Kişisel Verileri Koruma Dergisi
www.kvkk.gov.tr
Cilt: 1, Sayı: 1
Geliş: 10.05.2019
Kabul: 28.05.2019

A review on privacy preserving biometric authentication methods

Cengiz Paşaoğlu
Kişisel Verileri Koruma Kurumu,Ankara, Türkiye, cengizpasaoglu@kvkk.gov.tr
ORCID: orcid.org/ 0000-0002-4583-5461

Kayode Hadilou Adje
Gazi Üniversitesi, Mühendislik Fakültesi,Bilgisayar Mühendisliği Bölümü Ankara, Türkiye, kayodehadilou.adje@gmail.com
ORCID: orcid.org/ 0000-0002-7263-8498

Orkun Demirtaş
Gazi Üniversitesi, Mühendislik Fakültesi,Bilgisayar Mühendisliği Bölümü Ankara, Türkiye, orkundemirtas15@gmail.com
ORCID: orcid.org/ 0000-0001-8897-5096

ABSTRACT
By the exponential growth of smart services and technologies, the authentication issue has become more challenging. Recently, biometrics authentication methods have become quite popular due to the range of advantages they provide compared to classic authentication systems. Biometrics authentication methods have the ability to authenticate users, nevertheless that feature comes with its privacy risks. Users' privacy should be protected in every step of biometrics authentication. This article briefly presents privacy threats and challenges in biometrics systems and identifies some existing privacy-preserving authentication methods and regulations.
Keywords: Privacy-preserving biometric authentication, Personal data protection, Biometric data privacy risks,

Mahremiyet korumalı biyometrik kimlik doğrulama yöntemleri üzerine inceleme

ÖZ
Akıllı servislerin ve teknolojilerin katlanarak büyümesiyle birlikte, kimlik doğrulama önemli bir sorun haline gelmiştir. Biyometrik kimlik doğrulama yöntemleri, klasik kimlik doğrulama yöntemlerine kıyasla sağladıkları çeşitli avantajlar nedeniyle günümüzde oldukça popüler hale gelmiştir. Biyometrik kimlik doğrulama yöntemleri kullanıcıların sahip olduğu benzersiz biyometrik bilgiler ile kimlik doğrulama yeteneğine sahiptir. Bu durum mahremiyet problemlerine yol açabilir. Kullanıcıların mahremiyeti, biyometrik kimliğin doğrulamasının her aşamasında korunmalıdır. Bu araştırma makalesi, biyometrik sistemlerdeki mahremiyet tehditlerini, bunun sağlanması aşamasındaki zorlukları ve mahremiyetin korunmasına yönelik kimlik doğrulama yöntemleri ile mevcut hukuki düzenlemeleri içermektedir.
Anahtar Sözcükler: Mahremiyet-korumalı biyometrik kimlik doğrulama, Kişisel veri koruma, Biyometrik veri mahremiyet riskleri,

Atıf Gösterme Paşaoğlu, C., Adje, K., D., & Demirtaş, O., (2019). A review on privacy preserving biometric authentication methods, *Kişisel Verileri Koruma Dergisi*. *1*(1), 34-46.

INTRODUCTION

Today more people use smart services and technologies in their daily lives than ever before. The number of smart devices and the quantity of digital content created by these devices continue to grow exponentially. Therefore, together with this development, comes some challenges such as the authentication issue while securing the transactions with smart technologies.

Authentication is an important phase in securing systems, hence any fault in authentication could lead to several and unrepairable damages. Mobiles and web applications mostly use passwords to block access to unknown users or activities, other techniques including cryptographies, sophisticated methods and biometrics are also used to authenticate users and make systems and transactions more secure. While biometrics authentication methods present more advantages than classic methods, they are vulnerable to attacks that can lead to a leak of important information considered as private and personal data.

A stolen or hacked biometric data can be used as tool for theft, individual profiling, tracking or cross matching in different databases. A stolen or hacked biometric data can also be used to determine one's sensitive data such as ethnic group, religious orientation, political opinion, medical diseases or to perform illegal activities (Pagnin & Mitrokotsa, 2017). It is therefore clear that there is a need for privacy-preserving biometrics authentication systems. Privacy-preserving biometrics authentication systems are biometrics authentication systems that can overcome privacy risks mentioned above.

