A Multimodal Biometric Authentication System for electronic Banking

Jordi Aguilà*, Roberto Morales, Manel Medina **, and Mario Reyes ***

jaguila@lacaixa.es,
{rmorales,medina}@ac.upc.edu,
mreyes@bdigital.org

Abstract. Biometric technologies are increasingly spreading and are often referred as the future of authentication. Biometric authentication is considered more reliable and secure than traditional mechanisms like passwords or tokens because it precludes replicability and provides non-repudiation. However, despite its potential, the low adoption of biometrics in highly sensitive environments like electronic banking is determined by factors that are specific to such scenarios and should be identified and properly addressed. This paper studies the leading biometric technologies, their suitability and their adoption in electronic banking authentication. It analyzes and compares them in terms of security, efficiency, usability and costs, towards proposing a biometric authentication system for electronic banking using mobile devices.

Keywords: Authentication, biometrics, electronic banking, mobile authentication, security

1 Introduction

Biometric has been for long the target of future authentication; it is expected that biometric authentication will largely displace other means of authentication and access control. The rationale behind this is that, due to its non-replicable and non-transferable properties, biometric data cannot be lost, misplaced or passed along; moreover, being able to forge biometric data requires the use of very advanced technology, making it more secure when compared to traditional mechanisms (e.g., passwords, TAN-list, etc.). Due to its recent integration into mobile devices, biometric authentication has grown popular again. Its recent advancements together with the rapid proliferation of mobile devices are attracting major interest to both: industrial and research communities. Moreover, the information that mobile devices are able to provide, highly incentives researchers in even finding new forms of biometrics. However, despite biometrics' potential benefits, its adoption in electronic banking authentication remains limited. Results in [8], [11] and [13] showed that in Europe only a few banks implement

* CSRIT, CaixaBank, Barcelona, Spain
** DAC, Universitat Politecnica de Catalunya, Barcelona, Spain
*** Security Research Group, Barcelona Digital Technology Centre, Barcelona, Spain

biometric authentication in electronic banking. According to authors in [13] and [12] this phenomenon is associated with factors like technology maturity, legislation (data protection), user perceived usability, and naturally, costs. Therefore, those factors should be properly assessed and balanced according to the high requirements of the electronic banking scenario. The purpose of this study was to evaluate the suitability of the leading bio-metric technologies for electronic banking authentication, towards proposing a multimodal authentication system using mobile devices. To this end, we (1) characterized the electronic banking scenario; (2) investigated the factors influencing its lower adoption; (3) assessed the leading technologies according to those factors; and (4) proposed a novel biometric authentication approach using mobile devices.

2 Background

Authentication represents the major barrier for attackers to circumvent an electronic banking system and ultimately commit fraud, i.e. the more robust and sophisticated an authentication method is, the harder to be deceived. The implementation of strong authentication is not only an essential part of any security system, but is a must in electronic banking [5], implying the combination of two or more elements based on what you know, what your have and what you are. According to [13] the most implemented authentication methods in electronic banking are based on what you know (e.g., PIN, passwords, pass-phrases, etc.), and what you have (e.g., keys, tokens, smart cards, etc.). Those properties can be forgotten, lost, stolen or eventually disclosed; and furthermore, do not authenticate the user as such. Contrary to this, biometric authentication, which is based on what you are, allows users to be authenticated by referring to those physiological or behavioral characteristics that are uniquely associated to them, and assumed to be neither replicable nor transferable, promising to severely enhance the security of authentication systems and simplify its procedures.

2.1 Biometric Systems Operation

Biometric systems aimed at verifying the identity of individuals (authentication) basically carry out three processes [1].
Enrollment: it is the initial step, it collects user's biometric sample (e.g., fingerprint), which requires user's interaction. Ideally it is performed only once; however, most systems require the collection of several samples. Once the collection of samples is done, a feature extractor algorithm analyzes the sample, and extracts and measures specific biometric features (e.g., fingerprint minutiae).
Storage: it is performed at the user registration phase. It consists in storing recently extracted features (i.e. biometric template) locally or remotely; additional information is also needed for the authentication system to associate a biometric templates to an individual.
Verification: it is performed on each authentication attempt. It takes a new

sample of the biometric data, and provides a comparison between the new sample and the one stored during enrollment. Unlike conventional authentication methods, biometric systems provide a percentage of similarity between samples, i.e. an individual's identity is confirmed only if the resulting percentage is above a predefined threshold.

