Leveraging Continuous Multi-modal Authentication for Access Control in Mobile Cloud Environments

Gianni Fenu(✉) and Mirko Marras

Department of Mathematics and Computer Science, University of Cagliari,
V. Ospedale 72, 09124 Cagliari, Italy
{fenu, mirko.marras}@unica.it

Abstract. Mobile cloud computing integrates cloud computing into mobile environments, allowing users to use data, infrastructure, platforms, and applications on the cloud from their mobile devices. However, accessing and exploiting cloud-based resources and services is associated with numerous security implications (e.g. authentication and authorization) which represent the major barriers making individuals and organizations hesitant to migrate data or processing to the cloud. Using biometric techniques is increasingly emerging to secure such users' assets. In this paper, we propose a bi-modal continuous authentication approach integrating face and touch biometrics into mobile cloud environments, going beyond traditional one-off authentication. The system reacts to sliding windows of recent user's actions to dynamically update the trust in genuineness for the current user. For each biometric trait, it calculates the similarity scores resulting from the comparison between probes and templates, then they are fused together. If the fusion score is above a given threshold, the system rewards the current user; otherwise, they are penalized. In case the trust in the current user drops below a predefined threshold, the system raises an alarm. Experimental results indicate the advantage offered by our approach on performance of continuous authentication systems, providing a good security-usability tradeoff to mobile cloud environments.

Keywords: Mobile cloud computing · Mobile biometrics
Biometric access control · Multi-Modal authentication
Continuous authentication

1 Introduction

Mobile devices (e.g. smartphone and tablet) are increasingly becoming an essential part of everyday life, playing the role of the most convenient communication tool with no constraints in time and place. In parallel, various challenges in terms of the resource use and the communication workload are preventing the improvement of the service quality they can offer. Mobile Cloud Computing (MCC) integrates cloud computing into mobile environments in order to provide high-quality services to mobile users and overcome such emerging issues [1]. MCC is widely recognized as the next generation computing disruption, enabling mobile users to exploit infrastructure (e.g. servers and

S. Battiato et al. (Eds.): ICIAP 2017 International Workshops, LNCS 10590, pp. 331–342, 2017.
https://doi.org/10.1007/978-3-319-70742-6_31

networks), platforms (e.g. services and operating systems), and software (e.g. applications) made available on-demand by cloud providers (e.g. Google and Microsoft).

However, accessing and exploiting cloud-based resources and applications is associated with numerous security and privacy implications (e.g. user authentication and authorization) which represent the major barriers making individuals and organizations hesitant to migrate data or processing to the cloud [2]. For instance, a stolen mobile device could be abused to download sensitive data from the cloud, if a mobile user is registered with a cloud service provider. Using techniques to control the access to data and applications becomes essential to secure users' assets hosted by cloud providers [3].

Existing access control methods based on passwords and smartcards tend to suffer from the lack of authenticity and non-repudiation. By contrast, biometrics are becoming an attractive feature for cloud providers in order to provide novel security features and service models to their clients [4]. In user authentication, both physical and behavioral characteristics promise to be stronger than passwords. Human peculiarities cannot be easily stolen, forgotten, nor guessed. Emerging biometric systems are mainly required to (i) have a high level of accuracy to be secure and practical for widespread adoption in the cloud, (ii) operate continuously to avoid impostor users using the system after the genuine user logs in, and (iii) protect biometric samples to preserve users' privacy. Meeting the requirements is essential for the successful adoption of biometric systems.

In this paper, we specifically focus on the first two requirements and propose a multi-modal biometric approach in order to authenticate users continuously and transparently in mobile cloud environments. In our investigated scenario, the fusion system uses two standalone biometrics (i.e. face and touch) and calculates the score-level fusion of the corresponding matching scores. However, due to the natural variation in behavior and the heterogeneous conditions in operation, a user can deviate from the normal condition on a minority of situations as well as impostor users can appear as genuine for certain periods. The concept of trust in genuiness of the user models this variation. The system computes the similarity scores resulting from the comparison between probes and templates, then they are fused together. If the fusion score is above a given threshold, the system rewards the current user; otherwise, they are penalized. The global system trust in the user is updated accordingly. If it is above a given threshold, then the user continues the normal activities; otherwise, the user is locked out. Experiments on a publicly-available dataset were carried out to validate the methodology. The results show the potential of our approach to strength the security provided for MCC environments.