In the first section of this article, biometrics authentication methods are defined, then the main privacy threats that can be performed against users are presented in the second section. In the third section, technical challenges and existing privacy-preserving biometrics authentication methods are presented. In the last section of the article, Turkish Law on the Data Protection of Personal Data and General Data Protection Regulation about privacy in biometrics are reviewed and discussed.

DEFINITIONS

Biometric (or Biometry) is a method that allows a person to be recognized based on his physiological and / or behavioral characteristics. Biometric is a combination of two words: "*bio*" in Latin meaning "*life*" and "*metric*". As its name suggests, it is a technology that measures vital characteristics such are face shape, retinal, iris, vein, fingerprint, hand geometry and voice. These features linked to the DNA makes each person different.

Biometric and Biometric Systems

Biometric technologies provide safe identification and personal verification solutions in many systems. Biometric system is a model recognition system that allows the recognition of a person based on a derived feature vector.

In general, biometric systems have two functions: validation function and identification function. In the identification, the system compares the characteristic data with the previously captured biometric characteristics. The identification function finds out whom the property belongs to; for example, in a system with fingerprint access, first, the fingerprints of the subjects are recorded in the database. Then, when logging into the system, biometric system takes the current fingerprints and compares it to the rest of fingerprints in the database. If there is a match, the defining function occurs. If it belongs to a

user, the system determines the access rights that the user can perform on the system. Under a verification system, an individual presents himself or herself as a specific person. The system checks his or her biometric against a biometric profile that already exists in the database linked to that person's file in order to find a match. Verification is sometimes referred to as 1-1 identification.

Biometric Modalities

The data received in biometric authentication system must have the following biometric characteristics: universality, diversity, persistence, summability, acceptability, infiltration /extensibility (Kindt, 2013). There are two types of biometrics data: physical and behavioral aspects.

Physical Biometric

Physical biometric data includes fingerprint, face shape, hand geometry, iris and voice speech. These main examples are defined as follows;

Fingerprint: in terms of universality fingerprint can be taken as a characteristic (Kindt, 2013). The quality, difference and usage performances are high. Its ability to be recorded is ideal even if the face is lower than hand geometry. The ability of a malicious person to circumvent a system using fingerprints is very low (Jin, Ling & Goh, 2004).

Face Shape: the entire face shape is considered to be a single characteristic. Its diversity is low and its permanence is ideal (Kindt, 2013). The situations cannot provide a high persistence because the effect on face shape (age, external factors etc.) is higher than other biometric data. However, it is possible to have results closed to the match. The facial shape is highly recordable. The performance is also low because of the low difference.

Hand Geometry: wear in the hand can be taken as a separate characteristic feature within the framework of universality **(**Kindt, 2013). In general, other features are also ideal for matching in the biometric system.

Iris: visual impairment can be taken as a distinct characteristic. The iris analysis of the eye tissue is carried out according to the visible properties surrounding the pupils (Kindt, 2013). Although it has a high level of permanence, it is not suitable to use in systems. It needs high-level technological requirements. In general, iris based biometric authentication methods are considered as the safest.

Voice Speech: disorder can be taken as a separate characteristic within the framework of universality. The difference and permanence are low, so the performance is also low (Kindt, 2013).

Behavioral Biometrics

Unlike physical biometrics that relies on physical aspect of biometrics to authenticate users, behavioral biometrics is based on the measurement of human behavioral patterns for authentication. Behavioral biometry with the help of adequate smart sensors measure behavioral patterns observed in almost every activity: rather than the activity itself, it captures how users perform the activity, how users interact with a device or machine. The way of driving or walking (gait) of the individual, the way of using smart devices, its interactions with computer equipment, etc. are few examples of behavioral biometrics (Yampolskiy & Govindaraju, 2009).

Behavioral patterns captured are composed of distinctive attributes called semi-behaviors. These behaviors include the daily habits and micro habits of the individual, as well as speech and writing. When viewed from the outside, it may be thought that everyone drives or walks in the same way. But in fact, even though individuals may not distinguish them, these differences can be measured with smart sensors and analyzed using appropriate algorithms in order to reveal each user's unique profile. Patterns in behavioral biometrics are determined by many factors: physiological, social, phycological, etc. or health related factors (Internatiomal Biometrics+Identity Association, n.d.). This make it almost impossible or extremely difficult to get the same behavioral biometric for different people making authentication through behavioral biometrics more accurate than with physical biometrics.

