Use of Biometrics in Mobile Banking Security: Case Study of Croatian Banks

Ammar Avdić

BDO Croatia, Croatia

Summary
With the day-to-day advancement of digital technologies, it is becoming easier to integrate mobile phones into business processes. One of the first organizations to understand the benefits of using mobile phones as a device in business are financial institutions. With the development of technology, financial institutions, especially banks, use mobile applications as a direct way of communicating with customers, speeding up the process and generating savings in their businesses. But with the development of technology, there is also the question of whether the security of mobile applications follows the development of technology. In this paper, a brief overview of the impact of biometrics on modern business will be given, with emphasis on mobile technology. A survey at EU Member State will be presented to see if banks use advanced authentication methods using biometric user identifiers, and conclusions will be drawn on the results of research and use of biometric authentication methods in mobile banking.

Key words:
mobile biometrics; fingerprint; mobile banking; financial institutions

1. Introduction

From this section, input the body of your manuscript according to the constitution that you had. For detailed information for authors, please refer to [1].

Financial services are slowly moving towards the adoption of biometrics for authentication. Years of biometric research highlighted the advantages of biometrics and their potential to improve convenience and security for users. However, the deployment process needs to be performed in a thoughtful and comprehensive manner [9].

Worldwide, Biometrics Research Group estimates that the number of total smartphone users worldwide will surpass 3 billion in 2017. Continuing growth of the global smartphone user base along with the consumerization of biometrics will drive the growth of mobile biometric authentication. They project that inexpensive smartphones will open new opportunities for marketing and commerce in emerging markets, where many consumers previously had no access to the Internet. Meanwhile, in mature, established markets, smartphones will rapidly shift the paradigm to more consumer media usage and toward more enterprise-centric mobile usage. Biometrics Research Group,. expects that mobile commerce adoption and banking will also accelerate due to continuing wide-scale integration of biometric technology into smartphones [27].

Mobile devices have become an integral part of our routine activities. This is particularly the case with the rapid growth and widespread use of smartphones and digital tablets. The processing capability of these devices has advanced up to the point that most digital activities that can be accomplished on workstations or laptops can also be performed on these portable devices. Routine activities, such as personal and corporate e-mail communications, on-line banking transactions, accessing paperless prescriptions services, route navigation, etc. can also be carried out ubiquitously with these devices [25].

M-banking and m-payment apps are recognized far and wide as highly critical components of mobile information services, providing a host of value-added and technology-based financial services to consumers. These services include, but are not limited to, funds transfers, balance inquiries, buying insurance, paying utility bills, receiving critical service alerts, messaging personal banking advisors, and saving beneficiary information [10].

Payment methods using mobile devices instead of using traditional methods (cash, credit card, etc) has been gaining popularity all over the world. The ubiquitous nature of smartphones and tablets has widened the ambit for using these devices for payments and other daily life activities. Recent advancements in mobile technology along with the convenience of mobile devices made these applications possible. Despite the worldwide user adoption of mobile applications, security is the key challenge in mobile banking and payments system. Mobile payments systems need to be very efficient and provide utmost security endlessly [7].

While mobile security risks may be seen by some as an extension of existing threats to traditional computing systems, the mobile threat landscape is an extremely fast-moving environment [26]. The financial services industry has accepted the potential of mobile banking. The industry has deployed mobile banking applications to enable customers to reap various benefits offered by these applications. However, security threats in mobile banking has kept many customers from adopting it. The current concerns of mobile banking that worry potential mobile banking users are as follows [18]:

- Mobile malware: Today, malware attacks are

Manuscript received October 5, 2019
Manuscript revised October 20, 2019

migrating from traditional systems to online banking systems. The attackers have developed malware that specifically targets mobile banking applications, and the number and types of malware targeting mobile banking applications is expected to increase in future.

