon the completion of the experimental sessions, the participants filled a post-experiment questionnaire about their perceptions regarding the PIDaaS platform.

D. HBSI evaluation metrics

In order to apply the HBSI framework for the biometric-interaction evaluation, the definition of correct and incorrect voice or face biometric sample presentation was defined.

A correct voice presentation was defined using the same description as in our previous experiment (refer to [2]). A correct face presentation occurs when the user places the head within the silhouette displayed within the capture interface. The face must be clearly visible and in focus, without any part covered or occluded, and the light conditions must be uniform over the image without any shadows. An incorrect face presentation is defined as a face presentation that does not fit the correct presentation definition. An incorrect presentation might be due to the following reasons: a) head not fully placed within the shadow-picture-frame, b) head too close/far within the shadow-picture-frame, c) strong lights from the background making the face not clearly visible, d) shadows over the face, e) face partially occluded by clothes or other covering.

Once the correct and incorrect presentations were defined, the six HBSI presentation categories (Figure 1) can be mapped within PIDaaS experiment context. Within this context, the experiment assumed that the microphone will always properly record while the PMA shows the sequence of five numbers to the participant. The experiment also assumed that the front-camera will be functional and generate a picture after pressing the appropriate button. These assumptions remove the possibility of a DI or FTD.

A CI occurred when the biometric system successfully classifies an incorrect presentation. This classification was made by the VAD or the FAD modules. Due to this misclassification, a CI will be sent to the biometric system for further processing and enrolment or comparison. On the other hand, if the VAD or the FAD modules classified an incorrect presentation as correct, the presentation will fall into the FI category. If there was a correct presentation and the biometrics system successfully classified as such, the presentation will fall into the Successfully Processed Sample (SPS) category and is processed by the biometric system. If the VAD or FAD modules classified a correct presentation as incorrect, the presentation will be categorised as FTP.

Along with the HBSI presentation metrics, the HBSI framework also included usability metrics of efficiency, effectiveness and satisfaction.

Efficiency was defined as the time spent on performing a task (enrolment or verification) once the users have learned how to proceed.

Effectiveness refers to the extent to which the product behaves in the way that users expect it to and the ease with which users can use it for their intend purpose. It was measured with the following indicators: **a)** % of errors detected by the test operator (incorrect voice or face presentations)**; b)** % of assists during performing a task; and **c)** task completions rate (% of successful voice and face presentations and correctly classified as such by the VAD or the FAD modules over the total number of first attempt presentations).

Satisfaction was measured by means of a questionnaire after the experiment. As in our previous work, the participants were asked to provide their degree of satisfaction for different aspects of the PMA, including voice and face enrolment and verification. Moreover, in this experiment the System Usability Scale (SUS) usability questionnaire [11] has been also applied. The use of standardised satisfaction questionnaires provides a formal way to communicate the results, allowing the comparison with other evaluations. The SUS was created by Brooke in 1986 [11]. It consists of 10 items with 5 response options from 1 (strongly disagree) to 5 (strongly agree). The overall SUS score ranges from 0 to 100, although they should not be considered as percentages.

In terms of cognitive metrics, in this work the learnability and memorability of the PMA as defined in [10] have been analysed.

Learnability is related to the % of users that learn how to use the system (i.e. how easy is it for users to accomplish basic tasks the first time they encounter the design?). It was measured by: a) % of incorrect presentations and; b) % of successfully completed tasks (without assistance)**;** at the first attempt during the first session.

Memorability is related to how the users interact with the application after a period of inactivity. It was measured through the evolution of the learnability metrics at the first attempt during the second and third sessions.

V. RESULTS

This Section presents the HBSI metrics obtained from the participants' interaction with the PMA applying the methodology and HBSI metrics described in previous Section. It presents a thorough comparison between the two biometric modalities analysed: voice and face. This Section also highlights the differences with the results from our previous evaluation [2] due to the changes introduced in the enrolment phase, the scenarios set-up and the verification process.

A. HBSI presentation metrics

Figure 4 depicts the distribution of HBSI presentation metrics at the authentication task respectively.

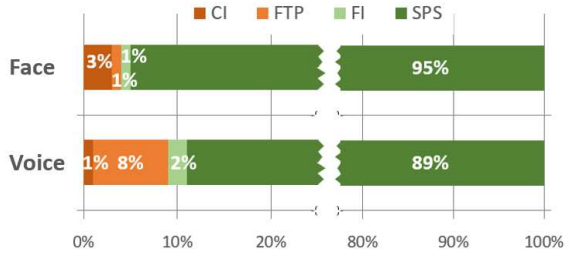

Fig. 4. HBSI presentation metrics for face and voice authentications

Face sample presentations show a 95% of Successfully Processed Sample (SPS), along with 1% of False Interaction (FI) and Failure to Process (FTP) and 3% of Concealed interaction (CI). Most of the CI presentations were due to unfocused pictures not detected by the Face Activation Detection (FAD) module. This, along with the 1% of FTP face sample presentations, indicate room for improvement in this module.

