enhAnced Mobile BiomEtRics

DELIVERABLE: D6.8

Issues and Challenges on Template Protection in Mobile Framework

Contract number:	675087
Project acronym:	AMBER
Project title:	Enhanced Mobile Biometrics
Project duration:	1 January 2017 – 31 December 2020
Coordinator:	Richard Guest, University of Kent, Canterbury, UK

Deliverable Number:	D6.8
Type:	R
Dissemination level	CO
Expected submission date	27.09.2019
Date submitted:	27.09.2019

Authors / contributors	Ebenezer Okoh, Patrizio Campisi
Contributing partners	UNIROMA3

RESEARCH & INNOVATION
Marie Skłodowska-Curie actions

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675087

Issues and challenges on template protection in the mobile framework

Ebenezer Okoh

***Abstract*—Privacy is becoming more and more a key issue that needs to be addressed for the acceptance of biometric systems by the general public. The design of privacy enhancing technologies (PET) tries to answer this need by transforming the biometric reference information, namely the template, in identifiers that ideally leak little or no information about the underlying biometric that was captured, thus minimising privacy issues. Furthermore, comparison is carried out directly in the transformed domain of the identifier space, thus allowing the original template to be discarded. With the embedding of biometric sensors in mobile devices and their use in everyday applications, the need to use template protection techniques properly designed for mobile applications, arises. This problem has not been given much attention in literature. As a result, this paper addresses security and privacy challenges in the design of template protection algorithms specifically tailored to the mobile scenarios.**

***Index Terms*—privacy, security, biometrics, PETs, template protection.**

I. Introduction

BIOMETRICS technology is mechanism for assigning a unique identity to an individual based on some anatomical, physiological, or behavioural properties. These properties are sometimes called as biometric modalities, identifiers, traits or characteristics. The current biometric traits are grouped into biological traits (e.g., DNA, EEG analysis, and ECG analysis), behavioral traits (e.g., signature dynamic, human gait, and voice signal) and morphological traits (e.g., fingerprint, face image, and iris pattern) [1]–[3]. Due to its merits, biometrics technology has fueled extensive industrial revenue and investments, and it is becoming mandatory in jurisdictions such as travel, immigration and border control as well as mobile applications [4]–[7]. Biometrics has empowered the current state of the art in terms of authentication to move beyond its conventional form such as passwords to a more secure and convenient system. In spite of the desirable properties of biometrics, there are still issues concerning security of biometric recognition systems that need to be addressed to foster public acceptance and integrity of the system [8]. More importantly is the security of the biometric template as public acceptance of biometric system is influenced by secure storage of the biometric data.

II. Background

Privacy is becoming more and more a key issue that needs to be addressed for the acceptance of biometric systems by the general public. The design of privacy enhancing technologies (PET) tries to answer this need by transforming the biometric reference information, namely the template, in identifiers that ideally leak little or no information about the underlying biometric that was captured, thus minimising privacy issues. Furthermore, comparison is carried out directly in the transformed domain of the identifier space, thus allowing the original template to be discarded. With the embedding of biometric sensors in mobile devices and their use in everyday applications, the need to use template protection techniques properly designed for mobile applications, arises. This problem has not been tackled in literature to date. This three-year project will deal with the design of template protection algorithms specifically tailored to the mobile scenario. Specifically our activity will be devoted to a) the design of biometric cryptosystems, that is systems that combine signal processing tools and cryptographic primitives, b) transformation based template protection approaches, that is systems that perform non-invertible transformations on the original template and c) defining effective metrics for security assessment of a protection scheme with respect to compliance with the required properties such as non-invertibility.