Behavioral biometrics technologies are now used in applications such as finance, criminal profiling, cybercrime investigation, fraud/threat detection, e-commerce, text authorship etc. and sometime in addition to existing physical biometry to further increase safety. Some examples of behavioral biometrics are: audit logs, biometric sketch, blinking, call-stack, calling behavior, car driving style, command line lexicon, credit card use, dynamical facial features, e-mail behavior, gait/stride, game strategy, handgrip, haptic, keystroke dynamics, lip movement, mouse dynamics etc. (Yampolskiy & Govindaraju, 2009).

Behavioral biometrics systems collect user's data in a continuous way instead of at a single point. This means even if the systems failed to properly gather data at a point, it will still be able to achieve high performance over time: behavioral biometrics is said to eliminate the risk of a single point failure. From a privacy point of view, behavioral biometrics is more privacy-friendly than physical biometrics. Behavioral patterns collected from human activities are free from personally identifiable information that can be used to directly identify an individual (Internatiomal Biometrics+Identity Association, n.d.). For example, with behavioral biometrics there is no need for user's fingerprint but instead the system collects user's gait and compares it to the patterns in its database, if the score is above a predetermined threshold, access is granted. The system only has to know if the current behavior is the one stored in its database, no more.

Sensitive Data Access Methods

There are two ways to access sensitive data in order to protect the privacy of the individual. The two have different properties;

Positive Recognition: a biometric identification system requires that the subject identify himself when presenting the data. The data sent is compared to other data saved in the system. This definition is also assumed to be below the registered ID if the sent dimension is close enough to match (Jain, Ross & Prabhakar, 2004). Non-biometric systems can also make unauthorized access to the stored biometric data by cyber-attack techniques, but biometric systems are much more reliable, because 9 out of the 10 trials fail to match. Positive identification can be made voluntary.

Negative Recognition: in the negative definition, sensitive personal data (age, citizenship and so on) is not required to be connected to another external record. Negative identification applications cannot be voluntary (Jain et al, 2004). For instance, assume a crime occurred and there is a fingerprint left in the scene place. When using the match to find the criminal, if the police do not save the biometric data in a database, the fingerprint data used for that operation is an example of a negative definition.

PRIVACY THREATS IN BIOMETRICS

Biometrics has many seductive usage scenarios: from controlling houses with voiceprint, opening doors with iris, to using faces and fingerprints to unlock mobile phones. In order to be useful, biometrics data are stored either in remote or local database (generally large database) to identify or verify the same subject in the future. If compromised, identification and verification methods used in biometrics present some threats and risks in term of user's privacy.

Raw biometrics data including face pictures, fingerprint patterns, and voice patterns can reveal top sensitive data such as one's health conditions, racial and ethnic origin, political opinions, religious or physiological belief which are considered as sensitive personal data and should not be shared or processed beyond the agreement with the data subject (Pagnin & Mitrokotsa, 2017).

Some biometrics systems store a representation (template) instead of the raw biometric data itself to ensure users' privacy but many research techniques have shown that it is possible to reconstruct raw biometrics data from templates. For example, a template previously stored to authenticate users can be used to obtain fingerprint data (Cappelli, Maio, Lumini & Maltoni, 2007).

If stolen, stored and shared under unsecured conditions, biometrics data can be used without user's consent for secondary purposes. It is called "the function creep".

Since they are unique, biometrics data can be used as unique identifier for connecting different databases, which is called the linkage problem (Belguechi, Cherrier, Alimi, Lacharme & Rosenberger, 2011). This concern has become quite real as governments, such as UK, who has large scale central databases for passports and eID cards with mandatory biometrics characteristics. If compromised, these large-scale databases, including names, addresses of citizens etc. can be linked with the biometrics data and then not only the governments but also the private parties may have access to citizens' sensitive data.

With the evolution of data science, computational power and the availability of large amount of data, a leak of one biometric data can lead to find the other(s) one. For example (Ozkaya & Sagiroglu, 2010) developed a model to find face pattern from fingerprints. With many of these techniques, the leak of a biometric data will directly lead to the breach of the rest causing an important privacy threat.

Biometric data related to human characteristic can have some changes over time, so for instance face patterns can be changed and become inaccurate or incomplete. Therefore, another problem can arise, false identification. An individual can be identified as a different person and can have some unexpected problem because of false identification.

