Privacy-preserving Biometric Authentication Model for e-Finance Applications

Christina-Angeliki Toli and Bart Preneel
imec-COSIC KU Leuven, Leuven, Belgium

Keywords: Biometrics, Cryptography, Security, Privacy-enhancing Technologies, Privacy Metrics, Access Control.

Abstract: Widespread use of biometric architectures implies the need to secure highly sensitive data to respect the privacy rights of the users. In this paper, we discuss the following question: To what extent can biometric designs be characterized as Privacy Enhancing Technologies? The terms of privacy and security for biometric schemes are defined, while current regulations for the protection of biometric information are presented. Additionally, we analyze and compare cryptographic techniques for secure biometric designs. Finally, we introduce a privacy-preserving approach for biometric authentication in mobile electronic financial applications. Our model utilizes the mechanism of pseudonymous biometric identities for secure user registration and authentication. We discuss how the privacy requirements for the processing of biometric data can be met in our scenario. This work attempts to contribute to the development of privacy-by-design biometric technologies.

1 INTRODUCTION

Systems that automatically recognize a user's identity based on his biometric characteristics are becoming increasingly prevalent or even compulsive. From fingerprint scanners, embedded in smart mobile phones, to border control infrastructures, the extensive use of biometric authentication applications has increased the security and privacy concerns (Prabhakar et al., 2003). Specifically, security and privacy are two different complementary fields (Campisi, 2013). Biometrics were initially introduced as a technology that overcomes the security limitations of the traditional authentication approaches, such as passwords or tokens (Furnell, 2015). However, biometric recognition relies on who a person is, or what someone does (Mordini and Tzovaras, 2012). Hence, biometric data may reveal more information about the user than necessary (Li and Jain, 2015).

State-of-the-art in cryptographic techniques presents concrete mechanisms that enhance the security of biometric designs (Campisi, 2013). The research focus on testing the approaches towards malicious adversaries, and evaluating the implementation in realistic scenarios (Nandakumar and Jain, 2015). Furthermore, the users' fundamental right to privacy has been internationally established and legally supported (Kindt, 2009). Security frameworks standardize the developments, while privacy principles confirm biometric data sources, ensuring that they are accurate and consistent (Podio, 2011). However, adopting the procedures and implementing these requirements are challenging tasks (di Vimercati et al., 2015). Cryptography has offered privacy-aware approaches, addressing the practical difficulties on the design of biometric schemes (Mordini and Tzovaras, 2012; Miltgen et al., 2013). In 2016, the European General Data Protection Regulation has set new recommendations for the processing of biometric information (EU, 2016). The criteria should be addressed from the early stage of the design, characterizing the architecture, and thus determining the user acceptance (ISO, 2017).

Achieving effective and privacy-aware means of authentication has been a long-recognized issue of biometric security (Cavoukian, 2013). While passwords are still dominant, current implementations exhibit a much greater diversity of architectures, particularly in relation to those used on mobile devices (Msgna et al., 2016). Nowadays, secret-based schemes that combine PIN codes and biometrics are widely implemented in electronic financial applications, achieving great public acceptance (Bertino, 2016). This paper addresses the very recent privacy regulations for biometric data and the advances in the field of cryptography for secure biometric designs. We define the terms of privacy and security for biometric designs and discuss the current legal

Toli, C-A. and Preneel, B.
Privacy-preserving Biometric Authentication Model for e-Finance Applications.
DOI: 10.5220/0006611303530360
In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, pages 353-360
ISBN: 978-989-758-282-0

framework. Additionally, we analyze the security measures and privacy-preserving cryptographic techniques found in the literature. Finally, due to the rapid deployment of biometric-based access control systems for electronic financial and payment purposes, we introduce a privacy-preserving biometric authentication model for e-Finance applications.

Our **contribution** is as follows:

- We analyze the advantages and limitations of privacy-preserving cryptographic techniques according to the current privacy principles for biometric information protection (ISO, 2011) and the new security recommendations of the European General Data Protection Regulation (EU, 2016).
- We present a biometric authentication model for e-Finance applications, based on the privacy-preserving cryptographic technique of pseudonymous biometric identities.
- We evaluate our proposal following the security framework for financial services (ISO, 2008). We discuss how the privacy requirements, presented in (ISO, 2016) can be satisfied during the technical implementation.