The rest of this paper is organized as follows. Section 2 introduces a brief overview of the related work, Sect. 3 describe the proposed approach, Sect. 4 presents experiments and results, and Sect. 5 provides conclusions and insights for future work.

2 Related Work

2.1 Access Control in Cloud Environments

Cloud services relies heavily on authentication methods based on passwords and/or personal identification numbers. Biometrics are an attractive feature to overcome various problems and emerge as a practical alternative to password authentication [5].

In biometric systems running on the cloud, one of the most challenging problems is preserving user's privacy and maintaining the confidentiality of users' biometric data during transfer or storing. Unlike passwords and tokens, biometric traits cannot be canceled and reissued (i.e. if a user's fingerprint is compromised it cannot be changed and the user cannot use it in the future). Moreover, unsecured biometric templates are vulnerable to biometric dilemma threat [6], where an impostor accesses a biometric template in a less secure biometric system and uses it to gain access to a high secure system. Hence, biometric authentication systems must consider the security of users' biometric data. Some schemes apply biometric authentication in the cloud without taking user's template protection into account. For instance, Cloud Iris Verification System (CIVS) [7] applies iris authentication for authenticating users of the cloud software as a service. CIVS stores iris patterns on the cloud without protection. Other approaches apply biometric authentication in the cloud with template protection mechanisms (e.g. Revocable Bio-tokens [8]). Biometric template protection mechanisms are surveyed by [9].

In general, biometric systems in cloud environments tend also to suffer from low matching accuracy and tradeoffs between FAR (False Acceptance Rate) and TAR (True Acceptance Rate). In general, whenever the FAR is set to a low level, the TAR falls down too. Moreover, the low FAR can be vulnerable to doppelganger threat [6], where a set of biometric data (i.e. stolen biometric database) can be applied to get access to a system by leveraging the FAR. It follows that biometric authentication should have a high TAR and very low FAR to be a secure and practical. For instance, the authors in [10] used keystroke authentication scheme for the cloud environment. Nevertheless it enhances the matching computation time, the authentication accuracy does not ensure high security (FAR = 1.65%, FRR = 2.75%). In fact, even though this FAR can be seen as practical rate, it can be exploited due to the biometric doppelganger attack [6].

In general, impostors can take advantage of the mentioned drawbacks to access data and applications improperly since existing biometric systems in cloud environments appear to authenticate users only at login time. By contrast, continuous authentication promises to verify users' identity throughout the session, strengthening the ability of the system of locking out impostors even when the recognition ability on an individual sample is not high. Moreover, they leverage behavioral biometrics which are not easily to be stolen and replicated since they depend on users' action in the context of the given session and application. This makes harder improper access even when impostors have a copy of the biometric trait. Furthermore, the fusion of behavioral biometrics and physical biometrics (e.g. face) can be exploited to improve overall recognition capabilities.

2.2 Continuous Biometric Authentication on Mobile Device

In recent years, biometrics and security research communities have developed techniques and methodologies for continuous implicit user authentication by mobile devices [11]. We show a set of academic and commercial examples, both uni and multi-modal.

Continuous biometric systems usually require real-time processing capabilities and optimization methods already explored in various domains such as finance [12] and computer networks [13]. First, biometric modalities such as gait, face, typing, or voice are continuously measured by the built-in sensors integrated into a mobile device (e.g. camera, touch screen, accelerometer, orientation sensor). Then, the system determines whether these biometric traits correspond to a genuine user. If the features correspond to a genuine user, the biometric system continues to process new incoming data [14].