Biometric authentication systems are evaluated using metrics such as FAR and FRR (Bhattasali, Saeed, Chaki & Chaki, 2014). FAR stands for False Acceptance Rate or the percentage of authentication instances in which unauthorized persons are incorrectly accepted while FRR stands for False Rejection Rate or the percentage of authentication instances in which authorized persons are incorrectly rejected. In many biometrics systems, the best performance is achieved at the intersection between FAR and FRR curves (Bhattasali et al, 2014). Lowering FAR means allowing less identical pattern to match with the stored pattern by decreasing the number of rejected cases. If we consider the fact that biometric data of different individuals can be close to each other, which means less different person can authenticate him as another one, may open doors to all privacy risks that are associated.

ATTACK POINTS IN BIOMETRICS

Biometric authentication systems are more convenient to use. The person does not need to remember any password. It makes sense because the authentication system can be more useful and more secure.

However, this comes with a problem: biometric data is sensitive data and mostly cannot be changed in the lifecycle. If that data would be stolen, then it constitutes huge risks. This part of the article includes vulnerability attacks in biometrics.

There are eight attack points. These attack points are divided into two categories: Direct and Indirect Attacks. In the figure 1, different ways of attacking biometrics authentication systems are shown.

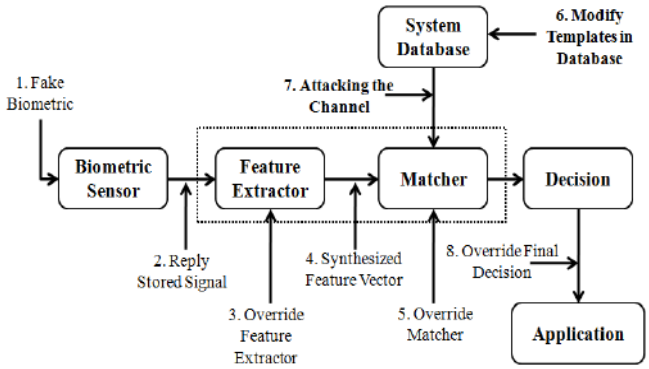

*Figure 1.*Attacks on Biometric Systems (Thanki, Dwivedi & Borisagar, 2018)

Direct Attacks

Direct attacks are also known as sensor attacks. The sensor is been attacked directly. For example, an attacker can use a fake identifier to attack a fingerprint sensor in order to identify himself. Attacking the sensor is the easiest way to attack because no specific knowledge about the system operation is needed and there is no digital protection for this. Sensors are unable to distinguish between fake and real characteristics of an individual and can be fooled easily by using synthetic fingerprints for example.

Indirect Attacks

Indirect attacks are brute force attacks and it includes the attacks forms 2,3,4,5,6,7 and 8 from figure 1. In these types of attacks, the attacker does not attack the physical environments; instead he attacks directly the modules using hacking techniques. Unlike direct attacks, indirect attacks are preventable.

Brute Force Attack: brute force attack depends on the rate of matching accuracy in the biometrics system. Attacker can create a wordlist to break a password. Because the content of the password is composed of characters, if the attacker is obsessed with the attack, he may access the system even if it takes months or years.

However, in biometric system, the change of capturing a biometric characteristic is very low due to the features that makes biometric data different for 7.6 billion people. A biometric system is used to produce or obtain a large number of samples so that the attacker can take over by brute-force attack.

The ability to produce a sample to break a biometric system is low compared to the other forms of indirect attacks (Fierrez & Galbally, 2015).

In normal encryption system, the attacker can create the wordlist by developing algorithm himself but it is not possible for a biometric system to create 10,000 characteristics if an algorithm of 0,001% accuracy is used with 10,000 users. Therefore, the attacker will need a biometric database as a wordlist.

Replay Attack: the attack point is known as "attack on the channel between the scanner and feature extractor". In a biometric system, a biometric data is scanned and sent to a feature extractor module for processing. In replay attack, the attacker attacks the channel between the scanner and the feature extractor to steal biometric data (Uludag & Jain, 2004).

This attack point is not the same as in brute force attack. In brute force, the attacker has biometric database and his purpose is hacking the system using this database. However, in this attack, the attacker steals the biometric data before it is saved. He steals it from the channel then he uses this data for his malicious purposes.

Trojan Attack: In this type of attack, the attacker attacks the feature extractor module with Trojan virus remotely. The attacker sends commands to his virus then controls the extraction module. Sensor sends data to feature extractor module to extract specific module for matcher module, so if attacker controls this module then he will be able to control the whole system (Uludag & Jain, 2004).