This work is the first to introduce a privacy-preserving e-Finance model, based on the findings of biometric development projects funded by the European Union, such as Turbine (Turbine, 2011) and Fidelity (Fidelity, 2015).

2 DEFINITIONS

2.1 Privacy

In the age of the Internet of Things, the growing utility of biometric technologies in cloud applications has enabled the aggregation of personal data from multiple sources (Bertino, 2016). This has resulted in a constant criticism, influencing negatively the public opinion (Mordini and Tzovaras, 2012). Users are skeptical, especially when they cannot prevent the biometric registration in an access control scheme. For instance, government designs, such as border control systems that demand the collection of biometric data without the permission of their users (Mordini and Tzovaras, 2012). This information can be gathered and shared for ambiguous and unintended purposes, without any official approval (Kindt, 2009). It is a common belief that even when a procedure is performed by a legislative authority, the collection of such a personal data unjustifiably violates the human rights (Campisi, 2013). Privacy for biometrics is a basic user's right in a society where anonymity is considered as an inalienable privilege (Mordini and Tzovaras, 2012). Thus, during the last decade, there is an accelerated pace of regulations development for the legal transmission of biometric data in government and industrial schemes (Cavoukian, 2013). Through legislation, European and International organizations emphasize the importance of privacy for biometric systems (Podio, 2011). These activities are analytically discussed in Section 3.

2.2 Security

The concept of security for biometric architectures refers to the technical characteristics of the system and it is related to its overall robustness (Campisi, 2013). The protection mechanisms are classified based on the vulnerable points, where direct and indirect attacks in a biometric recognition scheme may occur (Ratha et al., 2001). After 2001, complete collections of targeted attacks and possible security measures have been presented (Martinez-Diaz et al., 2011; Ngo et al., 2015; Toli and Preneel, 2015). Although the legislation to protect biometric data has been strengthened, the current legal regime is believed to be insufficient to preserve privacy (Mordini and Tzovaras, 2012). As a supplementary response to that call, cryptographic techniques have managed to decrease the security limitations of biometric schemes through biometric template protection mechanisms (Podio, 2011). Architectures that are more complex based on the combinations of multibiometrics and passwords or tokens have been introduced, while extra attention has been paid to anti-spoofing countermeasures (Rebera et al., 2014). A privacy-by-design approach that combines cryptography and respects the privacy principles is considered to be the optimal option for enhancing both security and user's privacy in biometric schemes (Kindt, 2009). Sections 4 and 5 present the most recent privacy-preserving cryptographic tools.

3 PRIVACY PRINCIPLES AND SECURITY REGULATIONS

For every given technology, international and national standards establish the criteria for the configuration of a process, tool or system (Kindt, 2009). In this way, the applicability is resolved according to the requirements that define the security for user's personal data. To such a degree, a common toolkit specifies the privacy metrics to avoid any misunderstanding among developers and users. For biometric designs, standards specify the formats for the interchange of private data, the platform independence, program interfaces, application profiles, calculations and tests for the results (Mordini and Tzovaras, 2012; Cavoukian, 2013). Hence, the architecture is neutral, without being in favor of any particular vendor or modality (EU, 2016; ISO, 2017).

In terms of security, standards set the general guidelines for systems, tokens, smart cards, authentication employments, ID management designs and cyber-security architectures (Bertino, 2016). In the context of privacy for biometric data, they define the principles of *limitation*, *minimization*, *accuracy*, *completeness*, *transparency* and *rectification* that regulate the process of personal data and provide suitable formats for the development of the procedures (ISO, 2017). The security requirements of *confidentiality*, *integrity*, *authenticity*, *availability* and *non-repudiation* should be met for every system that is linked to the network (Ngo et al., 2015; ISO, 2017). Supplementary security recommendations for biometric applications report the properties of *anonymity*, *unobservability*, *revocability*, *cancelability*, *non-invertibility*, *unlinkability* and *discriminability* (Campisi, 2013). They referred mainly to the data transmission and distribution and the prohibitions towards the parties (ISO, 2011).