2.2 Biometric Techniques

Biometric authentication techniques are classified by the type of characteristics evaluated: physiological attributes or behavioral singularities. According to authors in [6], the leading biometric techniques used in inherence-based authentication are those briefly introduced next.

Physiological Biometrics It consists of measurements taken from data obtained as part of the human body. This category includes: (1) fingerprints, technique that identifies the lines convergence points (minutiae matching); (2) facial recognition, technique that captures a sequence of images, and extracts features from the images ensemble; (3) hand geometry, technique that extracts hand features, such as shape, appearance, length and perimeters of fingers; (4) iris recognition, technique that identifies the location, shape and size of random patterns in the external iris of the eye; it transforms the iris rim into a rectangular shape texture; and (5) retinal identification, technique that maps the blood vessels in the back of the eye.

Behavioral Biometrics It consists of measurements taken from user's actions, some of them indirectly measured from the human body, e.g., voice recognition. Techniques within this category include: (1) voice recognition, technique that analyses power and spectral samples of the speech, building a statistical pattern from them; (2) keystroke dynamics, technique that identifies user's typing pattern taken from conventional keyboards or from touch screens (key tap dynamics). It measures and compares specific timing events also known as "typing signature". And (3) handwritten signature, technique that uses a digital version of the signature (modern sensors also measure pen position, pressure and inclination in a three-dimensional way).

3 Electronic Banking Scenario

Electronic banking is the most popular method for conducting financial transactions. It allows millions of consumers to interact with their bank accounts (anywhere and anytime) from a wide range of devices, significantly enhancing end user experience. Due to the sensitive nature of financial information, providing transaction security is of utmost importance. In this regard, the authentication process plays a major role, being the first barrier that security attackers must circumvent to access the system and commit fraud. This section characterizes the electronic banking application scenario; it identifies the authentication requirements and analyzes factors that potentially influence the adoption of biometrics.

3.1 Characterizing the Scenario

Electronic banking applications must provide robust mechanisms that allow users to authenticate transactions in a secure, simple and efficient manner. Users might be reluctant to adopt solutions that they do not understand or not authenticate them at the first try. To this end, we characterize our scenario by adopting the taxonomy introduced in [9], which is determinant for selecting the adequate biometric technologies for electronic banking.
User awareness: the collection of biometric data for electronic banking requires user's consent and interaction; therefore, the application scenario is overt.
Intended users: users will become habituated after a short period of time.
System supervision: the enrollment and authentication processes will take place without system supervision, allowing users to effectively enroll and authenticate without the need of additional support or training; therefore, the system is classified as non-attended.
Operational environment: it will not be controlled (e.g., lighting, noise, temperature, etc.); thus, biometric technologies should be able to operate outdoors and probably in unusual indoor environments.
End users: Users in electronic banking are commonly categorized in four main segments (i.e. retail, private, corporate and investor) [13]. Although, from different segments, users are considered public (e.g., users do not share a common device for accessing the system).
System type: it will not be designed to operate/share with external biometric systems or public biometric databases; therefore, it is characterized as closed.

3.2 Factors Influencing Biometrics Adoption in Electronic Banking

Electronic banking is one of the most sensitive scenarios requiring high levels of security. To be able to prevent fraud, strong authentication mechanisms are expected to authenticate transactions and users as such, which is not achieved by the yet, most implemented authentication methods (e.g., TAN code list, OTP-based hardware token). Moreover, those methods have shown important security weaknesses (e.g., the Eurograbber [4] and High Roller attacks [10]), and furthermore, inability to provide non-repudiation and fulfill demanding security requirements.