- Usage of third-party applications: Third-party applications are not fully trusted. Some of the applications have been developed by malicious fraudsters and attackers.
- Usage of unsecured Wi-Fi: Wi-Fi is available in most public places, such as shopping malls and airports, and hackers and cybercriminals may gain access to smartphones and launch man-in-the-middle and relay attacks.
- User behavior: User behavior is also helpful for an attacker to fulfill his/her malicious goals as users are prone to download third-party applications, use unsecured Wi-Fi, and open and click links in short message service or email. Attackers also gain access when the smartphones of the users are lost/stolen

As the level of security breaches and transaction frauds increase day by day, the need for highly secure identification and personal verification information systems is becoming extremely important especially in the banking and finance sector. Biometric technology appeals to many banking organizations as a near perfect solution to such security threats. Though biometric technology has gained traction in areas like healthcare and criminology, its application in banking security is still in its infancy. Due to the close association of biometrics to human, physical and behavioral aspects, such technologies pose a multitude of social, ethical and managerial challenges [29].

A survey [21] has found that there is seemingly a good level of awareness and acceptance of certain biometric methods. The participants had heard of the vast majority of methods, with only hand vein recognition being underrepresented, although this is perhaps understandable given that this technology is not particularly widespread. While there are significant differences between the underlying technologies of hand vein and palm print recognition the method of collection will look similar to the average person.

In that survey [21], it is notable that while there is a general acceptance of these technologies, it is very much dependent on the context. However, the research has highlighted that users are seemingly the most comfortable with those methods that are more commonplace and familiar (e.g., fingerprint or facial recognition). When considering methods that are slightly more intangible (e.g., typing or gait analysis) they are typically less well regarded or understood.

Additional survey [2] suggests that existing mobile face detection methods can be categorized into skin-tone, machine-learning and those based on the combination of both. Similarly, mobile face recognition methods can be broadly categorized into client-server or device oriented. The average reported mobile face detection and recognition accuracies of 89% and 83%, respectively, are quite low for mobile-based user authentication. Current countermeasures to face spoof attacks use motion, texture, image quality, and deep learning-based methods for print and replay attacks on a mobile device. However, the reported error rates are high, suggesting the need for further advancement

According to some authors [17] the biometric security systems are the systems which uses the physical characteristics of a person like fingerprint, hand geometry, face, voice and iris. These systems overcome the drawbacks of the traditional computer based security systems which are used at the places like ATM, passport, payroll, drivers' licenses, credit cards, access control, smart cards, PIN, government offices and network security

Some authors have proposed a simple, effective and user-friendly, behavioral biometric-based remote user authentication solution for financial sector. The paper targets the users of mobile banking apps and helps the bank server in identifying the genuine user from the timing-differences of the entered strokes and the movements the user makes while entering the 8-digit secret [1].

Several contributions have been made to this research area in this paper [23] Firstly, they enhanced the security and privacy protection of biometrics based on the cancelable biometric approach through one-way transformation and offline token matching. Secondly, they adopt the RS block coding approach to enable error handling in fingerprint features so that they are stable enough to be used to bind and unbind a biometric key. Thirdly, they show how to secure long biometric key from Fingerhash.

Multiple user active authentication, in contrast with single user active authentication, requires verification of identity of multiple subjects [24].

Personal identification technology is nowadays becoming more important in security systems. Today authenticating through traditional mode such as password, key, magnetic card etc., are vanishing and disliked by people since they could be stolen or easily forgotten. In order to fill this vanishing space biometric technology is emerging in wide number of systems. Also, biometric systems have been an important area of research in these recent years [6].

Biometric characteristics are [30]:

- Universality: Every individual accessing the application should possess the trait.
- Uniqueness: The given trait should be sufficiently different across individuals comprising the population.