Recently, the term of *renewability* (ISO, 2017) has been added to the security recommendations for privacy-preserving biometric designs (EU, 2016). It is considered the most challenging regulation as it indicates the necessity of a user's re-enrollment in a system for updating his data. *Permanence* is also included in the new recommendations. It determines the validity period of the stored data, while it guarantees the uniqueness of an attribute. The new regulation is focused on the importance of privacy-by-design, underlining that as biometric technology matures, the interaction increases among users, markets, and the technology itself (EU, 2016).

4 LITERATURE REVIEW

In this section, we present the existing cryptographic approaches that have been proposed for enhancing the security of biometric designs and preserving privacy of user's sensitive data. The literature analyzes the privacy weaknesses in biometric schemes and suggests ways to secure the implementation process (Miltgen et al., 2013; Nandakumar and Jain, 2015; Adamovic et al., 2017). The approaches include: ***Template Protection Schemes***, ***Biometric Crypto-Systems*** and ***Pseudonymous Biometric Identities*** (Campisi, 2013). The first category includes ***Features Transformation Mechanisms*** and ***Cancelable Biometrics***.

4.1 Features Transformation

Biometric template protection as a term refers to the techniques where data is transformed to prevent a possible leakage (Ngo et al., 2015). The mechanism transforms the template data extracted from the freshly captured biometric before storing it. Thus, the template stored in the database is strongly protected with a goal that it would be almost impossible to retrieve the genuine biometric feature from the template (Campisi, 2013). In case of attacks, it is computationally hard for an intruder to find the function that was initially applied to the biometric data (Lim et al., 2015). Although the technique offers reliable security, a recent analysis concludes that complex transformations may reduce the performance (Nandakumar and Jain, 2015). The mechanism can be utilized in unibiometric and multibiometric templates. However, multibiometric designs demand more complex parameters and it is not possible to apply one-way functions with a high cryptographic security level. Consequently, it is very challenging to make this approach compliant with the privacy recommendations of *non-invertibility* and *discriminability*.

4.2 Cancelable Biometrics

Inducing the privacy recommendations of *cancelability* and *revocability* in biometric systems (ISO, 2017), being presented in Section 3, the purpose is the user's data protection, under a threat scenario, by composing quotation to biometric templates (Martinez-Diaz et al., 2011; Campisi, 2013). The method of cancelable or revocable biometrics is introduced as the first privacy-preserving mechanism for biometric schemes that respects these privacy properties for biometric information (Ratha et al., 2001). The mechanism allows multiple transformed biometric templates, offering higher security levels. One of the basic objectives is the diversity that provides a larger number of protected templates from the same features and it prevents the use of the same references across the variety of applications. The recommendations of *non-invertibility* and *revocability* are covered, since this approach demands the re-issuance of biometrics after an attack (Kaur and Khanna, 2016). However, the privacy recommendation of *renewability* introduced in (EU, 2016) is not preserved. Human characteristics may change during time or due to other interferences, such as an injury. In this scenario, the biometric scheme presents high false rejection rates/FRR and system's performance is decreased, being vulnerable to intruders (Msgna et al., 2016).

4.3 Biometric Crypto-systems

Biometric crypto-systems or shortly crypto-biometrics belong to the second category of privacy preserving techniques for the protection of biometric data. They combine cryptographic encryption and decryption functions to derive keys from biometric data (Campisi, 2013). Mainly, there are two schemes that named after their role as key-generation and key-binding schemes (Adamovic et al., 2017). For the first group of the classification, biometric feature directly creates the generated keys and their products are shared to the involved entities to secure all the communication pipelines and tunnels. Key-binding approaches allow only the storage of information coming from the combination of biometric data with randomly generated keys. In this case, the keys are non-biometric elements such as a PIN, password or credential with certified container of attributes. Both schemes are fuzzy, since the demanded samples are slightly different each time, unlike the encryption keys in the traditional cryptography (Ngo et al., 2015). Crypto-biometrics are currently a popular technique, being one of the most suitable fields for applications that demand large-scale databases for the storage of biometric information and high robustness against multiple attacks, such as government or banking services (Li and Jain, 2015). It is a privacy-aware cryptographic method that respects the privacy recommendation of *unlinkability*. It can be used in access control mechanisms with high *complexity* (Riccio et al., 2016). However, this can affect the *flexibility* of the technique. Recent works report that its applicability is ineffective for anonymous database models (Adamovic et al., 2017).