To cope with those limitations, biometric authentication has been strongly suggested in the past. However, results presented by authors in [13], show that very few banks in Europe implement biometric authentication in electronic banking systems. The rationale behind this phenomenon is discussed next.
Security: The False Acceptance Rates (FARs) inherent to biometric technologies must comply with the high requirements of electronic banking and/or be complemented with additional security mechanisms. Thus, potential attacks to the overall authentication system, must be carefully assessed.
Usability: Users might be reluctant to adopt novel solutions, if they are not able to authenticate them at the first try. Thus, the suitability of different biometric

technologies can be hindered by unacceptable False Rejection Rates (FRRs).
Data Leakage: It is said that when biometric data is compromised, it is comprised forever (i.e. it is not possible to change the fingerprints, iris, etc.). Attacks to centralized databases storing biometric data, result in both: high associated risks and great responsibility to be accepted by the financial sector.
Law Enforcement: There exist legal issues when dealing with personal information. In Europe, specific consents from customers are required; this task might be difficult to achieve, if a vast majority of people do not trust the system (i.e. feel uncomfortable with granting permission on the storage of their biometric data due to security or privacy reasons).

4 Biometric Technology Evaluation

This section analyses the most leading biometric technologies and their suitability for online banking authentication. In order to provide a realistic assessment of those technologies, we propose selection criteria that could be applied to the requirements and characteristics identified in Section 3.

4.1 Selection Criteria

This section discusses a set of parameters used as selection criteria considered in real online banking authentication implementations.

1. Security: it is strength of the system in terms of covered risk and its efficiency to resist potential attacks (considering the risk they represent and its sophistication).
2. Accuracy: due to differences in environment where data is collected, or between readers/scanners employed in biometrics, a 100% of accuracy cannot be achieved. Thus, certain performance thresholds must be defined to consider reliable a biometric technology. The two conventional metrics used to evaluate biometrics performance are the FAR and the FRR.
3. Permanence: it is the condition that biometric should not change over time.
4. Usability: the quality of being user-friendly and closer to user needs and requirements (e.g., acceptability, ease of use, etc.).
5. Implementation difficulty and cost: in terms of technical requirements to be fully deployed and functional, and cost impact of the biometric system implementation effort.
6. Costs: Economic impact of the technology in the overall authentication system (e.g. implementation costs, maintenance, etc.).
7. Adequacy: The quality of being able to meet the needs and expectations of a particular user segment.

Table 1. Biometrics Suitability Assessment

	Security	Accuracy	Permanence	Usability	Implementation difficulty	Costs	Adequacy
Fingerprint	H	H	M	H	L	M	C,P,I
Facial	M	M	M	H	M	L	R,C,P,I
Hand geometry	H	M	M	M	M	H	C,P,I
Iris	H	H	H	L	H	H	P,I
Retina	H	H	H	L	H	H	P,I
Voice	M	M	L	H	L	L	R,C,P,I
Keystroke Dynamics	L	L	L	H	L	L	R,C,P,I
Handwritten Signature	M-	M-	L	M	M	H	C,P,I

Legend: H= High, M= Medium, L= Low

R= Retail, C= Corporate, P= Private, I= Investor customers' profile

4.2 Technology Suitability Assessment

This section shows our results on the evaluation of leading biometric techniques regarding its suitability for the electronic banking. The evaluation has been performed according to the selection criteria introduced in Section 4.1. First results (Table 1) have been derived from the analysis of different technologies (demonstrators) together with desktop research [6].

As it can be observed from Table 4.2, fingerprints, hand geometry, iris, retinal and handwritten signature are not suitable for all user segments. In summary those technique present valuable benefits: (1) **fingerprints recognition** provides a high level of accuracy and high acceptance rate; (2) **hand geometry** provides user-friendliness, its data can be exploited in many forms and requires low data template storage; (3) **iris pattern** matching is a highly accurate technique and relatively easy to operate, being one of the most efficient forms of biometrics; (4) **retinal scans** are highly accurate and require low storage; and (5) **handwritten signature** is widely deployed and well accepted.

However, those techniques, present a low adoption in the electronic banking scenario for two major reasons: the overall system implementation costs and the impact in usability, in terms of carrying an additional device (scanner). Delivering specific hardware to millions of electronic banking customers, may result on a large economic impact, surpassing even the losses of a single entity; while carrying an additional hardware device, might hinder the possibility to perform transactions anytime and anywhere.

In the case of fingerprint scanners, their integration into modern mobile devices, promises a wider adoption of this technique in electronic services, addressing both issues (costs and usability). However, since there is not yet a wide integration and/or accessibility to APIs (e.g. iPhone 6 and Samsung Galaxy S5), this technology remains suitable only to corporate, private and investor user segments (i.e. a smaller percentage of customers performing high risk transactions). In the case of iris and retinal scanners, an alternative could rely on the use of desktop or mobile cameras, resulting in cheaper costs but proven to be of in-

creased difficulty in operation, limiting the usability and its suitability for such scenarios.