Touch dynamics is one of the most commonly used continuous authentication methods for mobile devices using touchscreen input as a data source. The way users swipe their fingers on touchscreen of mobile devices is used to continuously authenticate users while they perform basic operations [15]. For instance, [16, 17] studied whether a classifier can continuously authenticate users based on the way they interact with the touchscreen of a smartphone. They proposed a set of behavioral touch features that can be extracted from raw touchscreen logs. Other continuous authentication systems monitor user's identity based on face recognition. In [18], it was designed a method for detecting partially cropped and occluded faces captured using a smartphone's front-facing camera for continuous authentication. The key idea is to detect facial segments in frames and cluster the results to obtain the region which is most likely to contain a face. Then, it was used for verification. In [19], a face-based continuous authentication system operates in an unobtrusive manner, fusing mobile device face capture with gyroscope, accelerometer, and magnetometer to correct face image orientation. Several studies have used contextual information to enhance the performance of continuous authentication such as investigating how the position in which the smartphone is held affects user authentication. For instance, the authors in [20] proposed a set of behavioral features useful to capture micro-movement and orientation dynamics resulting from how a user grasps, holds, and taps on smartphones. Behavior modelling as developed in [21] enabled cross-device authentication based on how users perform actions.

It has been observed that some of the limitations of unimodal continuous authentication systems can be addressed by deploying multi-modal systems that essentially integrate the evidence presented by multiple sources of information. For instance, [22] introduced a transparent authentication framework utilizing a combination of behavioural biometrics: keystroke dynamics and voice recognition. Similarly, [23] examined the combination of keystroke dynamics, behavioural profiling and linguistic profiling. In [24], the authors proposed a multi-biometric system based on the observation that the instinctive gesture of responding to a phone call can be used to capture two different biometrics, namely ear and arm gesture, which are complementary due to their physical and behavioral nature. Literature in this field demonstrates that human authentication based on multi-modal biometrics is becoming an emerging trend, and one of the most important reasons to combine different modalities is to improve recognition accuracy.

3 The Proposed System

The proposed approach is built on top of a modular architecture. Each component performs a task in the typical operational cascade of a biometric system. The implementation of single modules has been properly analyzed to ensure both the effectiveness and the efficiency of the overall system. It follows that this increases the number of functionalities provided with no degradation in the tradeoff between security and usability. Such feature is essential for biometric systems, especially when they operate continuously to authenticate users based on what they do.

The underlying architecture depicted in Fig. 1 includes two independent biometric authentication modules: face authentication module and touch authentication module. The input of each module is the data captured by the corresponding sensor on the mobile device, while the output is a matching score for each one of them. Each module performs score normalization separately on the obtained scores from each of these two biometric modules. Matching scores lie in the range [0,1], where 0 means totally different, while 1 means the same. Then, these scores are fused together by the Trust Manager to obtain the final matching score used to decide whether the test subject is genuine and update the trust level accordingly.

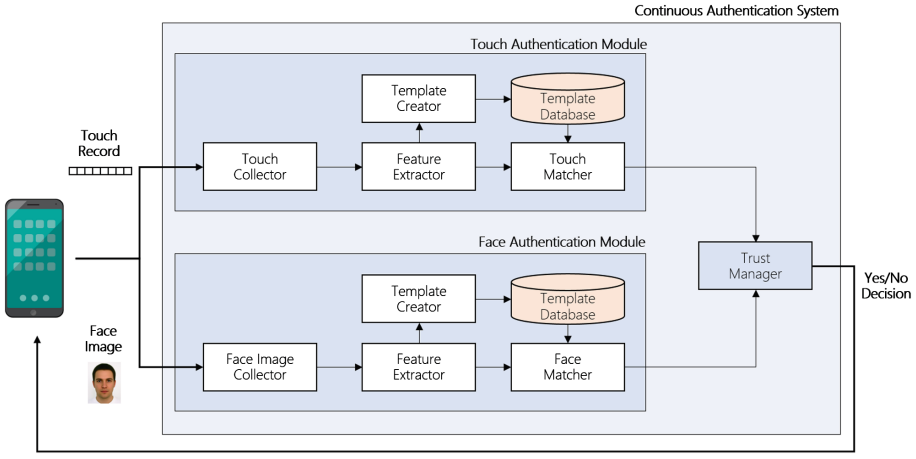

Fig. 1. Overall architecture of the proposed multi-modal system.