A. Biometric security systems

Biometric systems can be classified into different modules irrespective of the biometric characteristics used, with each module performing specific function. Ordinarily, biometric system comprises of five modules: sensor module, feature extraction module, system database module, matching module and decision module. The sensor module is the interface where the biometric data of the user is acquired. The design of the sensor module is highly crucial to the performance of the biometric system in general [9]. High quality biometric data rendered at the sensor level can highly increase system performance and vice versa. At the feature extraction module, the acquired biometric data is analysed and processed including signal enhancement to further improve its quality. At this stage, salient discriminatory features useful for distinguishing between users are extracted [8], [9]. The extracted feature set from the biometric sample is stored in a database as biometric templates. Storage of the biometric template is usually accompanied by users' identity attributes such as (name, address, ID number etc) when such information is available. In certain scenarios when users' attributes are not available such as crime scenes, captured latent prints are stored with system generated IDs. The matching module is an executable program that determines the similarity between two sets of biometric features i.e (stored template and query) [8]. It takes two sets of biometric data as input and outputs a similarity score. The decision module, based on the similarity score makes the

identity decision by either validating a claimed identity or provide ranking of enrolled users for identification purposes [9].

B. Vulnerability of Biometric security systems

The applications of biometrics as well as its benefits is well known but like any security system, it has vulnerabilities. Vulnerability is a weakness of an asset or control that has the potential of being exploited by one or more threats [10]. Biometric system vulnerability is defined as the avenue of attack against a biometric system that involves an active attacker [11]. A threat is a potential event that may cause an unwanted incident by causing damage to a system [10]. Three types of threat dimensions were identified by [12]; threat agents, threat vectors, and system vulnerabilities. Threat agent is a person or system that has the potential to compromise the biometric system either intentionally or unintentionally. The threat agent could either be an impostor (any person who intentionally or otherwise poses as an authorized user); an attacker (a system or person attempting to compromise the biometric system); or an authorized user [12]. In [1], the authors classified two types of threat agents within the biometric settings; intrinsic limitations and adversaries. In relation to exploitation of loopholes in biometric security system, the educational complexity of a threat agent is crucial in determining the capabilities or resources s/he possesses [13].

- Intrinsic Limitations: Intrinsic limitations of the biometric system is about inherent limitations of the biometric system modules such as sensor, feature extractor, matcher and decision modules. This type of limitation is largely brought about by the variability in the acquired biometric traits which can lead to incorrect decision by the biometric system. The two common types of errors as a result of incorrect decision by the systems are false match and false non-match. False match presents the scenario whereby two samples from different individuals with high similarity is declared by the system as a match. On the other hand, false non-match presents the situation whereby two samples of a particular trait belonging to an individual, with low similarity is declared by the system as non-match. This type of limitation is known as zero-effort attack as it does not require any effort from an impostor to circumvent the system. The performance of a biometric system hinges on its resistance to zero-effort attacks which is also considered to be the system's false accept rate (FAR) [11].
- Adversaries: Adversaries can manipulate a biometric system to fail as long as they gain logical or physical access to the system. In this case the adversary can be an insider or an impostor/attacker. Insider attack is one of the most greatest threats within computer/information security settings and which is typically categorized into traitors and masquerades [14]. A traitor is an authorized user with certain privileges to the biometric system but whose action is to cause damage to the system. A masquerade is the person who performs malicious acts by acquiring the identity of a legitimate user of the system. In [1], the authors further categorized into insider and infrastructure attacks. Typically, the infrastructure of a biometric system consists of integrated components (sensor, feature extractor, matcher, template storage, and decision) and the communication channels interlinking these modules. Loopholes in a biometric system infrastructure can be exploited by an adversary in many ways which can be generally categorized as insider attacks and infrastructure attacks [1].

An attack is an attempt to destroy, expose, alter, steal, disable, use or gain unauthorized access to a system [10]. In so far as the attacks on biometric systems is widely acknowledged, the interest in countermeasures to control and prevent these threats have increased significantly. The points of attack by which the biometric system could be attacked is known as threat vectors. Essentially, like any other security system, to ensure security means implementing countermeasures to militate against exploitation of vulnerabilities in the system. As pointed out by [1] security threats of a biometric system can be grouped into four classes: Denial of Service, Intrusion, Repudiation, and Function Creep which can result in loss of privacy and security threats. Denial of service and intrusion are the most prevalent security threats of a biometric system.

- Denial of Service
- Intrusion
- Repudiation
- Function Creep

Several taxonomy of attacks as well as attack vectors in biometric system which is fundamental to understanding and analyze ways by which the biometric system can be attacked have been well elucidated in the following works [1], [8], [15]–[17]. From these works, it could be discerned that the attack vectors are largely dependent on the biometric system design. Ratha et al. [17] identified eight points of attack in a generic biometric system with which it is vulnerable to attack as shown in Figure 1 below. Anil K. Jain et al. [8] grouped the attack points identified by Ratha et al. into the following four categories: attacks at the user interface; attacks at the interfaces between modules; attacks on the modules; attacks on the template database.