5 BACKGROUND

5.1 Pseudonymous Biometric Identities

Pseudonymous identities from biometric samples are the newest interface in the domain of privacy-preserving cryptographic approaches for biometrics (Breebaart et al., 2008). Figure 1 presents the complete architecture of renewable pseudo-identities in a typical biometric application (Delvaux et al., 2008). The mechanism utilizes non-invertible functions, to create pseudo-identities based on the references of biometric data. After the user's registration, the created pseudo-identity is securely stored. After the authentication procedure, the pseudo-identity expires while for a second recognition, the scheme can create a new pseudo-identity. For higher levels of security, the scheme requires the presence of a password or credential that are used as supplementary data.

During the enrollment phase, a biometric device captures the biometric templates from user's fresh features, while the user provides a password. Subsequently, an encoder generates the pseudo-identity and creates additional helper non-biometric data, using as an input only the user's supplementary data. The initial biometric information and supplementary data is destroyed. The design involves the parameters for the separation and individualization of the elements, preventing impersonation, bringing obstacles for users that have very similar characteristics (Li and Jain, 2015). Helper data and pseudo-identity references are securely stored as different templates in an encrypted domain, such as a database, card or token.

The authentication process is divided in two dif-

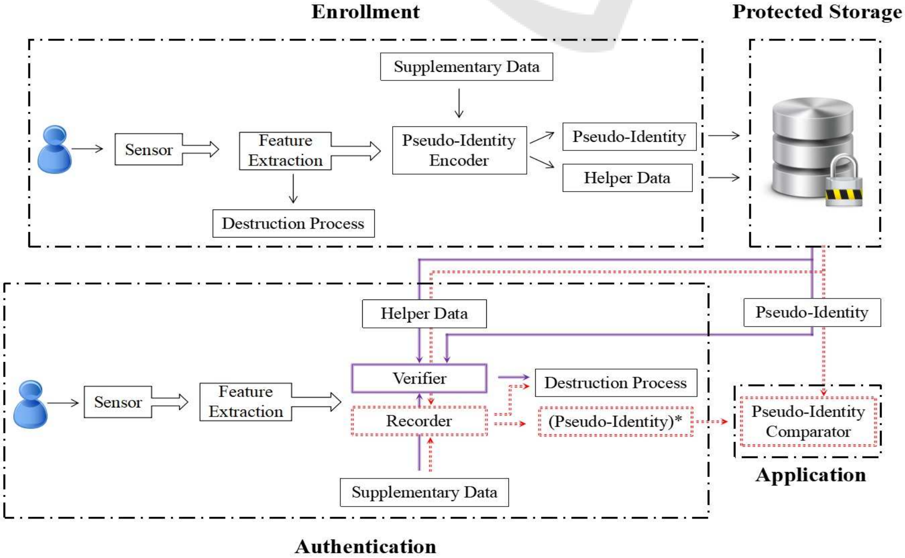

Figure 1: Architecture for renewable biometric pseudo-identities.

Table 1: Privacy-preserving cryptographic approaches.

Technique	Advantages	Disadvantages
Features Transformation	• Applicability to multibiometric designs • Meets privacy principles (ISO, 2011)	• Complexity affects performance • Non-preserved non-invertibility • Non-satisfied discriminability
Cancelable Biometrics	• High flexibility and interoperability • Meets privacy principles (ISO, 2011) • Offers non-invertibility • Offers cancelability and revocability	• Renewability affects performance • Non-satisfied discriminability • Non-preserved anonymity
Crypto-Biometrics	• High security and flexibility • Meets privacy principles (ISO, 2011) • Offers non-invertibility and renewability • Offers confidentiality and unlinkability	• Complexity affects flexibility • Non-satisfied interoperability • Non-preserved anonymity
Pseudo-Identities	• High security and flexibility • Meets privacy principles (ISO, 2011) • Meets properties (EU, 2016) • Offers cancelability and revocability • Offers renewability and unlinkability • Satisfies confidentiality and anonymity	• Minimization affects flexibility • Interoperability is under evaluation