3.1 Face Authentication Module

Nowadays, mobile devices provide routines and drivers to access on-board cameras. Using them, it is easy to acquire users' face images coming from a continuous clip.

The module receives an image as input. It implements the FaceNet algorithm [25] for the localization of the relevant subregion of the image containing the face. FaceNet has been proven to work well when face samples are collected in the wild, including partial visibility, illumination changes, occlusion and wide variation in poses and facial expressions. To accomplish this task, a FaceNet-based model is pre-trained on

CASIA-Webface dataset[1]. The face region is cropped and aligned. Then, the module detects the key points of interest on the face. More precisely, it tries to localize and label the left eyebrow, the right eyebrow, the left eye, the right eye, the nose and the mouth. The implemented landmark detector is based on the ensemble of regression trees trained to estimate the facial landmark positions directly from the pixel intensities as proposed in [26]. Each landmark is cropped and stored separately. An image correction routine is used to normalize illumination on both the face image and the landmark images.

Five different types of features are extracted as follows: (i) the pre-processed face is converted to grayscale, rescaled and vectorized as uni-dimensional vector; (ii) from the 64×64 rescaled grayscale image, Local Binary Pattern (LBP) features as uni-dimensional vector are extracted for a cell size of 8×8 pixels; (iii) bounding boxes of the landmarks are computed for each face part from the pre-processed grayscale image. The eye-based, nose and mouth bounding boxes are resized to 16×20, 28×17 and 22×46 pixels respectively, then vectorized to a uni-dimensional vector; (iv) LBP features are obtained from the resized bounding boxes with a size of 12×12 pixels; (v) FaceNet embeddings resulting from the whole face and individual landmarks are extracted.

The above features are concatenated to form a unique feature vector whose values are transformed in the range [0,1] by min-max normalization. It constitutes the user's template. The matching score between the template and the probe is calculated using Cosine Distance. As output, the module returns such distance to the Trust Manager.

3.2 Touch Authentication Module

The module receives raw touchscreen logs as input. Then, it divides up them into individual strokes considering three types of events: finger down, move and finger up. Each stroke is a sequence of touch data beginning with touching the screen and ending with lifting the finger. No input is recorded between two consecutive strokes. Every stroke is encoded as a sequence of 4-tuples data = (x_i, y_i, p_i, t_i) for $i \in 1,\ldots,N_c$ where x_i, y_i is the location coordinates and p_i is the pressure applied at time t_i, and N_c is the number of data points captured during the stroke. The module is set to process only strokes containing more than three data points during feature extraction.

From each stroke with $N_c \geq 4$, a 30-dimensional feature vector is extracted using the method described in [16]. The features include measures related to velocity and acceleration both between internal-stroke points and first and last stroke points. Past research has proven that these stroke features exhibit a larger variance across different users than for a single user. The template is represented by an ensemble of three classifiers properly trained with genuine data and impostor data coming from the dataset in [16], following the one-vs-all protocol. More precisely, the three classifiers are the AdaBoost classifier, RandomForest classifier and Stochastic Gradient Descent classifier with a log loss function and L2 penalty. During verification, the ensemble classifier predicts the overall matching score based on the maximum argument of the

[1] http://www.cbsr.ia.ac.cn/english/CASIA-WebFace-Database.html.

sums of the predicted probabilities from each classifier, which is recommended for an ensemble of well-calibrated classifiers. The matching score is normalized in the range [0,1] by min-max normalization. As output, the module return such value to the Trust Manager.