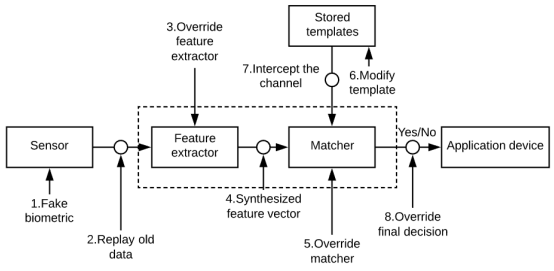

Fig. 1: A generic biometric system attack points (adapted from [17])

C. Advancements in Biometric Template security

Biometric template is the data obtained from the capture of biometric sample by the biometric capture device. The data,

upon further analysis is converted into another format mainly (binary mathematical file or statistical model) which contains unique and salient features of the biometric trait. The template is a compact digital representation of the sensed biometric trait that contains salient discriminatory information necessary for individual recognition [1]. There are a number of ways by which the stored template if not secured can be exposed to adversaries and thus lead to security problems. Attacks on template database lead to the following vulnerabilities [8]: i; a template can be replaced by impostor template ii; physical spoof can be created from compromised template iii; compromised template could be replayed. Due to the immutability nature of biometrics, stolen or leaked biometric template can gravely affect the privacy of enrolled users in the system. To this end, revocation and reissuance of compromised biometric template continues to be a challenge within the biometric segment. This is due to the fact that exposed template cannot be replaced with biometric sample of the same trait as in the case of compromised passwords. Essentially, if biometric template is compromised in one application can lead to the compromise of other applications that employ the same biometric trait (cross-matching). Vulnerabilities associated with the biometric template have engendered research into template protection schemes. In principle, biometric template protection scheme should satisfy the following properties [18]:

- Non-invertibility: It should be computationally difficult to obtain the original biometric template from the secured template.
- Renewability: It should be possible to revoke and reissue new instances of biometric reference based on the same biometric data when compromised.
- Non-linkability: This property is to prevent cross-matching across different applications, thereby ensuring users' privacy.

Biometric template protection schemes are commonly categorized into; biometric cryptosystems and cancelable biometrics.

D. Evolution of Biometrics in mobile security

Mobile devices have revolutionized communication within the age of information. Mobile devices affect every aspect of our lives as mobility continues to transform and redefine ubiquitous computing. Survey conducted by [19] in 2017 shows that mobile devices was a basis of increase in web page views worldwide, 49.5% while in 2018 the global mobile population amounted to 3.7 billion unique users. The same survey projects global mobile data traffic to increase about seven fold from 2016 - 2021 as a result of the increase in the use of mobile devices. Figure 2 shows the global digital population of October, 2018 from [19]. The evolution of mobile devices have been immense in terms of their complexities. In that mobile devices are increasingly becoming powerful with computing capacities approaching that of traditional PCs. Though a lot of biometric traits have made a lot impact on security of mobile devices in recent times, it was the fingerprint trait that was first introduced.

It all started when Apple introduced iphone 5S featuring fingerprint scanner in 2013. According to [20], before the release of Apple's iphone 5S, other companies had already launched mobile phones featuring fingerprint capability. Actually, in 2004, Pantec Inc. released the first working mobile phone with fingerprint sensor. Later on in 2007, Toshiba and HTC Corporation introduced the G-series and P-series of phones respectively with fingerprint scanners. Around 2009 - 2010 other companies like Acer Inc., LG Electronics Inc. and Motorola Inc. joined the race. From the mobile phones market standpoint, it was the release of Apples's iphone 5S in association with its fingerprint feature (TouchID) that revolutionize the mobile phone industry. Smartphones in recent times have sufficient processing power and hardware capabilities to process personal, corporate and financial data as well as act as communication hubs.