Regarding voice sample presentations, 89% of the presentations were SPS. However, there 8% of correct presentations were classified as incorrect (FTP) and 1% of incorrect presentation were classified as correct (CI). Most of the FTP misclassifications came from a strict timing constraint to start repeating the numbers shown at the voice interface screen by the Voice Activation Detection (VAD) module. The high level of FTP clearly indicates that the VAD is not able to allow natural variation in response times for different users.

The comparison between face and voice HBSI presentations metrics shows that, as expected, participants are more used to taking "selfie" pictures than repeating a random 5-digit sequences. This habituation will favour the participant's satisfaction towards the use of face authentication over voice authentication.

B. Usability metrics: efficiency and effectiveness

The **efficiency**, or average time spent, of the enrolment task has been measured over the first session and for those enrolment procedures performed without mistakes, detailing the time spent on typing the email, the PIN and the Password, voice and face biometrics samples and welcome screen subtasks.

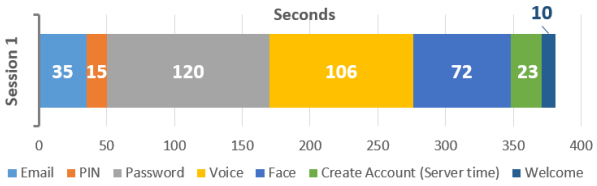

Fig. 5. Enrolment efficiency (average task/subtask times)

The overall registration process took an average of 6 minutes and 20 seconds as shown Figure 5. It can be noticed that the most time-consuming subtask is the selection of a strong password at an average of 120 seconds, due to the complexity requirements. The second most consuming task is the voice registration, with 106 seconds, due to the 6-time repetition of the 5-digit sequence, followed by the face registration process with 72 seconds. However, most of the participants of the experiment didn't show discontentment with the enrolment process as they understood the reasons for the multiple face and voice samples and the complexity requirements of the password.

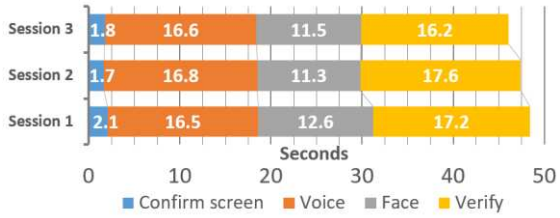

Fig. 6. Authentication request efficiency times

The **efficiency** of the authentication task (Figure 6) was 48 seconds. In session 2 the efficiency is slightly improved to 47 seconds, showing that participants became familiar with the process. In session 3 the improvement came mostly from the server process time, therefore not related to the user's habituation. This authentication server time is the most time-consuming task of the process and it should be significantly reduced in order to enhance the users experience. The server time significantly increased from previous experiment, and participants showed their dissatisfaction with such a long delay. The face subtask is significantly faster than the voice subtask. It is important to note that the voice capture subtask time is fixed by the PMA design as the participant must repeat the 5-digit sequence synchronised with the PMA voice capture interface. This explains the lack of improvement in the voice subtask between session 1 and 2 compared with the improvement of the face subtask.

The **effectiveness** has been analysed by three different metrics: a) % of errors, b) %) of assist and c) task completions rate. These metric are summarised in Figure 7.

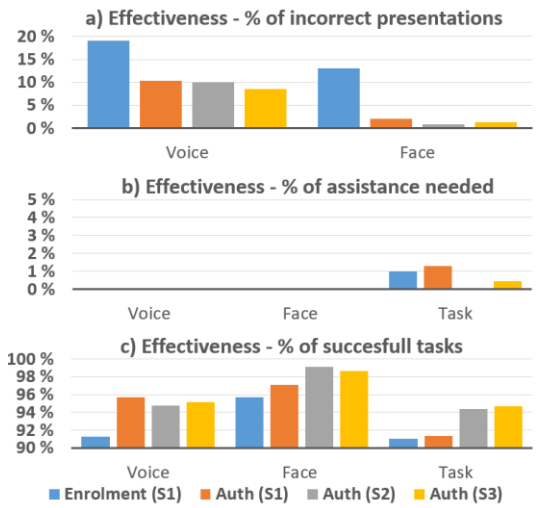

Fig. 7. HBSI effectiveness metrics for enrolment and authentication tasks

In terms of % of incorrect presentations (Figure 7a), there is a significant difference between the face and the voice tasks. Both tasks show high percentages of incorrect presentation during the enrolment, which indicates that the instructions shown in the enrolment interfaces are ambiguous. However, the face task shows a significant reduction at the authentication tasks in sessions 1 to 3, while the voice task keeps unacceptable level of incorrect presentations. These incorrect presentations are caused mostly by the time constraints imposed by the VAD module and the lack of preparation of participants to start repeating the 5-digit sequence. These problems should be addressed in future version of the PMA by improving the VAD to be more accurate in detecting the repeated digits and enhancing the information shown to the users in order to better prepare them for the task.