Replayed Attack in the Channel between Feature Extractor and Matcher: this attack looks similar to the second type of attack but the difference is the channel. The attacker attacks the channel between the feature extractor and the matcher. He intercepts this channel then steals the real biometrics (Uludag & Jain, 2004).

Attacks on Matcher : the attacker attacks the matcher module to generate the high matching score as selected by the imposter (Uludag & Jain, 2004).It means that, biometric data does not matter; he uses a wrong data to enter the system.

Attacks on Database: The attacker finds a security bug in the database, which is generally very difficult to do (Cappelli et al, 2007). Then, he hacks the database and steals some biometric data. After that, he can use this biometric to data enter the system or for other purposes.

Attack in the Channel between Database and Matcher: The attacker, attacks the channel between the database and matcher module. The purpose of these type of attacks is to erase valid records in database so that on the channel, the wrong data and data stored in the database can match.

Attack of the Decision Module: The attacker attacks the decision module for changing the system's decision. It means that wrong feature is extracted, scanner gets wrong data, and matcher did not find a valid matching in database, so decision module has to deny the access to the system.

PRIVACY ENHANCING BIOMETRIC METHODS

Safe identification and personal verification solutions can be provided in many systems with biometric technologies. However, the technology may have serious privacy implications, so it may lead to

serious threats to identity even more serious as defined in the previous sections. In this part of the article, privacy-preserving biometric authentication methods are reviewed.

De-Identification and Irreversible De-Identification

In biometric, de-identification is defined as the process of replacing biometric identifiers or removing biometric identifiers in order to prevent the capture of sensitive data (Nandakumar, Jain & Pankanti, 2007).

De-identification is one of the main approaches to privacy protection in biometric authentication systems, while permitting other uses of personal information. The terms de-identification and anonymization are synonyms, but some experts make the difference between them: de-identification refers to the reversible process of removing or obscuring any personally identifiable information from individual records. Irreversible De-Identification is as same as Anonymization. In biometric, anonymization (Irreversible De-Identification) involves the destruction of any connection or links between de-identified datasets and original datasets (Nandakumar et al, 2007). Therefore, after anonymization, it would be possible to reach or process the sensitive data.

The de-identification process is required to be of sufficient effectiveness, regardless of whether the recognition attempts are made by humans or by machines.

Cancelable Template

In common biometrics authentication systems, people are mostly afraid of having their biometrics traits stored in the system. Cancelable template solves such privacy issues by storing a distorted pattern of the biometric data instead of the original one. Cancelable template is a template protection method where the original template is intentionally distorted in a repeatable way in order to protect users' sensitive data (Pagnin & Mitrokotsa, 2017). If, for some reason, the original pattern is compromised, a new different distorted pattern can be generated by changing the distortion characteristics. By storing only the distorted pattern, the cancelable template protection mechanism results in enhancing users' privacy.

There are two types of cancelable templates: Biometric Salting and Non-Invertible Transforms, but all cancelable templates have four common properties (Takahashi & Hirata, 2011):

Diversity: Cancelable features across applications should be different. This requires generating a high number of protected templates from the same biometric pattern.

Reusability: If compromised, the revocation and reissue of a template based on the same biometric feature should be straightforward.

Non- Invertibility: Templates are non-invertible. This prevents the recovery of original biometric data.

Accuracy Performance: The formulation should not deteriorate the recognition performance.

Biometric Cryptosystem

The biometric cryptosystem approach used to store biometric data on the computer, benefits from auxiliary data to preserve the biometric data template. The auxiliary data used for encryption is called

key binding if it is independent of biometrics (e.g., only a mathematical function) and key generation or key extraction if it is derived from the biometric template. Biometric data is accepted as a digital image before any switching is performed. Then it is thinned to a smaller size and converted into binary image (Nandakumar et al, 2007). After these operations, switching is performed. This form of keys is much more advanced than an ordinary combination of encryption since the pattern obtained after switching is blurred (Zhang, Qin & Du, 2015). In the key extraction process, this turbidity can be solved due to the fact that the mathematical form to which it is transformed is known (Abidin & Mitrokotsa, 2014). The security phase differences between the normal biometric system and the biometric cryptosystem is shown in figure 2.