Contrary to the aforementioned technologies; facial recognition, voice, and keystroke dynamics are considered suitable for all user segments. At the second stage of our research, we have selected them for further evaluations. We have performed several usability and security experiments with 30 users and 3 different mobile devices; we concluded that, a single biometric technology is not able to fulfill current scenario requirements; therefore, to increase authentication performance, it is recommended to combine more than one approach.

- **Facial recognition** benefits from high user acceptance. Biometric data extraction can be easily achieved without the need of specific sensors; therefore, its implementation can be low cost when taking advantage of modern technologies, such as mobile devices equipped with embedded cameras. Nonetheless, our results demonstrated low performance (75% accuracy) in non-standard environments. Moreover, when asking users about their experience, they were unhappy because of its limited usability in non-controlled scenarios. Finally, this method showed to be vulnerable, allowing authentication using "selfies", which are not difficult to acquire. Therefore, it must be accompanied from additional methods such as liveness detection mechanisms.
- **Voice recognition** provide authentication in a unique and non-intrusive form. It benefits from high acceptance rate because of its high usability. Its hardware requirements represent no bigger costs, since microphones are used to capture the biometric data and they are readily available. Similar to facial recognition, our results demonstrated low performance (85.88% accuracy) in non-standard environments. Thus, voice authentication technologies cannot be considered mature enough and again, they must be accompanied or combined with additional mechanisms. Moreover, voice recognition algorithms must be tolerant to noise and should not be influenced by variations of the voice produced by sore throat or cold.
- **Keystroke dynamics** represent almost no costs (i.e. no especial devices are required). Usability and acceptability are considered high because in most cases it can be performed transparently to the user. However, the main drawbacks of this technique are its low accuracy and low security level during the training phase; therefore, it can be used neither as first factor, nor as second factor authentication. Nevertheless, it is suitable for implementing continuous authentication.

5 Authentication System Architecture

This section proposes an n-factor authentication system for mobile devices. The proposed approach is based on multimodal biometrics and follows client-server system architecture to provides user, device and transaction authentications.

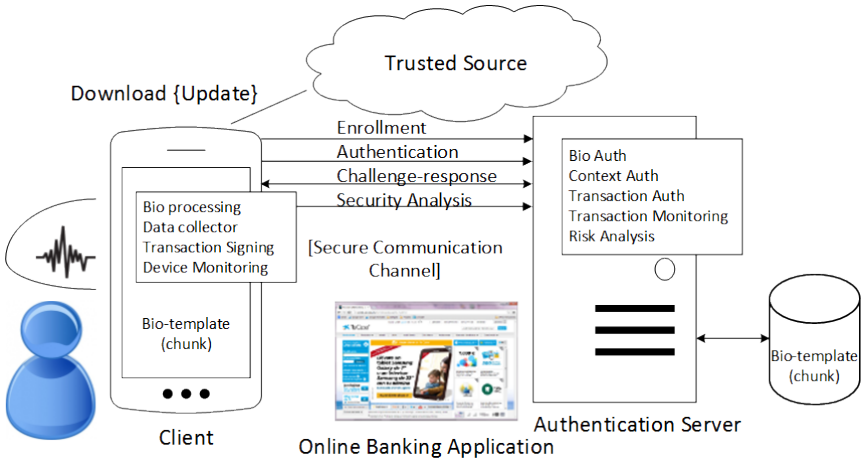

Fig. 1. Client-Server System Architecture

5.1 Client

The client consists in a mobile application that users will download from a trusted source (App Market) (Figure 1). Once the application has been installed and launched, the client will establish a secure communication channel with the server i.e. the online banking authentication server, and allow the registration process. In general, the main goal of the client is to enable users to register in the system, authenticate and perform transactions, while monitoring the security of user's device. To provide those services, the client is comprised of the following modules.

Biometric Processing This module enables server side authentication based on voice recognition, which requires user's explicit interaction. It first collects user's biometric data (voice), extracts the corresponding features, and transforms them, resulting in a biometric template, which is encrypted and split into two or more chunks; one is stored locally (in the device) and the other one remotely (at the online banking system).