- Permanence: The biometric trait of an individual should be sufficiently invariant over a period of time with respect to the matching algorithm. A trait that changes significantly over time is not a useful biometric.
- Measurability: It should be possible to acquire and digitize the biometric trait using suitable devices that do not cause undue inconvenience to the individual. Furthermore, the acquired raw data should be amenable to processing in order to extract representative feature sets.
- Performance: The recognition accuracy and the resources required to achieve that accuracy should meet the constraints imposed by the application.
- Acceptability: Individuals in the target population that will utilize the application should be willing to present their biometric trait to the system.
- Circumvention: This refers to the ease with which the trait of an individual can be imitated using artifacts (e.g., fake fingers), in the case of physical traits, and mimicry, in the case of behavioral traits.

Some authors [15] conducted the study which purpose was to examine the willingness of financial institutions to adopt mobile banking and how the service features and security methods of mobile banking vary among those financial institutions adopting mobile banking. Specifically, the research focused on whether states coverage, size and charter type will affect financial institutions' decision in adopting mobile banking, and how those three factors will affect mobile banking service features and security methods provided. In addition, commercial banks and credit unions were compared to examine whether they differed in providing mobile banking service features and security methods.

One study [22] conducted forensic examination of twelve popular Android m-banking apps in Nigeria and assessed their performance based on five OWASP MASVS-L2 requirements. From our findings, while all of the apps performed well in two of the requirements: not saving sensitive data in backup generated by the mobile OS and educating users on security best practices, all except one of the apps held data of sensitive value, such as PII and transaction-generated data, in the memory of the test device and did not enforce any device access security policy. All the m-banking apps failed the requirement of removing sensitive data when backgrounded. In this particular paper, authors conducted forensic investigations and security assessment analysis of seven popular Android m-banking apps in Thailand. We determined that data of forensic interest, including sensitive user data, pertaining to the use of such apps can be recovered using DD and JTAG techniques. For example, we were able to recover from Bank F information such as account number, account type, and account balance, from Bank B, Bank C, and Bank F information such as citizenID, date of birth and thumbnails for banking transactions, and from Bank A and Bank G information such as user's PIN code. The SMS messages we recovered could also be used to verify prior transactions (e.g. timestamp and OTP). Authors also conducted a security assessment analysis of the apps and determined that more than three of the apps investigated do not implement root device detection. In addition, despite the built-in encryption libraries, the study reveals that some apps do not encrypt user data. The repackaging app analysis also shows that it is possible to modify the m-banking apps and install the repackaged apps. If the repackaged apps are implemented to intercept SSL traffic, an attacker is then able to intercept SSL traffic and obtain sensitive information.

The findings of other study [4] revealed that perceived risk, compatibility of software, customer profile and external threat are the factors that influence the usage of mobile banking services. Customer perceived risk about completion of a transaction or loss of money makes them reluctant to use mobile banking. In addition, external threats such as hacking and phishing make people reluctant to use mobile banking.

The results of this study [19] show that perceived vulnerability, self-efficacy, response cost, descriptive norm and psychological ownership all were important in determining personal computing security intentions and behavior for both home computer users and mobile device users. However, perceived severity was only found to play a role in mobile device security behavior and neither response efficacy nor subjective norm influenced security intentions for either type of user.

Some studies [3] have unveiled the core barriers that have so far impeded the adoption and usage of M-banking. There is not a unified position concerning adoption and usage blockades. Factors differ with contexts, markets, time and kinds of innovations. However, this study is unlike past studies that merely studied students within a specified institute in a restricted jurisdiction. This is one of the first studies to have nationally explored adoption and usage issues; thus, it is anticipated to potentially contribute to the prevailing literature especially in Pakistani context where a few studies prevail, addressing M-banking adoption and usage barriers.

Some authors [31] had designed and developed a mobile application for securing the mobile payments. They used the login mechanism to secure the mobile application and an RSA encryption scheme to secure the transactions among the banks. To secure the login, they used biometrics and have proposed a new algorithm named privacy-preserving biometric-based authentication algorithm. For secure transactions, they use RSA encryption scheme on direct debit method. They analyze

their novel privacy-preserving biometric-based authentication algorithm for privacy, correctness, and complexity. Further, they gave a solution to improve the system using cloud computing.