3.3 Trust Manager Module

The module receives two distances as matching scores coming from the Touch Authentication module and the Face Authentication module, as input. It can operate in two different modalities: *standard continuous mode* and *trusted continuous mode*. The first one includes the fusion of the matching scores using a weighted sum. If the fusion score is above a given threshold the user continues the activities, otherwise an alarm is raised.

However, due to the natural variation in behavior and the heterogeneous conditions in operation, a user can deviate from the normal condition on a minority of situations as well as impostor users can appear as genuine for certain periods. Hence, the second mode of operation includes the concept of trust in genuiness of the user. If a specific action is performed in accordance with the normal behavior of a genuine user, then the system's trust in the genuineness of this user will increase. If there is a large deviation between the behaviour of the genuine user and the current user, the trust of the system will decrease. A small deviation from the behavior of the current user, when compared to the template, leads to a small decrease in trust, while a large deviation to a larger decrease. The fusion score is computed by merging the scores from the independent biometric systems as performed in standard continuous mode. But, if the score is high enough, the system will reward the current user, otherwise the user is penalized. If the system trust drops below a pre-defined threshold T, the system locks itself. The penalty/reward and the current system trust are calculated dynamically using the formulas provided in [27]. As parameters for those formulas, the module sets A = 0.54, B = 0.005, C = D=2, T = 50. The upper limit of the system trust is 100 to ensure an imposter cannot benefit from the high trust obtained by the genuine user, before they access the system.

4 Experimental Evaluation

4.1 Dataset

To evaluate the applicability of our proposed approach, we used the highly-challenging UMDAA-02 [28] multi-modal database. It consists of data recorded by built-in cameras and touchscreen sensors during activities performed on smartphones.

It includes a set of over 33,000 images captured by smartphone cameras and recorded during all the sessions of 43 users at 7-s intervals for the first 60 s of interaction during each session. The number of images varies between 300 to 2,700 per user, while the number of sessions varies between 25 and 750, providing a wide range of images for each user and session. They include faces with partial visibility, illumination changes, occlusion and variation in poses and facial expressions.

From the same set of users during the same tasks, raw touch events were also recorded. The number of strokes varies around 3,500 per user, while the number of strokes per user for each session is around 196. The maximum number of data points in a stroke ranges between 4 and 3,000. These features demonstrate this database meets our goal.

4.2 Evaluation Protocol

We carried out extensive experiments in two different settings based on the mode of operation of the Trust Manager (i.e. standard continuous mode and trusted continuous mode) in order to evaluate the effectiveness of the proposed continuous biometric approach. For each setting, we firstly consider the biometric modules separately. During face verification, the combination of N consecutive face images is computed by averaging the matching scores to reinforce the recognition during each iteration. In the same way, M consecutive strokes are used to calculate the matching score for touch authentication. Then, we combined the biometrics by averaging the scores obtained by matching N face images and M touch strokes. M and N varies during the experiments.

In standard continuous mode, we calculated the False Recognition Rate (FRR) by matching the user's template against the remaining samples of the same user. If the matching h against g is performed, the symmetric one (i.e. g against h) is not executed to avoid correlation. Then, we computed the False Acceptance Rate (FAR) by matching the template of each user against all the samples of the other subjects. Finally, the Equal Error Rate (EER) is calculated starting from FAR and FRR values.

In trusted continuous mode, we replicated the evaluation protocol in [27] based on the computation of the Average Number of Imposter Actions (ANIA) and the Average Number of Genuine Actions (ANGA) as evaluation metrics. These indicators reveal how much imposters can do before they are locked out and how much genuine users can do before they are locked out of the system. Each user can be classified into one of the following categories: the genuine user is never locked out and all impostors are detected (+/+); the genuine user is not locked out, but some impostors are not detected ($\pm$); the genuine user is locked out, but all the impostors are detected ($\mp$); the genuine user is locked out, while some of the impostors are not detected (–/–).