ferent approaches (Breebaart et al., 2008). The scheme can proceed to a direct and simple verification of the pseudo-identity. The user presents his biometrics at the system's sensors and provides the password that was presented during the enrollment phase. Given the stored templates of the helper data and the pseudo-identity, a verifier provides and communicates the decision result to the application's parties. After a successful authentication, user's fresh biometrics and the password are destroyed. According to the second authentication method, the new captured biometric features, the supplementary data and the template of the helper data are provided to a pseudo-identity recoder, allowing the generation of a new (pseudo-identity)*. It follows the destruction process for the biometric and supplementary data, while the new pseudo-identity is provided to the application's comparator. The authentication decision is determined by the comparison of the new created (pseudo-identity)* with the template of the stored pseudo-identity.

The technique can combine passwords and biometric data, presenting high levels of security (Delvaux et al., 2008). It preserves the privacy principles of (ISO, 2011), while it also respects the properties in (EU, 2016). The embedded one-way functions are subject to the recommendation of *non-invertibility*. The mechanism offers individualized comparison parameters to optimize the performance, offering *renewability*, *cancelability* and *revocability*. It allows the creation and communication of multiple pseudo-identities for the same user in several non-local architectures, for instance cloud-based designs that demand high *flexibility*. The security requirements of *confidentiality* and *anonymity* are satisfied. Hence, it overcomes the limitations of the other mechanisms (Ngo et al., 2015). However, the recommendations of *interoperability* and *integrity* are evaluated for different threat scenarios. The integration of minimal data as a user's input, such as minutiae fingerprints is examined, testing the overall accuracy of the implementation in realistic use cases. Table 1 compares and summarizes the presented approaches.

6 PRIVACY-PRESERVING AUTHENTICATION MODEL

In this section, we introduce an authentication model based on the privacy-preserving cryptographic mechanism of pseudo-identities. Due to their advantages and high security results, the pseudo-identities are the ideal technique for our model that is specially designed for e-Finance applications. Following the legal framework for privacy and security in services of the financial sector (ISO, 2008), we present the practical issues in technically addressing the privacy principles and security regulations introduced in (ISO, 2011; ISO, 2016; EU, 2016).

6.1 Related Work

Literature offers a variety of proposals for secure biometric authentication in mobile devices (Msgna et al., 2016). Moreover, privacy-preserving approaches that combine passwords and biometrics in electronic financial architectures, present reliable security levels (Breebaart et al., 2011; Mrdaković and Adamović,