Data Collector This module continuously collects user and device information (i.e. interaction of users' with the application); this information is sent to the online banking authentication server in order to enable continuous authentication. The interactions between the data collector, the application, and the authentication server are transparent to the user.

Transaction Signing This module is part of a challenge-response mechanism; it is activated when a user performs an operation. It receives a challenge from

the authentication server as an image displayed to the user; it records the user's voice (response to the challenge) and sends it to the authentication server to be validated. It is assumed that this process cannot be done without user's explicit interaction.

Device Monitoring This module performs security validations on app execution. Results from those validations (e.g., fingerprinting) are sent to the authentication server to enable detection of potential security breaches.

5.2 Server

The server is represented by the online banking system and its infrastructure (Figure 1). It is responsible for establishing secure communications with the clients, and granting or denying access to the online banking system. Server modules enable user, device and transaction authentication, as well as typical transaction monitoring. It also performs risk assessment based on the security information provided by the client device.

Biometric Authentication It implements voice-based authentication, which is done by comparing newly extracted biometric information to the previously stored template. It receives from the client a chunk of the biometric template originally stored in the device at the enrollment process, and retrieves from the database remaining chunks; the authentication server merges and reconstructs the template being able to determine user's identity and decide whether or not to grant access to the electronic banking system.

Transaction Authentication it implements a challenge response mechanism which generates a challenge base on user's operation information. It verifies the authenticity of the response by comparing it to an expected value. Different thresholds might be applied, depending on the operation risk classification [13].

Continuous Authentication this module works independently from the provided credentials, and it is transparent to the user. Its purpose is to enhance the confidence level of user's and transaction's authenticity to the online banking service provider by evaluating context and device information (Tables 2 and 3).

Transaction Monitoring It authenticates transactions based on historical account information. It analyzes parameters like user's behavior on the online banking system (Table 4).

Risk Analysis based on the security analysis of client's device and mobile application behavior, it performs risk assessment, taking decisions, such as, blocking a device or reporting it to the system and user.

6 System Communication

This section details the communication between the authenticating client and the authentication server; all communications will be done via the establishment of a secure communication channel. Data sent from the client to the server will be encrypted using the online banking system public key.

6.1 Registration

This process takes place once a banking mobile application has been downloaded and successfully installed. When the application is launched for the first time it generates a master random key K_m (AES 128bits) and automatically initiates the registration process.

User Registration The identity of an individual and its device will be confirmed at this stage; first, users are required to introduce an activation code or token in order to activate their mobile application. Such token or code can only be obtained by means of a different communication channel (e.g., telephone banking, ATM, banking branch office, etc.). The activation code is valid for a single user and device for a limited lifetime (days), allowing the system to link the application to the device and online banking user registration. Alternatively, the system might require additional valid credentials (e.g., username and password). Upon successful validation of token and credentials, user is requested to setup an application password and afterwards, to register his/her voice.

The client will implement the functions and algorithms to capture and extract user's voice and its corresponding features. It will generate and transform the biometric template using non-invertible transformations. The resulting transformed template will be divided into two or more chunks and stored in a distributed fashion. The first chunk will be encrypted by the mobile application and securely stored in the user device (using a password-based key derivation function). Additional chunks of the template will be encrypted using the authenticating server's public key $PK_{AS}Sig(M)$, and ultimately sent to the authenticating server.

Device Registration The activation code is valid for registering one mobile device per valid user. On activation, device characteristics (Table 1) and network session parameters (Table 2) are sent to the authentication server, and stored for further validations that will support the continuous authentication module. Note that, registration of new devices (e.g. in cases of theft or loss) will require a valid (new) token associated to the new device.

Profile Registration The key tap dynamics (i.e. key tap size, coordinates, time, pressure, etc.) obtained through the device's sensors will be collected and sent to the authentication server during registration, at each login attempt and during user's application interaction. A training phase of at least 15 user interactions [7] might be required before considering key tap authentication.

6.2 Individual's Authentication

User authentication occurs every time a user launches the mobile banking application. In order to enable its features the application password is required.