4.3 Experimental Results

Standard Continuous Mode. The EERs obtained using different values of M and N for touch and face respectively are reported in Fig. 2. The values of M range from 2 to 14. N is set to M/2 to achieve a good tradeoff between security and usability.

From these results, we see for single-trait biometric verification, face matcher achieved the lowest performance comparing to touch and fusion matchers. This is reasonable, since the face images collected into the database contain a vast variety of challenging conditions regarding illumination, head pose, facial expression, and age difference. All these factors contribute negatively to the verification process. Meanwhile, the multi-modal fusion always obtained higher performance than single-trait

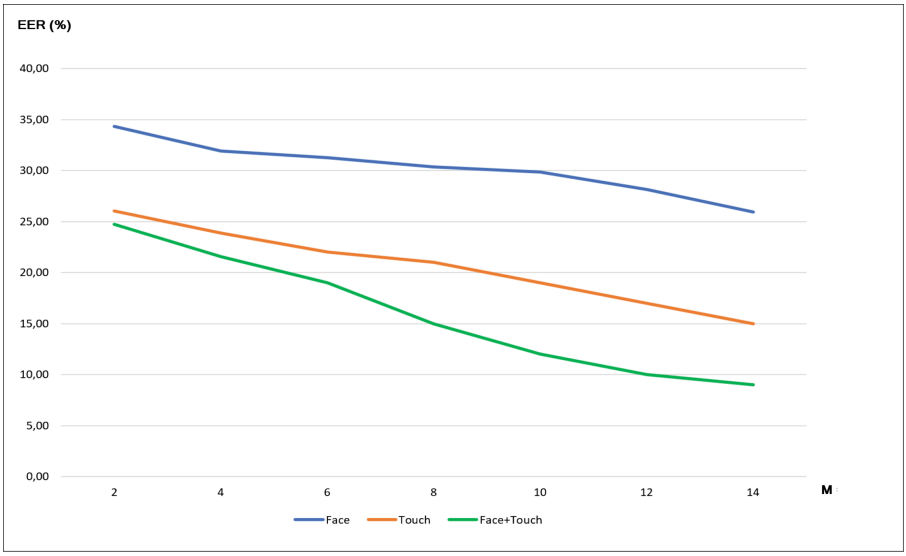

Fig. 2. The performance of the proposed bi-modal approach in standard continuous mode.

approaches. As proposed in this work, integrating these two modalities into the fusion system and averaging their contribution results in a performance improvement. In addition to it, we observed that the lowest EER values achieved in the benchmark results carried out on the UMDAA database for uni-modal traits are EER = 18.44% and EER = 22.10%, using N = 30 face images and M = 16 touchscreen strokes respectively. With our approach, we achieved EER = 9.61% combining only M = 14 touch strokes and N = 14 face images. This demonstrated that the bi-modal fusion can improve both effectiveness and efficiency.

Trusted Continuous Mode. Table 1 shows the results achieved by our approach fusing face and touch biometrics. We report results for M = 2 and N = 1 to hold a good trade-off between usability and security while maintaining efficiency. The guidelines followed to report the performance are provided by [27]. The column "# Users" defines the number of users for each category. The ANGA indicates the average number of genuine actions before genuine users are locked out. If the genuine users are not locked out, no ANGA is reported. The column ANIA displays the average number of impostor

Table 1. The performance of our bi-modal approach in trusted continuous mode (M = 2, N = 1).

Category	#Users	ANGA	ANIA	#NDI
+/+	16	–	30	–
+/–	7	–	42	27 (9%)
–/+	18	680	26	–
–/–	3	344	113	3 (2%)

actions based on the assumption that all impostors are detected. The actions of the non-detected impostors are not used in this calculation, but the number of non-detected impostors is given in the column #NDI. This number should be seen in relation to the number of biometric subjects in that category (see the percentage in the #NDI column).