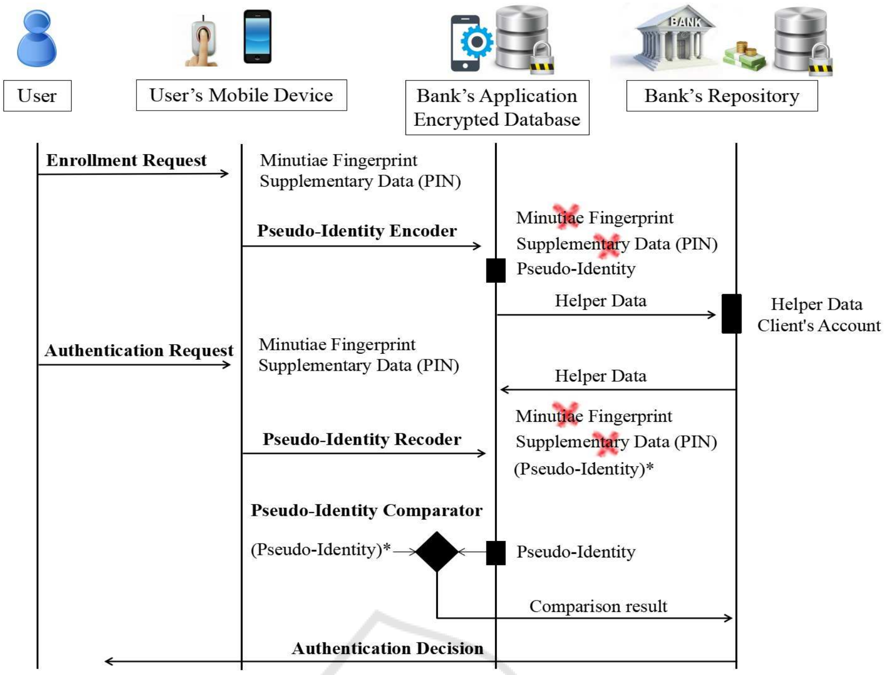

Figure 2: Biometric pseudo-identities model in an e-Finance application.

2015). The cryptographic technique of pseudonymous biometric identities is characterized as the optimum mechanism for commercial applications (Delvaux et al., 2008; Breebaart et al., 2008). In terms of security and privacy, although its promising results, state-of-the-art offers only theoretical works that lack of applicability (Gafurov et al., 2013). We exploit and analyze the mechanism in an e-Finance service scenario.

6.2 Scenario, Parties and Roles

Figure 2 presents the registration and authentication processes. For higher levels of security, our model utilizes the second approach of authentication that involves a pseudo-identity recoder as it is presented in Section 5. The design involves a user, a bank and the user's mobile device with an embedded fingerprint sensor. The bank, through the application running on the device controlled by the user, offers to the clients the service of the online financial checking. The user creates an electronic bank account and gains the e-Finance service access.

The architecture of pseudo-identities presents a classification of systems according to the choices for storage and comparison (Breebaart et al., 2008). The models for cloud-based applications are more accurate when they distribute the templates of comparison, according to the evaluation introduced in (Turbine, 2011). We select this approach in order to reduce the parameter of tampering attacks and prevent a malicious user from registering, using another person's name and getting access to his account. The signal processing subsystems of the pseudo-identity encoder and recoder are local. Our model stores the information distributed on user's mobile device and on server. The results are transmitted through decision subsystems, while bank's application handles the comparison procedures that take place on server.

6.3 Registration and Authentication

For the user's enrollment procedure, the client utilizes the bank's application, requesting the creation of his account. The biometric sensors capture and extract minimal minutiae data of his fingerprint, while the application demands the presence of a PIN code that is used as supplementary data. The device's encoder uses this information to generate the pseudo-identity and create additional helper non-biometric data, using as an input only client's PIN code. The pseudo-identity is encrypted and locally stored at the device, the helper data template is securely transmitted at the bank. It is stored and associated with the client's account information. Biometrics and PIN code are erased.

During the authentication, the client requests access at his account, using the bank's application and presenting his fingerprints and the PIN code. For the comparison procedure, the bank securely transmits to the bank's application the encrypted helper data for the given user's PIN code. The decision is not determined only by the helper data, since the subsystem of a pseudo-identity recoder creates a new (pseudo-identity)* based on the new biometric features that the client presents. At this phase, there is no storage of private biometrics and their related references. The pseudo-identity comparator of the bank's application communicates to the bank the result of the comparison between the new created (pseudo-identity)* and the initial stored pseudo-identity, while PIN code and biometric minimal data is destroyed. The authentication decision is provided to the client.

6.4 Security and Privacy Requirements

The **security requirements** of *confidentiality*, *cancelability* and *revocability* (ISO, 2017) can be met through the utilization of the pseudo-identities approach. The new recommendation of *renewability* introduced in (EU, 2016) is also covered. According to the security regulations for financial services (ISO, 2008; ISO, 2016) the property of *permanence* is critical for privacy-aware schemes. Our model preserves the recommendation, since the pseudo-identities expire and can be re-created. Finally, our design is based on two levels of security, combining passwords and biometrics. Thus, it offers higher robustness, as this is suggested in (ISO, 2016)

The **privacy requirements** of *non-invertibility* and *unlinkability* (ISO, 2011) are preserved. It is noted that the term of *unlinkability* is not referred to the bank. This party is considered semi-honest, and the privacy regulations are related to the malicious third parties. In case of an attack, the pseudo-identities are canceled and the compromised templates become incompatible with the user's original ones, respecting client's privacy (Turbine, 2011). Though the one-way functions, the model prevents the use of biometric data for any other purpose than the one originally intended (ISO, 2008). In that way, further processing of additional data across applications and other databases is avoided. The original biometric feature cannot be recovered and the system offers *confidentiality* against access by an unauthorized intruder. For the online environment of the bank's application, it is challenging to study the implementation of minimal data for preserving *data minimization* and offer user's control over his data (ISO, 2016).