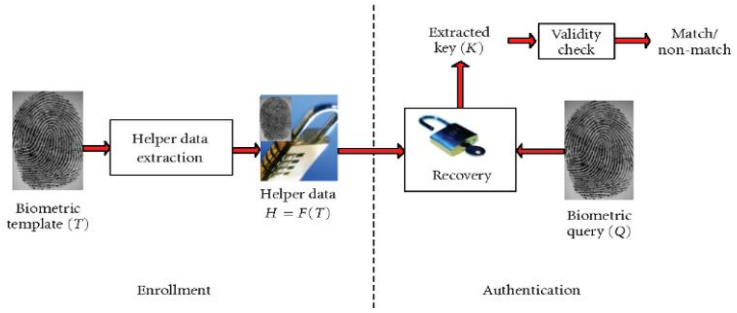

Figure 2. Biometric Cryptosystem (Jain, Nandakumar & Nagar)

Bio Hashing

Other than biometric cryptosystems structure, change based on methodologies appear to be increasingly suited to guarantee the cancelability and irreversibility for the most part, and satisfy the accuracy and cancellability. Bio-hashing is a two-factor validation approach which consolidates pseudo-arbitrary number with biometrics to produce a minimized code for each individual (Goh & Ngo, 2003).

All bio-hashing strategies share the normal standard of creating a unitary bio code from two information: the biometric one and an arbitrary number, which should be stored, called tokenized random number. The same scheme, detailed below, is applied.

During the enrolment phase, only the bio code is stored rather than the raw biometric data. At the confirmation phase, another bio code is created from the stored arbitrary number. At that point, the confirmation depends on the calculation of the "Hamming Distance" between the reference bio code and the recently issued one. The method allows bio code cancelability and diversity by utilizing diverse irregular numbers for various applications. The bio hashing procedure is shown in figure 3.

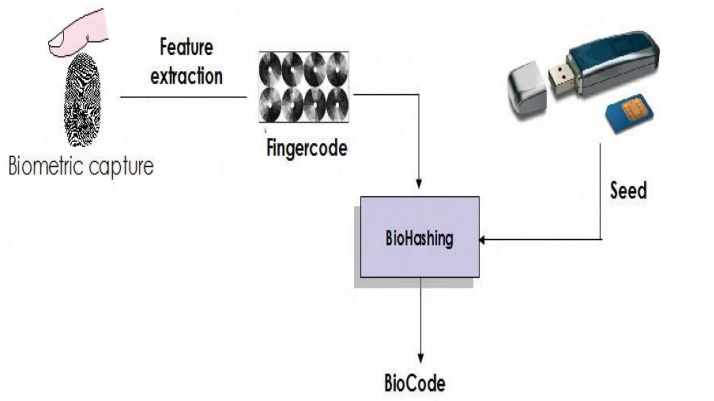

Figure 3: Bio Hashing (Ghammam, Barbier & Rosenberger, 2018)

Secure Storage Systems

A key point is related to the storage of biometrics data and its security: Is it saved locally with various dangers of access and abuse? The issue turns out to be increasingly significant when managing substantial scale biometric data, for example, the biometric national ID or biometric passport. For systems requiring high-level security and privacy preserving technics, secure elements can be used. A secure element is a microprocessor chip used in multiple systems and hardware to store sensitive data and run applications without any security or privacy risks (General Data Protection Regulation, 2018). It is predominantly utilized in smart cards or cell phones to host sensitive data and applications, for example, biometrics templates or payments applications. It allows a high state of security and trust.

PRIVACY-PRESERVING REGULATIONS IN BIOMETRICS

Privacy laws are the set of rules that regulates how personal data are collected, stored and used by government, private sector or any data controller. There exist many different privacy regulations and laws in different countries such as "The Personal Information Protection and Electronic Document Act" in Canada, "The Right to Privacy" in the Indian Constitution, the “General Data Protection Regulation (GDPR)” in European countries, “Turkish Law on the Protection of Personal Data” in Turkey etc. The most recent and complete privacy law is the GDPR. In this section, privacy preserving directives, regulations and laws in biometrics introduced in the GDPR and Turkish Law on the Protection of Personal Data are reviewed.

Law on the Protection of Personal Data

After a referendum Constitution of Republic of Turkey Article 20 amended in 2010 with new clause and give everyone right to request for protection of his/her personal data, which guarantees the privacy of individuals. In addition, National Grand Assembly of Turkey accepted a law to protect personal data, the Law No. 6698 on the Protection of Personal Data, became effective upon promulgation in the Official Gazette of 07.04.2016.