In Table 1, 16 participants obtained very good recognition and only 30 actions as ANIA. In this category, none of the genuine users is locked out and all the impostors are detected. In the second category, we find 7 participants which are not locked out. The average ANIA is similar (42 actions) to the first category and a total of 27 imposters were not detected (i.e. 9%). The remaining 18 genuine users in the third category were locked out at least once by the system. For these users, we have an average ANGA and ANIA of 680 and 26 actions, respectively. There are only 3 participants that fall into the worst category where ANGA and ANIA are 344 and 113 actions respectively and 3 imposters are not detected. Such users are not sufficiently protected against impostors.

The experimental results promise that our approach integrating face and touch biometrics can be a practical solution to improve both effectiveness and efficiency of continuous authentication in comparison with uni-modal approaches.

5 Conclusions

In this paper, we presented an approach for integrating face recognition together with touch behavior recognition to increase the overall performance of a continuous multi-modal authentication system in mobile cloud environments, going beyond traditional one-off authentication. The system reacts to users' actions and dynamically update the trust in genuiness for the user. Experimental results show promising performance which indicates the advantage offered by our system and makes it suitable for mobile cloud applications requiring a good security-usability tradeoff.

In next steps, we will investigate approaches to improve recognition scores returned by individual biometric systems, adding novel types of feature as an example. Larger datasets where to test our approach will be considered. Furthermore, we will study other penalty-reward equations in order to dynamically update the trust level. We also plan to employ Big Data architectures to support large-scale fast computations and leverage the cloud's unbounded computational resources and attractive properties of flexibility, scalability, and cost reduction to enhance the overall performance of our approach.

Acknowledgements. Mirko Marras acknowledge Sardinia Regional Government for the financial support of his PhD scholarship (P.O.R. Sardegna F.S.E. Operational Programme of the Autonomous Region of Sardinia, European Social Fund 2014-2020 - Axis III Education and Training, Thematic Goal 10, Priority of Investment 10ii, Specific Goal 10.5).

References

1. Dinh, H.T., Lee, C., Niyato, D., Wang, P.: A survey of mobile cloud computing: architecture, applications, and approaches. Wirel. Commun. Mobile Comput. **13**(18), 1587–1611 (2013). Wiley
2. Coppolino, L., D'Antonio, S., Mazzeo, G., Romano, L.: Cloud security: Emerging threats and current solutions. Comput. Electr. Eng. **59**, 126–140 (2017). Elsevier
3. Onankunju, B.K.: Access control in cloud computing. Int. J. Sci. Res. Publ. **3**(9), 1 (2013). IGI Global
4. Alizadeh, M., Abolfazli, S., Zamani, M., Baharun, S., Sakurai, K.: Authentication in mobile cloud computing. J. Netw. Comput. Appl. **61**, 59–80 (2016)
5. Ali, M., Khan, S.U., Vasilakos, A.V.: Security in cloud computing: opportunities and challenges. Inf. Sci. **305**, 357–383 (2015). Elsevier
6. Scheirer, W., Bishop, B., Boult, T.: Beyond PKI: the biocryptographic key infrastructure. In: Workshop on Information Forensics and Security (WIFS), pp. 1–6. IEEE (2010)
7. Ruiu, P., Caragnano, G., Masala, G.L., Grosso, E.: Accessing cloud services through biometrics authentication. In: 10th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS), pp. 38–43. IEEE (2016)
8. Scheirer, W.J., Boult, T.E.: Bipartite biotokens: definition, implementation, and analysis. In: Tistarelli, M., Nixon, Mark S. (eds.) ICB 2009. LNCS, vol. 5558, pp. 775–785. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01793-3_79
9. Jain, A.K., Nandakumar, K., Nagar, A.: Biometric template security. EURASIP J. Adv. Signal Process. **113** (2008). ACM
10. Zhu, H.H., He, Q.H., Tang, H., Cao, W.H.: Voiceprint-biometric template design and authentication based on cloud computing security. In: International Conference on Cloud and Service Computing (CSC), pp. 302–308. IEEE (2011)
11. Alotaibi, S., Furnell, S., & Clarke, N.: Transparent authentication systems for mobile device security: A review. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 406–413. IEEE (2015)
12. Aymerich, F.M., Fenu, G., Surcis, S.: A real time financial system based on grid and cloud computing. In: Proceedings of ACM Symposium on Applied Computing, pp. 1219–1220 (2009)
13. Fenu, G., Nitti, M.: Strategies to carry and forward packets in VANET. In: Cherifi, H., Zain, J.M., El-Qawasmeh, E. (eds.) DICTAP 2011. CCIS, vol. 166, pp. 662–674. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-21984-9_54
14. Patel, V.M., Chellappa, R., Chandra, D., Barbello, B.: Continuous user authentication on mobile devices: recent progress and remaining challenges. IEEE Signal Process. Mag. **33**(4), 49–61 (2016)
15. Jiang, L., Meng, W.: Smartphone user authentication using touch dynamics in the big data era: challenges and opportunities. In: Jiang, R., Al-maadeed, S., Bouridane, A., Crookes, P., Beghdadi, A. (eds.) Biometric Security and Privacy. Signal Processing for Security Technologies, pp. 163–178, Springer, Cham (2017)
16. Frank, M., Biedert, R., Ma, E., Martinovic, I., Song, D.: Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans. Inf. Forensics Secur. **8**(1), 136–148 (2013)
17. Van Nguyen, T., Sae-Bae, N., Memon, N.: DRAW-A-PIN: authentication using finger-drawn PIN on touch devices. Comput. Secur. **66**, 115–128 (2017). Elsevier