7 CONCLUSION

Biometric authentication for e-Finance and e-Payment purposes gains ground globally, increasing the privacy concerns in financial sector. In the light of the foregoing critique, research on the field of cryptography for biometrics offers mechanisms that their practical implementation brings new privacy-enhanced designs. In this paper, we discussed the current security approaches and privacy practices that can offer protection of user's biometric information, respecting his privacy rights. We presented a privacy-preserving biometric authentication model for e-Finance applications, based on the recent cryptographic technique of pseudonymous biometric identities. In compliance with the data protection regulations, we discussed the ways that privacy can be addressed and how the security requirements could be satisfied during the design process. Authors' future direction is the design of the protocols and the technical implementation of the model. The proposed approach can lead to the toolkits for secure and privacy-aware identity management in financial services.

ACKNOWLEDGEMENTS

This work was supported in part by the Research Council KU Leuven: C16/15/058. Authors would like to thank, for his ideas on this research, Professor Arun Ross of the Department of Computer Science and Engineering, Michigan State University. The comments of anonymous reviewers are gratefully acknowledged.

REFERENCES

Adamovic, S., Milosavljevic, M. M., Veinovic, M. D., Sarac, M., and Jevremovic, A. (2017). Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics. *IET Biometrics*, 6(2):89–96.

Bertino, E. (2016). Data security and privacy in the IoT. In *Proceedings of the 19th International Conference on Extending Database Technology, EDBT, Bordeaux, France, March, 2016, Bordeaux, France.*, pages 1–3.

Breebaart, J., Buhan, I., de Groot, K., and Kelkboom, E. (2011). Evaluation of a template protection approach to integrate fingerprint biometrics in a pin-based payment infrastructure. *Electronic Commerce Research and Applications*, 10(6):605–614.

Breebaart, J., Busch, C., Grave, J., and Kindt, E. (2008). A reference architecture for biometric template protection based on pseudo-identities. In *BIOSIG 2008 - Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, September 2008 in Darmstadt, Germany*, pages 25–38.

Campisi, P., editor (2013). *Security and Privacy in Biometrics*. Springer.

Cavoukian, A. (2013). *Privacy-by-Design*: Leadership, methods, and results. In *European Data Protection: Coming of Age*, pages 175–202.

Delvaux, N., Chabanne, H., Bringer, J., Kindarji, B., Lindeberg, P., Midgren, J., Breebaart, J., Akkermans, T. H., van der Veen, M., Veldhuis, R. N. J., Kindt, E., Simoens, K., Busch, C., Bours, P., Gafurov, D., Yang, B., Stern, J., Rust, C., Cucinelli, B., and Skepastianos, D. (2008). Pseudo-identities based on fingerprint characteristics. In *4th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2008), Harbin, China, August 2008, Proceedings*, pages 1063–1068.

di Vimercati, S. D. C., Foresti, S., Livraga, G., Paraboschi, S., and Samarati, P. (2015). Privacy in pervasive systems: Social and legal aspects and technical solutions. In *Data Management in Pervasive Systems*, pages 43–65.

EU (2016). European General Data Protection Regulation 2016/679, http://eur-lex.europa.eu/homepage.html.

Fidelity (2015). European Project Fidelity, http://fidelity-project.eu/.

Furnell, S. (2015). From passwords to biometrics - in pursuit of a panacea. In *ICISSP 2015 - Proceedings of the 1st International Conference on Information Systems Security and Privacy, ESEO, Angers, Loire Valley, France, February, 2015.*, pages IS–7.