Key Tap Dynamics After the training phase, the system will start validating user's key tap dynamics. Collected patterns will be compared against historical patterns (stored in the authentication server), the resulting score will be used to determine the authenticity of the user and enforce the continuous authentication module. If no interaction is detected, a session timeout will take place, and the online banking system will force new authentication to the mobile application.

Voice Authentication Banking operations or transactions will require voice-based authentication; a challenge response mechanism will be triggered delivering an image with a challenge associated to user's operation. On each authentication the voice-based response will consist on a newly generated template that will be sent along with the chunk of the template stored in the device. The authentication server will request remaining chunks to banking database server. Thus, the full template will only be available during authentication; the authentication server will merge all chunks in memory; it will compare the new sample to the template and compute the scoring value that will determine user's authenticity. Afterwards, the full template will be deleted from the memory of the authenticating server.

6.3 Device Authentication

Device information obtained on each session will be compared against historical information.

Device Fingerprinting The fingerprinting of the device (Table 2) is evaluated every time the user interacts with the banking application. Through the device authentication, user's identity will be reinforced. If different device data is detected, a scoring will be computed and the continuous authentication module will trigger a warning that could cause blocking further communications from detected device. Additionally, security analysis of the banking application on execution will be done, by performing traditional tamper proof checks (e.g., integrity checks, emulator detection, etc.).

Network Session Identification Contextual information such as user's network characteristics will be evaluated. If session parameters reveal anomalous data, e.g., from a source listed as compromised or associated to fraudulent activity, current transaction might be blocked.

6.4 Transaction Authentication

Table 2. Device Fingerprinting: Evaluation Parameters

Type of characteristics	Parameters
Device unique characteristics	UUID, IMEI, IMSI, MSISDN, MAC
Hardware characteristics	CPU model, clock speed, memory latency, memory size
Other characteristics	OS and browser characteristics

Table 3. Network Characteristics: Session Parameters

Type of characteristics	Parameters
Blacklisted, whitelisted and anonymous proxies	IP address
Geographical distance between operations	IP address geolocation
High risk country classification	IP address geolocation
Frequency of access from a single source to multiple accounts	IP address, timestamp, number of sessions

Table 4. Transaction Monitoring: User's Account Parameters

Type of characteristics	Parameters
Banking sessions	Operation timestamp, time between operations, frequency of access
Unknown or blacklisted accounts	Destination account number
Operations amounts	Single operation amount; average amount in operations

Challenge-Response A user selects and configured an operation (e.g., a money transfer), the challenge-response component generates the operation-based challenge, using actual operation's parameters (e.g., last four digits of destination account, random selected numbers of the transfer amount, etc.). The challenge is then delivered to the client as an image. User must respond to the challenge using his mobile's microphone. The client device will capture user's voice sample, generate the biometric template, compress the audio file and send both to the authentication server. The authentication server receives the data and validates its integrity; it performs bio-authentication, while verifying that the response fully corresponds to the operation or transaction.

Transaction Monitoring It performs evaluations of user's account behavior (Table 4) in parallel to the authentication module. Tracking user's electronic banking operations and transaction history while interacting with the service, allows the system to identify deviations from the expected online behavior and ultimately detect fraudulent activity.

7 Related Work

Until now continuously evolving biometric methods, solutions and techniques have led to a wide set of interesting authentication approaches. We have focused on those aimed at providing authentication in electronic services.

Authors in [12] proposed a biometric-based authentication solution based on fingerprints. At enrollment, users must physically visit a branch to register their fingerprints in a secure manner. Afterwards, users receive from the bank a fingerprint scanner that contains user's fingerprint and an embedded secure password. To authenticate themselves users need to plug the device in a USB port, and place their finger on the scanning device. Although interesting, this approach has not considered the usability and costs that represent distributing fingerprint scanners to potential (millions of) electronic banking users.

Authors in [2] proposed a novel biometric-based authentication system to secure online transaction using real time fingerprint image. Their approach, provides authentication to Android-based mobile banking applications. Although promising, fingerprint-based approaches rely on the use of fingerprint scanners, which are not yet integrated into all mobile devices. In this regard, authors also proposed, the use of mobile digital cameras to capture the fingerprint image at run time, process it and send it to the server. Its main drawback is that the proposed approach does not consider a realistic scenario, which is much more complex than described by the authors. There is lack of details on how to addressed common issues associated to electronic banking scenario, such as, the storage of biometric data, performance and security in terms of potential replay attacks.