Regarding the number of assists requested during the process from the participants (Figure 7b), it can be noticed that the strategy of physically separating the participant from the operator has made them to be more autonomous at both voice and face tasks compared with previous experiment. Only a few participants requested help during the enrolment and the authentication processes, which should be addressed with better guidance within the interfaces of the screen.

Lastly, in terms of percentage of successful tasks, it can be seen again how the voice process has a lower effectiveness than the face process. Participants are familiar with the process of taking "selfie" pictures, which makes them more familiar with the face interface and process and less prone to errors.

C. *Cognitive metrics: learnability and memorability*

Learnability has been analysed based on the following metrics: a) the number of incorrect presentations and b) the number of successfully completed tasks (without assistance) in the first attempt during the Session 1 at the authentication task. This is shown in the blue columns in Figure 7. It can be noted how the familiarity of participants with "selfie" pictures resulted in 100% correct presentations. On the other hand, the voice interface shows 13% incorrect presentations. This indicates the participants were not well guided by the instructions shown in the voice interface. Most of these incorrect presentations were due to the participants not repeating the first number of the sequence as they did not understand the capture process. After this first attempt, most of the users understood the process and provided correct voice sample presentations. The third learnability indicator used was the percentage of successful task completion rate (blue columns in Figure 7c), where the same patterns can be observed. Figure 7 also shows the percentage of successful task completion for the entire authentication process (taking into account all the different interfaces the participants have to go through to complete an authentication request). This indicator shows a poor performance, lower than 80%, which again clearly indicates the information provided to the participants within the PMA interfaces for the authentication task at their first attempt should be substantially improved, especially the voice interface guidance.

The **memorability** of the PMA interfaces and process is analysed via the evolution of: a) the percentage of incorrect presentations and b) the percentage of successful task completion at the participants' first attempt across the three sessions. Both indicators show high levels of memorability. The participants learn how to perform the authentication process in the first session, and remember the process at both session 2 and 3, with the exception at the face results in session 3. The reason behind these errors might be explained due to participants being over confident with the face authentication process and paying less attention in providing a picture within the limits of the silhouette shown in the face capture interface. Pictures with faces not fully located within the silhouette were still classified as correct presentation by the FAD module and successfully compared with the participant's face template. The performance of the face comparison engine should be evaluated for this type of pictures. If the performance is satisfactory, the silhouette restriction could be removed.

D. *Participant's satisfaction: System Usability Scale (SUS) and questionnaires*

The participants were asked to rate from 1 to 5 (1 being very dissatisfied and 5 being very satisfied) their satisfaction with the enrolment process and the use of voice and face biometrics for authentication using the PIDaaS platform. The average satisfaction values are shown in Figure 8:

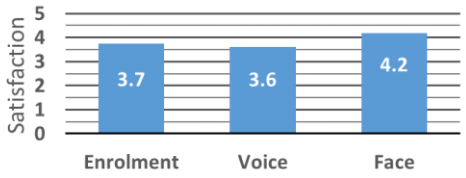

Fig. 8. PIDaaS 2nd pilot lab participant's satisfaction

Both the enrolment and the use of voice biometrics are rated between 3 and 4, which indicates a slight satisfactory experience for the users. On the other hand, the use of face

biometrics is rated above 4, indicating an overall positive satisfaction. It was noticeable that the participants preferred the face authentication over the voice authentication. Participants showed a better attitude towards taking pictures than towards talking to the phone. This behaviour may be explained by the strong habituation of the participants to taking "selfies" pictures. Some participants also expressed their concerns about speaking a 5-digit sequences in presence of others.

Regarding the overall satisfaction with the PIDaaS platform, in this experiment we asked the participants to answer the 10 items of the System Usability Scale questionnaire. The SUS score is shown in Figure 9.

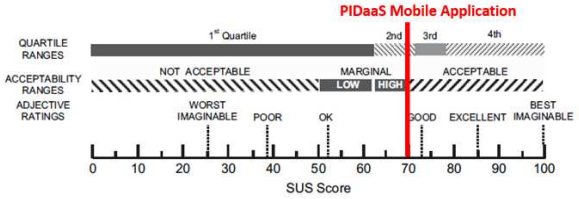

Fig. 9. PIDaaS System Usability Scale score

The SUS score obtained for the PMA was 70, which is just about the average SUS (68). As it can be seen, the PIDaaS SUS score stands at a good usability performance. This result reveals that there are many aspects of the PMA and the PIDaaS authentication process to improve in terms of usability. As previously mentioned, better guidance to the users in order to avoid incorrect biometric presentations, improvement on the VAD and FAD modules, a significant reduction of the server times and more friendly interfaces could lead to a significant improvement on the user's satisfaction regarding the PIDaaS platform.