Gafurov, D., Bours, P., Yang, B., and Busch, C. (2013). Independent performance evaluation of pseudonymous identifier fingerprint verification algorithms. In *Image Analysis and Recognition - 10th International Conference, ICIAR 2013, Póvoa do Varzim, Portugal, June, 2013. Proceedings*, pages 63–71.

ISO (2008). ISO/IEC 19092/2008, Financial Services – Biometrics – Security Framework.

ISO (2011). ISO/IEC 24745/2011, Information Technology - Security Techniques - Biometric Information Protection.

ISO (2016). ISO 13491-1:2016, Financial Services – Secure Cryptographic Devices – Part 1: Concepts, Requirements and Evaluation Methods.

ISO (2017). ISO/IEC 2382-37/2017, Information Technology - Vocabulary - Part 37: Biometrics.

Kaur, H. and Khanna, P. (2016). Biometric template protection using cancelable biometrics and visual cryptography techniques. *Multimedia Tools Appl.*, 75(23):16333–16361.

Kindt, E. (2009). The use of privacy enhancing technologies for biometric systems analysed from a legal perspective. In *Privacy and Identity Management for Life - 5th IFIP WG 9.2, 9.6/11.4, 11.6, 11.7/PrimeLife International Summer School, Nice, France, September, 2009, Revised Selected Papers*, pages 134–145.

Li, S. Z. and Jain, A. K., editors (2015). *Encyclopedia of Biometrics, Second Edition*. Springer US.

Lim, M., Teoh, A. B. J., and Kim, J. (2015). Biometric feature-type transformation: Making templates compatible for secret protection. *IEEE Signal Process. Mag.*, 32(5):77–87.

Martinez-Diaz, M., Fiérrez, J., Galbally, J., and Ortega-Garcia, J. (2011). An evaluation of indirect attacks and countermeasures in fingerprint verification systems. *Pattern Recognition Letters*, 32(12):1643–1651.

Miltgen, C. L., Popovic, A., and Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "big 3" of technology acceptance with privacy context. *Decision Support Systems*, 56:103–114.

Mordini, E. and Tzovaras, D. (2012). *Second generation biometrics: The ethical, legal and social context*, volume 11. Springer Netherlands.

Mrdaković, M. and Adamović, S. (2015). Privacy friendly biometrics. In *Proceedings of Synthesis 2015 - International Scientific Conference of IT and Business-Related Research, Belgrade, Singidunum University, Serbia,*, pages 67–70.

Msgna, M. G., Ferradi, H., Akram, R. N., and Markantonakis, K. (2016). Secure application execution in mobile devices. In *The New Codebreakers - Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*, pages 417–438.

Nandakumar, K. and Jain, A. K. (2015). Biometric template protection: Bridging the performance gap between theory and practice. *IEEE Signal Process. Mag.*, 32(5):88–100.

Ngo, D., Teoh, A., and Hu, J. (2015). *Biometric security*. Cambridge Scholars, Newcastle upon Tyne.

Podio, F. L. (2011). Biometric technologies and security - international biometric standards development activities. In *Encyclopedia of Cryptography and Security, 2nd Ed.*, pages 124–130.

Prabhakar, S., Pankanti, S., and Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, 1(2):33–42.

Ratha, N. K., Connell, J. H., and Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634.

Rebera, A. P., Bonfanti, M. E., and Venier, S. (2014). Societal and ethical implications of anti-spoofing technologies in biometrics. *Science and Engineering Ethics*, 20(1):155–169.

Riccio, D., Galdi, C., and Manzo, R. (2016). Biometric/cryptographic keys binding based on function minimization. In *12th International Conference on Signal-Image Technology & Internet-Based Systems, Naples, Italy, December, 2016*, pages 144–150.

Toli, C. and Preneel, B. (2015). Provoking security: Spoofing attacks against crypto-biometric systems. In *2015 World Congress on Internet Security WorldCIS, Dublin, Ireland, October, 2015*, pages 67–72.

Turbine (2011). European Project Turbine: TrUsted Revocable Biometric IdeNtitiEs, http://cordis.europa.eu/project/rcn/85447.html.