Authors in [3] provide empirical performance evaluation of a challenge-based speaker recognition approach; they evaluated the most prominent algorithms in literature and demonstrated their availability for mobile authentication.

Authors in [7] proposed an authentication mechanism that constructs and analyzes four different keystroke dynamic classifiers from mobile sensors, which identify key tap patterns of users and detect anomalous key tap dynamics. Their approach focuses on the login process of mobile devices (not specifically electronic banking). It is able to verify after certain training whether a login attempt is done by registered user or by an attacker in possession of the user's credentials. Their system evaluates parameters, such as, duration and size of each key tap, latency between key taps, and all accelerometer readings over the course of a login attempt. Other sensor data could be considered, to improve its performance in terms of FAR and FRR.

8 Conclusions

This paper has analyzed the potential of biometric authentication. It has been shown that, despite the great advances of biometric technology, they continue to raise important concerns regarding security, usability, privacy and costs, which limit its adoption in electronic banking systems. From the suitability assessment we can conclude that, fingerprints, facial and voice recognition are the most promising techniques for online banking authentication. The main reasons are because of the trade-offs between technology's maturity, usability, and hardware related costs. Key tap dynamics also provide a high degree of usability and low costs. However, due to its low accuracy rate, it could only be con-

sidered as a complementary solution. As a result, this paper has proposed a secure and cost-effective multimodal biometric authentication system using mobile devices, which combines different techniques to provide user, device and transaction authentication. The proposed approach particularly addresses the usability, performance and security concerns in electronic banking that common (generic-purpose) biometric systems do not consider. Future research directions are aimed at the implementation of a proof of concept. Our evaluation plans include a functional banking application, with multiple devices and multiple (stressed) scenarios.

References

1. WG Art. 29. Dictamen 3/2012 sobre la evoluci'on de las tecnologias biometricas. Technical report, Directiva 95/46/CE, 2012.
2. Mossab Baloul, Estelle Cherrier, and Christophe Rosenberger. Biometric mechanism for enhanced security of online transaction on android system: A design approach. In *14th International Conference on Advanced Communication Technology (ICACT)*, pages 1193 – 1197. IEEE, February 2012.
3. Mossab Baloul, Estelle Cherrier, and Christophe Rosenberger. Challenge-based speaker recognition for mobile authentication. In Arslan Brmme and Christoph Busch, editors, *BIOSIG*, pages 1–7. IEEE, 2012.
4. Darrel Burke and Eran Kalige. A case study of eurograbber: How 36 million euros was stolen via malware. Versafe, December 2012. White paper.
5. eIDAS Task Force European Comission. Regulation (eu) n910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec. *European Comission*, 2014.
6. Alexander Eng and Luay A. Wahsheh. Look into my eyes: A survey of biometric security. In *ITNG*, pages 422–427. IEEE, 2013.
7. Grant Ho. Tapdynamics: Strengthening user authentication on mobile phones with keystroke dynamics. Technical report, Stanford University, 2013.
8. Seyyede Samine Hosseini and Shahriar Mohammadi. Review Banking on Biometric in the World's Banks and Introducing a Biometric Model for Iran's Banking System. *Journal of Basic and Applied Scientific Research*, 9(2), 2012.
9. Davide Maltoni James Wayman, Anil Jain and Dario Maio. *Biometric Systems Technology, Design and Performance Evaluation*, chapter An Introduction to Biometric Authentication Systems. Springer, 2005.
10. Dave Marcus and Ryan Sherstobitoff. Dissecting operation high roller. McAfee, 2012. White paper.
11. Manel Medina, Jetzabel M. Serna-Olvera, Andreas Sfakianakis, Jordi Aguilà, and Luis Angel Fernandez. eidas in e-finance and e-payment services: Current practices and recommendations, 2013.
12. Rana Tassabehjia and Mumtaz A. Kamalab. Evaluating biometrics for online banking: The case for usability. *Journal of Information Management*, 32(5), 2012.
13. Jorge Aguila Vila, Jetzabel Serna-Olvera, Manel Medina, and Andreas Sfakianakis. An Analysis of n-factor Authentication in e-Banking Environments. *Journal of Information Assurance and Security*, 9(1), 2014.