According to article 6 of the Law mentioned above, biometric data is deemed to be personal data of special categories which can also be mentioned as sensitive personal data and it is prohibited to process the personal data of special categories without the explicit consent of the data subject. Hence, there is an exception which is mentioned in the third paragraph of the sixth article, the special nature of personal data mentioned in the first paragraph except those relating to health and sexual life, can be processed without seeking explicit consent of the data subject, in the cases provided for by laws ("Kişisel Verilerin Korunması Kanunu").

In addition, adequate measures determined by the Personal Data Protection Board in January 2018 must be taken while processing the personal data of special nature including biometric data (Kişisel Verileri Koruma Kurumu, n.d.).

General Data Protection Regulation

The General Data Protection Regulation was introduced on 25 May 2018 and European Members States started to transpose it to their national law by 6 May 2018 (Vojkovic & Milenkovic, 2018).

With GDPR, the European Union sets down rules to protect people with regard to the usage of personal data and protect fundamental rights in particular the right to the protection of personal data.

GDPR is the first legislation ever that defines biometric data as personal data obtained by using features related to human physical, physiological characteristics, or characteristics of an individual's behavior, which provides the uniqueness property or confirm the unique identification of the individual, such as fingerprint, iris, and face shape. In clear, GDPR brings many novelties in terms of privacy in biometrics systems.

GDPR clearly defines the privacy rules in biometrics by its Article 9 entitled "Processing of special categories of personal data" (General Data Protection Regulation, 2018).

Moreover, according to the first paragraph of the Article 9, biometrics data requires higher and more sophisticated protection methods. Therefore, one can clearly understand that GDPR prohibits the processing of biometric data revealing one's sensitive information i.e biometrics data.

In the second paragraph details about the exceptions of processing sensitive personal data is mentioned. Which means paragraph one shall not apply if one of the following applies: data subject's explicit consent, necessity for legal obligations and rights by controller or data subject, necessity to protect data subject's life if he/her/it cannot give explicit consent, non-disclosing legitimate activities of organizations on members or former members on connection with the organization's purposes, public personal data database, courts judicial capacity, Union or Member State's public for scientific or statistical interests.

Compared to the Turkish Law on the Protection of Personal Data, GDPR is more detailed and clearer about preserving privacy in biometrics.

CONCLUSION

Biometric systems are used in diverse technologies requiring high-end security systems. By relying on users' unique biological or behavioral features, biometrics systems differentiate each individual to authenticate only allowed users and make technologies and devices that implement it more secure and reliable. Behavioral biometrics technologies should be preferred as they are more privacy-friendly, advances and researches in smart sensors and artificial intelligence algorithms could lead to more performant and privacy-preserving behavioral biometrics. As in other non-biometric authentication methods, attackers can develop tools or use illegal means to get access to users' personal data for malicious purposes. Privacy preserving biometrics authentication methods ensure that applications and systems make use of personal data without leaking them. To prevent privacy attacks in biometrics, many laws and regulation have been established in different countries and privacy preserving techniques and methods have been developed. The main motivation behind every privacy preserving biometrics authentication method is to design a tool that can guarantee privacy preservation while securing the system and allowing the use of personal data.

In addition since we are in the digital age, especially behavioral biometrics are becoming very important and assumed to be innovative and game changer technology in biometrics, such as keystore patterns, finger press, typing recognition, gait, signature etc. As for future study we are planning to make detailed research about behavioral biometric systems, possible vulnerabilities of these systems and attacks on the systems with the authentication problems. This will make it possible to see effects of emerging technological changes in the privacy preserving biometrics field. Moreover, legislation is keeping up with new technological developments. Thus, these innovative technologies such as behavioral biometrics will open a door to review existing data protection and privacy regulations and possibly push law makers to make some proper changes in the privacy laws.

REFERENCES

Abidin, A., Mitrokotsa, A. (2014). A Privacy-Preserving Biometric Authentication Protocol Revisited, *In Proceedings of YACC*, Porquerolles island, France.

Belguechi, R., Alimi, V., Cherrier, E., Lacharme, P., Rosenberger, C. (2011). An overview on privacy preserving biometrics. *Recent Application in Biometrics*,65-84.