VI. Conclusions

The biometric interaction evaluation carried out in this work on the PIDaaS platform has provided thorough insights about the user's experience. A new version of the PMA has been tested, which incorporated all the steps designed for the PIDaaS authentication process: voice and face capture enrolment and comparison.

The metrics proposed by the HBSI framework provided a comprehensive view of how the users interact with the new multi-modality PMA version, where the errors are and what can be done to minimise these errors in future version of the application. The HBSI metrics provide valuable insights into the efficiency of multi-modality implementations, allowing comparison between biometric modalities. Furthermore, these metrics enable us to measure the learnability and memorability of interaction steps, which are key factors to ensure a user friendly and satisfactory implementation.

The integration methodology proposed in our previous work [2,8], which makes use of mobile analytical tools and biometric system logs in order to ensure the acquisition of sufficient information, has been shown to facilitate and quicken the analysis of the data captured. This integration also aims to enable remote evaluation of mobile biometric systems, allowing the online distribution of the mobile application to a wider population and the collection of data without the supervision of an operator in real scenarios. The successful tested physical separation between the operator and the participants is a significant step towards enabling this type of remote evaluations.

Regarding the evaluation results of the voice and face implementation within the PMA, the integration of face has been revealed to be more user-friendly to the participants than the voice implementation. Face authentication showed generally better HBSI presentation, efficiency and effectiveness metric results. These results led to higher satisfaction rates within this modality. This behaviour is explained by the strong habituation of the participants to take pictures which makes them more familiar to the face integration interfaces and less prompt to errors. Furthermore, the System Usability Scale usability questionnaire has provided comparable usability scores, allowing an identification of where the PMA and the PIDaaS platform stands compared with other application and the extent of potential improvements to the platform.

Acknowledgment

This work has been co-funded under the EU ICT Policy Support Programme CIP (Call CIP-ICT-PSP-2013-7, project reference 621021).

References

[1] University of Kent, CSI-Piamonte, Ricoh, Bantec, Gjovik University College, E-Bros, Eurecat, "Private Identity as a Service (PIDaaS)," EU CIP, 2014. [Online]. Available: www.pidaas.eu.

[2] O. Miguel-Hurtado, R. Blanco-Gonzalo, R. Guest, and C. Lunerti, "Interaction evaluation of a mobile voice authentication system," IEEE Int. Carnahan Conference on Security Technology, Florida, 2016.

[3] M. Brockly, S. Elliott, R. Guest, and R. B. Gonzalo, "Human-Biometric Sensor Interaction," in Encyclopedia of Biometrics, Springer, 2014,.

[4] A. Wamsley, S. Elliott, C. Dunkelberger, and M. Mershon, "Analysis of slap segmentation and HBSI errors across different force levels," in 2011 Carnahan Conference on Security Technology, 2011, pp. 1–5.

[5] E. Kukula and S. Elliott, "Implementation of hand geometry: an analysis of user perspectives and system performance," IEEE Aerosp. Electron. Syst. Mag., vol. 21, no. 3, pp. 3–9, Mar. 2006.

[6] E. P. Kukula and S. J. Elliott, "Evaluation of a facial recognition algorithm across three illumination conditions," Aerosp. Electron. Syst. Mag. IEEE, vol. 19, no. 9, pp. 19–23, 2004.

[7] R. Blanco-Gonzalo, R. Sanchez-Reillo, O. Miguel-Hurtado, and E. Bella-Pulgarin, "Automatic usability and stress analysis in mobile biometrics," Image Vis. Comput., vol. 32, no. 12, Dec. 2014.

[8] O. Miguel-Hurtado, R. Guest, and C. Lunerti, "Users-Centric Design: introducing remote usability evaluation in mobile implementations," in Int. Biometric Performance Testing Conference, Gaithersburg, 2016

[9] "Common environmental noise levels." [Online]. Available: http://chchearing.org/noise/common-environmental-noise-levels/. [Accessed: 15-Oct-2015].

[10] J. Nielsen, "An introduction to usability," 2012. [Online]. Available: https://www.nngroup.com/articles/usability-101-introduction-to-usability/. [Accessed: 9-July-2017]

[11] J. Brooke, "SUS: A Quick-and-Dirty Method of System Evaluation." User Inf. Arch. Adv. Dev. Group, DEC, Reading, UK, 1986