Confidential transactions are increasingly performed on these devices which calls for measures to prevent potential threats. According to [21] report that 61% of people use their mobile phone for banking activity while 78% of people had made purchases with their mobile phones as at 2017. There has been a growing concern of the security of smart devices. Kaspersky lab press release in 2016 shows that mobile devices have become a new target for spam and malware attacks [22]. In any security system, authentication is known to be the fundamental component. Conventional authentication methods such as passwords, PIN, tokens are known to be fraught with vulnerabilities. These security concerns have led consumers adopt biometrics as authentication mechanism. Mobile biometrics have shown promising signs of providing security as well as user convenience. Biometrics are increasingly being added to mobile devices of which fingerprint is most widely used. Other biometric traits such as face, voice, keystroke, iris are increasingly being explored. As more biometric traits are being explored in securing mobile devices in place of conventional authentication mechanisms, it raises new privacy and security issues.

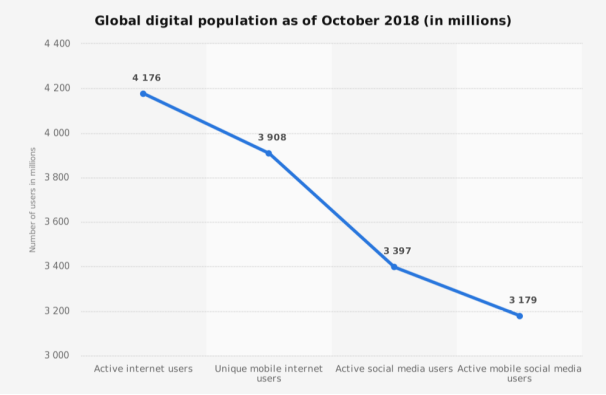

Fig. 2: Global digital population as of October, 2018 [19]

It is generally acknowledged that mobile technology has been spreading at unprecedented speed in the last two decades. Rapid growth of the mobile technology clearly shows how they are integrated into our everyday life. The focus is gradually being shifted from personal computers to mobile devices

in that mobile devices have evolved and are increasingly becoming more sophisticated with enough hardware capabilities. With the added functionalities of mobile devices, make them capable of wide range of tasks such as storage of personal/business information, internet banking, online payment, social networking etc. and not just a tool of communication. The trend in the mobile industry has introduced another phenomenon within the business sector known as Bring Your Own Devices (BYOD). Businesses adopting BYOD policies seek to boost productivity, save money as well as increase employee satisfaction and convenience.

These devices store and transmit sensitive personal and corporate information as they are used to access a wide range of services [23]. Clearly, mobile devices with their added capabilities open up new opportunities however, they also bring with itself associated security risks. In as much as the concept of mobility promotes convenience with regards to the consumer, it may also come along with security risks. This means that users' devices are at a greater risk of being lost or stolen. Mobile applications are becoming the focal point of security attacks (particularly malware attacks, identity theft)as users tend to spend much time on and also perform virtually all their transactions on. Information contained on these devices has become attractive to all kinds of malicious attackers which poses a greater risk when information (personal or business) gets into the wrong hands. The rise in the use of mobile devices has made them a rich target for developers of malware and all forms of cyber attacks and which has acted as a spur to the rise of mobile malware. In the first quarter Kaspersky Lab report of 2017, they stated mobile ransomware attacks have gone up by 253% [24].

To address these security threats, the first line of defence has always been user authentication [25]. Secure authentication is essential in protecting the mobile device as well as the applications on it.

III. Security and privacy challenges in mobile devices

Many mobile devices are like computer device or second computer device for most users in that they may have operating systems allowing other applications or softwares to be installed and run. Along with the rapid increase in mobile device usage has seen a surge in cybercrimes adapting to exploit the potential increase in mobile device vulnerabilities. One of the most common ways by which cybercriminals exploit potential vulnerabilities in mobile devices is through Malwares, which are malicious softwares specifically designed to target the mobile device. Malwares once implanted in a mobile device can inflict a lot of damage such as steal credit card information or login credentials. Because information has become valuable in recent times so is stolen data. As a result, deployment of malwares to steal data have become such a lucrative trade not only for isolated teenage groups but by governments, criminal groups and hacktivists [26]. According [26], malwares in recent times are more sophisticated in that they can easily evade antimalware techniques. They classify the evasive techniques into three categories:

- Anti-security techniques: Used to avoid detection by antimalware engines, firewalls, application containment, or other tools that protect the environment.
- Anti-sandbox techniques: Used to detect automatic analysis and avoid engines that report on the behavior of malware.
- Anti-analyst techniques: Used to detect and fool malware analysts.