Bhattasali, T., Saeed, K., Chaki, N., & Chaki, R. (2014). A Survey of Security and Privacy Issues for Biometrics Based Remote Authentication in Cloud. *Computer Information Systems And Industrial Management*, 112-121. doi: 10.1007/978-3-662-45237-0_12

Cappelli, R., Maio, D., Lumini, A., & Maltoni, D. (2007). Fingerprint Image Reconstruction from Standard Templates. *IEEE Transactions On Pattern Analysis And Machine Intelligence*, *29*(9), 1489-1503. doi: 10.1109/tpami.2007.1087

Fierrez, J., & Galbally, J. (2015). *Indirect Attacks on Biometric Systems*. Presentation, Biometric Recognition Group -ATVS, Universidad Autonoma de Madrid,Spain

General Data Protection Regulation (GDPR).(2018) Retrieved from https://gdpr-info.eu/

Ghammam, L., Barbier, M., & Rosenberger, C. (2018). Enhancing the Security of Transformation Based Biometric Template Protection Schemes. *2018 International Conference On Cyberworlds (CW)*,316-323.

Goh, A., & Ngo, D. (2003). Computation of Cryptographic Keys from Face Biometrics. *Communications And Multimedia Security. Advanced Techniques For Network And Data Protection*, 1-13.

Internatiomal Biometrics+Identity Association.(n.d.).Behavioral Biometrics. Washington, DC. Retrieved from https://www.ibia.org/download/datasets/3839/Behavioral%20Biometrics%20white%20paper.pdf

Jain, A., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions On Circuits And Systems For Video Technology*, *14*(1), 4-20. doi: 10.1109/tcsvt.2003.818349

Jain, A., Nandakumar, K., & Nagar, A. Biometric Template Security. Retrieved from https://www.semanticscholar.org/paper/Biometric-Template-Security-Jain Nandakumar/29f0414c5d566716a229 ab4c5794eaf9304d78b6/figure/9

Jin, A., Ling, D., & Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, *37*(11), 2245-2255. doi: 10.1016/j.patcog.2004.04.011

Kindt, E. (2014). *Privacy and data protection issues of biometric applications*. Dordrecht: Springer.

Nandakumar, K., Jain, A., & Pankanti, S. (2007). Fingerprint-Based Fuzzy Vault: Implementation and Performance. *IEEE Transactions On Information Forensics And Security*, *2*(4), 744-757. doi: 10.1109/tifs.2007.908165

Ozkaya, N., & Sagiroglu, S. (2010). Generating One Biometric Feature from Another: Faces from Fingerprints. *Sensors*, *10*(5), 4206-4237. doi: 10.3390/s100504206

Kişisel Verileri Koruma Kurumu.(n.d.).Özel Nitelikli Kişisel Verilerin İşlenme Şartları. Retrieved from https://www.kvkk.gov.tr/Icerik/5238/Ozel-Nitelikli-Kisisel-Verilerin-Islenme-Sartlari

Pagnin, E.,&Mitrokotsa,A.(2017). Privacy-Preserving Biometric Authentication: Challenges and Directions. *Security And Communication Networks*, *2017*, 1-9. doi: 10.1155/2017/7129505

Takahashi, K., & Hirata, S. (2011). Cancelable Biometrics with Provable Security and Its Application to Fingerprint Verification. *IEICE Transactions On Fundamentals Of Electronics, Communications And Computer Sciences*, *E94-A*(1), 233-244. doi: 10.1587/transfun.e94.a.233

Thanki, R., Dwivedi, V., & Borisagar, K. (2018). Issues in Biometric System and Proposed Research Methodology. *Multibiometric Watermarking With Compressive Sensing Theory*, 47-63. doi: 10.1007/978-3-319-73183-4_3

Uludag, U., & Jain, A. (2004). Attacks on biometric systems: a case study in fingerprints. *Security, Steganography, And Watermarking Of Multimedia Contents VI*. doi: 10.1117/12.530907

Vojkovic, G., & Milenkovic, M. (2018). GDPR in access control and time and attendance systems using biometric data. *2018 41St International Convention On Information And Communication Technology, Electronics And Microelectronics (MIPRO)*. doi: 10.23919/mipro.2018.8400207

Yampolskiy, R., & Govindaraju, V. (2009).Taxonomy of Behavioural Biometrics. *Behavioral Biometrics For Human Identification*, 1-43. doi: 10.4018/978-1-60566-725-6.ch001

Zhang, Y., Qin, J., & Du, L. (2015). A secure biometric authentication based on PEKS. *Concurrency And Computation: Practice And Experience*, *28*(4), 1111-1123. doi: 10.1002/cpe.3539