A group of authors [16] claim that Governments have put in a significant amount of resources in order to develop facial biometrics and have begun to implement them for day-to-day use. Biometrics have had a positive impact on border crossing at airports, identifying fugitives and criminals, and with the right development, can also be implemented in banks, shops, and many other offices. Facial biometrics can easily save those in danger if used in the right way, leading us to believe that the development of facial biometrics is critical and will continue. However, the growth of this technology is completely dependent on the security measures in place to ensure that privacy is protected, and accuracy is exact. In order to do so, authentication needs to be precise.

Some past studies [28] contribute to the gap in biometric research, by addressing the call for more user-centric studies to identify and understand user attitudes, perceptions and acceptance of biometrics in specific applications and contexts. Using the ebanking sector, as a relevant and probable application of biometrics, we found that self-efficacy and perceptions of the security biometrics can provide to b-banking, are influential factors in the potential adoption of b-banking by users. These findings can be used by organizations in the ebanking sector to examine the potential viability of introducing biometrics from the perspective of the user. They can also be used to inform the development of management strategy to influence how this new service can be disseminated to and promoted amongst its customers, to capitalize on the organizational investment in developing a banking system.

Of course, the question of privacy in digital ages is inevitable. Some authors [11] discussed about privacy and digital privacy concept. They have identified the factors that determine the level of privacy and recommended a framework for digital privacy and taxonomy diagram for domain.

Some authors [12] claim that there is no security system that is completely out of spoofing. Every system is subject to breakable. The techniques used to prevent the attacks help to increase the time, and cost. Fingerprints can be easily forged from touched surfaces and can be copied in a small amount of time using readily available materials. All the liveness detection mechanisms in fingerprint systems can be easily overwhelmed using wafer thin gelatin and silicon artificial fingerprints. Some authors presented an evaluation framework for analyzing factors influencing user interaction in mobile devices with respect to touch interactions [8].

Mobile-Banking industry in today's technology is facing several major challenges and issues. First and perhaps most important is the security concern. Customers are certainly concerned of giving their bank account information online or paying an invoice through internet. Another challenge facing mobile-banking industry and the E-business in general is the quality of delivery service including both delivery speed i.e., short advance time required in ordering and delivery reliability which means delivery of items or services on time. Mobile-banking application at present is using the username and password security mechanism which can easily reached by mere guess work and password can be hacked. To reduce the potential vulnerabilities regarding to the security, a combination of user id & password and fingerprint recognition system seem to be one of the most reliable means of authentication in a, mobile banking application environment. In order for mobile banking to continue to grow, the security and the privacy aspects need to be improved [14].

Some authors [5] claim that electronics transaction is increasing in day-by-day in common man's life therefore it is luring to people involve in unlawful activity to commit frauds in electronics tractions also. They understand the weakness of the system and exploit. Though may very effective Public- Private-Key based algorithms have been developed providing security for transmissions of electronic data there is still have room for leakage of key. According to them,if we use biometrics based in electronic transmission then we can ensure most safe transmission of data, especially in commercial tractions.

Some authors [25] have also investigated how the accuracy performance may be influenced by variations in factors such as the timing resolution of timing feature data, combinations of different feature data types, input string lengths and subject sizes. Experimental results show that, with the use of the two-factor authentication method, even if an impersonator knows the input string (i.e. PIN) of a legitimate subject, 9 out of 10 impersonation attempts can be successfully identified. Authors also showed that the accuracy performance can be increased by combining different feature data types. The results we have obtained so far demonstrate that touch dynamics biometrics can be an effective solution to strengthen the security level offered to mobile devices.