Through malwares, cybercriminals are able to gain access to the mobile in diverse ways to carry out attack. The advanced and evasive nature of malwares in recent times makes it difficult to implement security mechanism that successfully neutralizes the threat.

A. Security challenges in biometric-based mobile platforms

Surveys have shown mobile devices are under increasing attack from mobile malware. There has not been much of awareness creation since the inception of mobile device malwares. As a consequence, mobile device users have had the perception they are not susceptible to such threats. However, in recent times there has been gradual awakening in respect to its impact to stakeholders and users.These dreadful programs attack all mobile device platforms but in recent times majority of the attacks have targeted Android platforms. Essentially, depending on the attack vector cybercriminal might use to gain access to the mobile device, mobile security threat can be classified under one of the following categories: physical, application-based, web-based, and network-based threats.

B. Privacy challenges in biometric-based mobile platforms

Privacy has different interpretations under different jurisdictions. Generally, data privacy within the jurisdiction of Information Technology (IT) that usually relates to proper handling of personal data stored on a computer system which involves data sensitiviy, consent, notice, and regulatory provisions. As such privacy is seen to touch on legal, technological and procedural concerns. However, in the context of this research work, we refer to regulatory restriction such as the general data protection directive (GDPR) 2016\679. At the center of GDPR's interpretation of data privacy, is personal data. Art. 4 GDPR specifies various definitions regarding GDPR. GDPR defines personal data in Art. 4(1)(1) as any information which are related to an indentified or identifiable natural person. It goes on to define an identifiable natural person as one who can be identified, directly or indirectly, especially by reference to an identifier such as name, identification number, location data, online identifier, one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. There are inherent privacy concerns in relation to biometric data use as authentication method in general and particularly in mobile platforms. It is of utmost importance to take a critical overview of privacy risks pose by biometric applications in mobile platforms in spite of the great opportunities it provides to individuals and industries. A typical biometric authentication system works by comparing the biometric reference captured and stored during the feature extraction process to the biometric sample provided

during authentication. Biometric authentication system can be categorized based on where the biometric reference is stored i.e. smartcard, device itself, or data center [27]. Most mobile devices such as smart phones store biometric information locally on the device itself. The argument made in favor of storing it locally is that, storing the biometric information on a server can be easily hacked since its connected to the internet, whereas local storage could be exploited by adversaries as well. That being said, this section will focus on damaging effects of locally storing biometric information in relation to privacy concerns.

To address these privacy concerns, it is essential we take a critical view of the charateristics of privacy that seek to conceptualize it in order to understand how mobile biometric data relates to the various concepts. The conceptualization will focus more on theoretical theories rather than legal definition. We believe the theoretical conceptions would give us a clear idea as to what privacy is as a whole and where biometric data specifically fits in. We draw the privacy claims as stated by [28]. DeCew in [28] recognized privacy to be dependent on three types of privacy claims: Control of information i.e. Informational privacy; Limited access i.e. Accessibility privacy; and Expressive privacy. These privacy claims overlap as seen in figure 3.

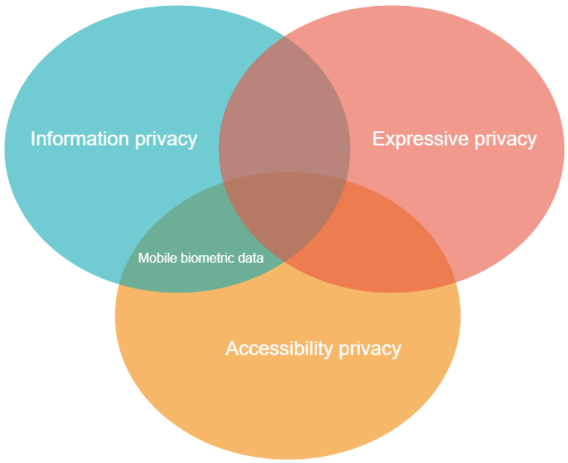

Fig. 3: Conceptualization of privacy

We explain briefly the privacy claims are as follows:

- Informational privacy relates to control over information about oneself.
- Accessibility focuses on information or knowledge and most importantly on observations, physical access and physical proximity. In essence, the concept relies on limited-access and this aspect overlaps with informational privacy.
- Expressive privacy safeguards a domain for expressing one's self-identity or personhood through speech or activity.