18. Mahbub, U., Patel, V.M., Chandra, D., Barbello, B., Chellappa, R.: Partial face detection for continuous authentication. In: IEEE International Conference on Image Processing (ICIP), pp. 2991–2995. IEEE (2016)
19. Crouse, D., Han, H., Chandra, D., Barbello, B., Jain, A.K.: Continuous authentication of mobile user: fusion of face image and inertial measurement unit data. In: International Conference on Biometrics (ICB), pp. 135–142. IEEE (2015)
20. Buriro, A., Crispo, B., Zhauniarovich, Y.: Please hold on: unobtrusive user authentication using smartphone's built-in sensors. In: International Conference on Identity, Security and Behavior Analysis (ISBA), pp. 1–8. IEEE (2017)
21. Wang, X., Yu, T., Mengshoel, O., Tague, P.: Towards continuous and passive authentication across mobile devices: an empirical study. In: Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 35–45. ACM (2017)
22. Crawford, H., Renaud, K., Storer, T.: A framework for continuous, transparent mobile device authentication. Comput. Secur. **39**, 127–136 (2013). Elsevier
23. Fridman, L., Weber, S., Greenstadt, R., Kam, M.: Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS. IEEE Syst. J. (2016)
24. Abate, A.F., Nappi, M., Ricciardi, S.: I-Am: implicitly authenticate me person authentication on mobile devices through ear shape and arm gesture. IEEE Trans. Syst. Man Cybern. Syst. **74** (2017). IEEE
25. Schroff, F., Kalenichenko, D., Philbin, J.: Facenet: a unified embedding for face recognition and clustering. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 815–823. IEEE (2015)
26. Kazemi, V., Sullivan, J.: One millisecond face alignment with an ensemble of regression trees. In: IEEE Conference on Computer Vision and Pattern Recognition. IEEE (2014)
27. Bours, P., Mondal, S.: Performance evaluation of continuous authentication systems. IET Biometrics **4**(4), 220–226 (2015). IEEE
28. Mahbub, U., Sarkar, S., Patel, V.M., Chellappa, R.: Active user authentication for smartphones: a challenge data set and benchmark results. In: International Conference on Biometrics Theory, Applications and Systems, pp. 1–8. IEEE (2016)