Some authors [20] claim that while banks continue to take new and stronger security measures for mobile and online banking applications, security vulnerabilities in banking applications are searched by malicious people with various methods and they will continue to search these security vulnerabilities. For this reason, banks are required to carry out all safety tests starting from the first stage of the software, especially the penetration tests. The tests to be carried out for each stage are very important, as every new application feature developed can cause a different security vulnerability. When developing internet banking systems, weaknesses in existing systems must be

thoroughly analyzed for designing better authentication systems and new measures should be taken accordingly.
They [20] also claim biometric recognition systems developed for mobile devices such as fingerprint reading should be integrated and used in mobile banking applications. From time to time, banks are advising users not to connect to phishing links from fraudsters and not to share one-time passwords with anybody includes bank staff. In this regard, it can be suggested that these fake links, which are shown as advertisements especially on social media, can also be identified and prevented by banks. Users should also be conscious of social engineering attacks.
In this paper [13], authors have discussed about the architecture of UPI based Apps, their transaction flow, authentication mechanism and its USP against other mobile banking payment solutions. They have identified few security issues and have proposed security enhancement solutions to deal with them (MPIN update transaction security issues and detection of fraud transactions related to MPIN update and UPI financial transactions). It is observed that inclusion of email alerts and additional fields in MPIN authentication shall enhance the security of existing UPI application.

2. Methodology

As a source of data for this paper, theoretical background of mobile biometrics was gathered through secondary data from numerous books and articles in the area of contemporary application of mobile forensics [22, 24, 26] but also examples from business practice were used, as well as analysis of gathered information of the offers for mobile banking that Croatian banks use. The data was collected in the period between January 24th and May 28th, 2019. Financial data of the banks were collected through publicly available information, such as bulletin from Croatian National Bank [32]. It is important to note that the financial data from 2017 is published in the 2018, while the 2018 data is published in 2019., that is why the author used 2017 data.

3. Results and Discussion

A great number of Croatian banks are offering mobile banking as an additional service. Out of 24 banks (as of December 31st 2017), 19 of them offered mobile banking services:

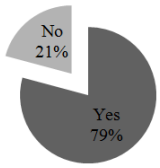

Fig. 1 Does a Bank offer mobile banking?. (Author's illustration)

If we compare the size of the assets Banks are having compared to offering mobile applications services, we can see that the banks with larger assets offer mobile banking:

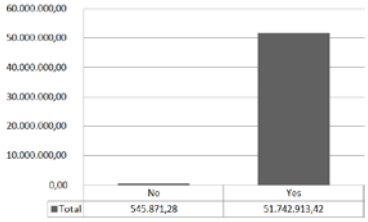

Fig. 2 Total value of assets (in 000 €) of banks in 2017 depending on whether they are offering mobile banking or not (Author's illustration)

If we compare the profit of the Banks compared to offering mobile applications services, we can see that there is not a huge difference in profits:

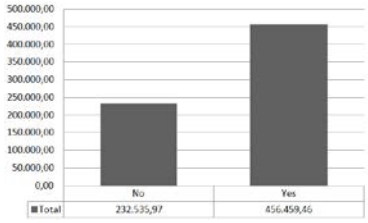

Fig. 3 Total profit (in 000 €) of banks in 2017 depending on whether they are offering mobile banking or not (Author's illustration)

Next, we have researched the situation in whether it is possible to use fingerprint as an authentication method (the N/A refers to those banks who have not offered mobile banking services):

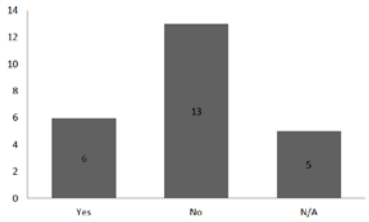

Fig. 4 Fingerprint as an authentication method (Author's illustration)

And face recognition as an authentication method:

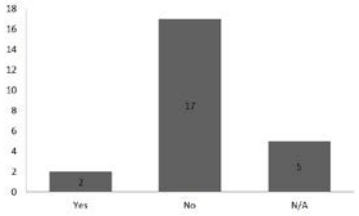

Fig. 5 Face recognition as an authentication method (Author's illustration)

As seen from the figure above, the face recognition is still not fully implemented as a method of authentication. Of course, this cannot be only seen as a service problem, but rather a technical problem, since not many smartphones on the market today offer face recognition. The potential customer base at the moment is simply too small.