Of course, it goes without saying that most of these privacy concepts are deeply rooted in traditional concepts of privacy such as intrusion of physical space, and disclosure of secrets. The biggest challenge we face today is how to understand, identify and address privacy problems in the age of technology advancements. As such, recent advances in new technologies have brought to the fore different privacy problems particularly mobile data privacy. For instance, technology makes it possible for knowledge about someone to be established without physically breaching the person's space.

Though privacy conceptualization helps to understand how mobile biometric data in this context relates to the various concepts of privacy, it is worth considering development of taxonomy to help address privacy issues arising as a result of mobile biometric data. Taxonomy of privacy presents a framework to understand the myriad of privacy issues, how they arise, similarities, differences, and the relationship among them [29]. Solove, in [29] proposed a taxonomy of privacy that is based on four privacy problems or harmful activities: information collection, information processing, information dissemination, and invasion. We present a taxonomy of mobile biometric data privacy adapted from [29] and depicted in figure 4. Within the context of mobile devices and in particular mobile biometric data, we talk about:

- ***Biometric data collection*** is the first step to measuring the physiological or behavioral characteristics of users widely accepted to be distinctive, repeatable and permanent. Privacy concerns are at the heart of information collection, and biometric data which contains identifiable information about individuals is no exception. Collection of biometric data are often associated with intrusion of privacy. Biometric data is widely recognised as a personally identifiable information. This recognition is rooted in data protection legislations or guidelines enacted by countries to protect data such as the EU GDPR directive. Moreover, the GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person". At the heart of the definition given by article 4 of the GDPR directive on personal data is "identified or identifiable natural person (data subject)". It defines identifiable natural person as "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". Under the article, it can be noticed that a spectrum of activities can harm privacy of the individual through the process of data collection. The use of biometrics on mobile devices in this modern era has been projected primarily to providing better security to mobile devices and making mobile transactions. Opting for biometric authentication on mobile devices is gradually becoming the norm as it affords the user convenience and secure authentication mechanism. On mobile devices such as smartphones and tablets, the first step of biometric data collection is at the enrolment stage. At this stage, users who are wary about privacy become concern about rendering their biometric data. A number of questions privacy wary users contend with at this stage include:

Why must I render my biometric data?; Is biometric data really needed to achieve my goals?; What happens after providing my biometric data?; Who would own my biometric data?

Data collection process involves presenting users' biometric characteristics to the mobile sensor. A sensor that is appropriate for measuring or recording the biometric characteristics is used. The mobile sensor captures the biometric sample, digitized and converted to biometric template. Biometric sensors embedded in a mobile device is well adapted to measuring specific biometric characteristics such as fingerprint, iris, or face. The biometric sensor could be in the form of infrared cameras for capturing iris characteristics, high definition cameras for capturing face characteristics, optical, solid-state, or ultrasound sensor devices for capturing fingerprint characteristics, or infrared imaging devices for finger/palm veins.