4. Conclusion

Mobile information services have revolutionized business models and service delivery methods by facilitating consumer access to information and order placement via mobile apps. In developed markets, mobile banking (mbanking) and mobile payment (m-payment) applications have replaced text-based mobile services [10].

This case study was developed to provide an in-depth analysis of the current status of using biometric methods of authentication regarding mobile banking application in Croatia. Through the study, author identifies the applicability of biometric controls in banking environment. The success factors displayed in this paper through other papers and studies would help banking organizations to plan their business strategies and processes with the required flexibility and adjustments that are warranted for a successful biometric security implementation.

Author concludes that although there is some implementation of biometric authentication on mobile banking applications, it is not yet fully accepted inside Croatian banks. Less than 50% of banks have implemented some sort of biometric method of authentication for their mobile banking application. Various social, ethical and technological issues need to be dealt with before implementing this kind of security. With dealing with it, more biometric in banking sector would be welcomed.

References

[1] A. Buriro, S. Gupta and B Crispo, " Evaluation of motion-based touch-typing biometrics for online banking" 2017 International Conference of the Biometrics Special Interest Group, 2017.

[2] A. Rattani, and R. Derakhshani, "A survey of mobile face biometrics" Computers & Electrical Engineering, vol. 72, pp. 39-52, 2018.

[3] A. W. Siyal, D. Ding and S. Siyal, "M-banking barriers in Pakistan: a customer perspective of adoption and continuity intention", Data Technologies and Applications, Vol. 53(1), pp.58-84, 2019

[4] A. Yadav, "Factors influencing the usage of mobile banking among customers" IUP Journal of Bank Management, vol. 15(4), pp. 7-18, 2016.

[5] A: Tyagi, P. B. Singh, V. S. Yadav, S. K. Singh and A. Tiwari, "Security role of biometrics in electronic transactions" 2012 IEEE International Conference on Computational Intelligence and Computing Research, 2012.

[6] B.Prasana Lakshmi and A.Kannammal, "Secured authentication of space specified token with biometric traits - face and fingerprint", International Journal of Computer Science and Network Security, vol .9(7), pp.231-234, 2009.

[7] D. Pal, P. Khethavath, T. Chen and Y. Zhang, Y. "Mobile payments in global markets using biometrics and cloud". International Journal of Communication Systems, vol. 30(14), 2017.

[8] E. Ellavarason, R. Guest, and F.Deravi, (2018). "A framework for assessing factors influencing user interaction for touch-based biometrics". 26th European Signal Processing Conference, pp. 553-557, 2018.

[9] G. Lovisotto et al. "Mobile biometrics in financial services: A five factor framework", University of Oxford, 2017.

[10] H. Karjaluoto, A. A. Shaikh, H. Saarijärvi, and S. Saraniemi, "How perceived value drives the use of mobile financial services apps" International Journal of Information Management, 2018, in press.

[11] J. Cosic, Z. Cosic and M. Baca, "Towards creating a digital privacy framework", International Journal of Computer Science and Information Security, vol. 13, no. 8, pp. 1-4, 2015.

[12] J. George Chellin Chandran and R. S. Rajesh, "Performance analysis of multimodal biometric system authentication", International Journal of Computer Science and Network Security, vol .9 (3), pp. 290-296, 2009.

[13] K. K. Lakshmi, H. Gupta and J. Ranyan, "UPI based mobile banking applications - security analysis and enhancements", Amity International Conference on Artificial Intelligence, pp 903-908, 2019.

[14] L. Sharma and M. Mathuria, "Mobile banking transaction using fingerprint authentication" 2nd International Conference on Inventive Systems and Control, pp. 1300-1305., 2018.

[15] L., Huei; Z, Yu; and K. L. Chen, "An investigation of features and security in mobile banking strategy", Journal of International Technology and Information Management: vol. 22(4), pp. 23-45, 2013.
[16] M Galterio, S. Shavit and T. Hayajneh, "A review of facial biometrics security for smart devices", Computers, vol. 7(37), pp. 1-11, 2018.
[17] M. N. Uddin et al. "A survey of biometrics security system", International Journal of Computer Science and Network Security, vol .11(10), pp.16-23, 2011.
[18] M. Wazid, S. Zeadally and A.K. Das, A. K., "Mobile banking: evolution and threats: malware threats and security solutions" IEEE Consumer Electronics Magazine, vol. 8(2), pp. 56-60, 2019.
[19] N. Thompson, T. J. McGill and X. Wang, "Security begins at home: Determinants of home computer and mobile device security behavior". Computers & Security, vol. 70, pp. 376-391, 2017.
[20] N. Yildirim, N., and A. Varol, "A research on security vulnerabilities in online and mobile banking systems". 7th International Symposium on Digital Forensics and Security, 2019.
[21] O. Buckley and J.R.C. Nurse, "The language of biometrics: Analysing public perceptions", Journal of Information Security and Applications, vol. 47, pp 112-119, 2019.
[22] O. Osho, U.L. Mohammed, N.N. Nimzing, A.A. Uduimoh and S. Misra, "Forensic analysis of mobile banking apps", The 19th International Conference on Computational Science and its Applications, Lecture Notes in Computer Science, vol. 11623, pp. 613-626, 2019.,
[23] O. T. Song, A. Teoh Beng Jin, T. Connie, "Personalized biometric key using fingerprint biometrics", Information Management & Computer Security, vol. 15 (4), pp.313-328, 2007.
[24] P. Perera, and V. M. Patel, "Face-based multiple user active authentication on mobile devices", IEEE Transactions on Information Forensics and Security, 2018, unpublished
[25] P. S. Teh, N. Zhang, A. B. J. Teoh and K. Chen. "TDAS: a touch dynamics based multi-factor authentication solution for mobile devices" International Journal of Pervasive Computing and Communications, vol 12(1), pp. 127-153, 2016.
[26] R. Chanajitt, W. Viriyasitavat and K.-K. R. Choo, "Forensic analysis and security assessment of Android m-banking apps", Australian Journal of Forensic Sciences, vol. 50(1), pp. 3-19, 2016.
[27] R. O'Neil and C. Burt, "Mobile biometric applications", Biometrics Research Group, 2017.
[28] R. Tassabehji and M. A. Kamala, "Improving E-banking security with biometrics: modelling user attitudes and acceptance" 3rd International Conference on New Technologies, Mobility and Security, 2009.
[29] S. Venkatraman and I. Delpachitra, "Biometrics in banking security: a case study", Information Management & Computer Security, vol. 16(4), pp.415-430, 2008.
[30] V. S. R. Polly, N. Arcot and J. Charapanamjeri, "Evaluation of biometrics", International Journal of Computer Science and Network Security, vol .9(9), pp.261-269, 2009.
[31] A. A. Hnaif and M. A. Alia, “Mobile payment method based on public key cryptography”, International Journal of Computer Networks & Communications, vol 7(2), pp. 81-92, 2015.
[32] Croatian National Bank, “Bank Bulletin”, Croatian National Bank, 2018.

Ammar Avdić MA is currently employed as IT auditor at BDO Croatia Ltd. and as an external associate on Department of Informatics at Faculty of Economics and Business in Zagreb. He received his MA degree in the field of managerial informatics in 2010 Faculty of Economics and Business Zagreb where he also finished specialist postgraduate study in the field of IT management in 2014. He is currently enrolled as a PhD student at Faculty of Organization and Informatics in Varaždin. His areas of interests are information systems audit, computer security, IT governance and IT management. The author can be contacted at ammaravdic@gmail.com.