The Home key of most smartphone devices act as the fingerprint recognition sensor. Fingerprint sensors used in mobile phones are usually categorized as swipe sensor and area sensor [30]. Generally, fingerprint scanners can be categorized into one of the following: optical, solid-state, and ultrasound [31]. The optical sensor is the oldest acquisition technique. The technique essentially, involves capturing optical fingerprint image (2D image) and using algorithm to analyse and detect patterns in the image. The principle is based on total internal reflection of light. The technique involves a light source emitted unto the fingertip to reveal the ridges and valleys of the fingerprint which is read by the sensor. The downside of this technology is that it can be easily spoofed through printed images or prosthetic means. Solid-state sensors are commonly known as silicon sensors. The silicon-based sensors comprise of an array of micro-cells with each micro-cell being a tiny sensor by itself capable of reading fingerprint pixels. Four main techniques can be classified under this technology: capacitive, thermal, electric field, and piezoelectric [31]. Among these, capacitive sensors are the most common and are mostly used in smartphones. As a result of their popularity, solid-state sensors are usually referred to as capacitive sensors. It is well suited to be integrated in small devices such as smartphones as it can be greatly reduced in terms of size. The technology is difficult to spoof especially with a 2D-image or prosthetic material than the optical sensor in that the material must have the same conductivity as the skin and also have to be of 3-dimensional. The disadvantage is that the technology is prone to dirt, water, or sweat as it changes the conductivity of the sensor. The ultra-sound scanner has two main components: a transmitter that generates acoustic pulses or ultrasonic waves and a receiver that detects the responses after bouncing off the fingerprint surface [31]. The waves emitted by the transmitter can pass through glass or metal but get reflected by the finger that is placed on the scanner. The echo signal is used to compute the depth and the ridge structure of the fingerprint [31]. Apparently, some of the pulses generated are absorbed and some get reflected depending on the ridges and pores of the finger to create a 3D image. The technology is the latest and yet to be commercialized by the mobile phone industry. The technology is believed to be more secure and for that matter difficult to spoof.

Front facing cameras in most smartphones are used to capture detailed iris characteristics. The iris recognition system uses the unique characteristics of iris to provide security to the mobile phone and its contents. The iris recognition camera has infrared diode embedded which emits near-infrared (NIR) light into the eyes to extract detailed iris information. The infrared wavelength is unobtrusive and also avoids undesirable interference from the environment. Certain mobile phones utilize the high resolution front facing infrared cameras equipped with special sensors to capture details of the face. An attempt is made to acquire as much face biometric data as possible especially where certain smartphones require users to rotate their head left to right or nod. Present facial recognition feature on most smartphone devices is 2-dimensional where acquisition process generates 2D map of the users' face. Typically, facial recognition feature acquire users' face prints by recognizing nodal points on the face. However, emerging technologies are exhibiting features such as 3D sensing functionality for facial recognition in mobile communication. For example, Apple's facial recognition feature, faceID comprises of infrared(IR) camera and projector. The IR projector emits thousands of IR rays toward the user's face to create a 3D model of the face. Other manufacturers have proposed devices having a combo sensor that combines two biometric characteristics such as iris scanner and facial recognition.

- ***Biometric data*** the second step after data collection. With regards to facial recognition, biometric data is obtained by measuring the facial structure. These measurements are touted to be distinguishable among users. Most facial recognition algorithms identify facial features by extracting distinguishable landmarks or nodal points that capture the variations in the face. It is estimated each human face to have approximately 80 nodal points. The nodal points are endpoints that measure for example: the distance between the eyes, shape of the cheekbones, length of the jaw line, width of the nose, and depth of the eye sockets. Acquiring face data involves capturing nodal points on a digital image and creating a numerical code called faceprint. To create faceprint, the system puts the face in preset position while it chooses from various lists of approaches:
  - Geometric approach: which involves calculation of location and spatial relationship between certain facial features.
  - Photometric approach: it refers to the interpretation of face as a weighted combination of standardized faces.
  - Skin texture analysis: maps the unique placement of pores, lines and spots on the skin.

  With respect to iris recognition, it is essential to capture high quality iris images that exhibit unique patterns

to recognize an individual. Factors such as; partially closed eyelids, intruding eyelashes, harsh or non-uniform illumination, low resolution, and extremely dilated or constricted pupil can have negative effect on iris images [1]. The iris patterns and underlying textural details is best viewed with NIR illumination and NIR sensor [1]. Typically, wavelength illumination between range of 700nm-900nm is recommended for iris image acquisition which is compliant with standards such as ISO 60825-1 [32].

Fingerprint scanners depending on the technology used in the mobile device scan image of the fingertip. The scanner illuminates the fingertip through typically an array of light-emitting diodes. It generates an image of the finger consisting of the variations of the ridges and furrows of the fingertip skin to represent the fingerprint. Fingerprint information is the most matured of all the biometric information. The finger or hand skin consists of friction ridges with pores which are found to be distinguishable among individuals. The quality of the fingerprint image has an appreciable impact on recognition performance. some of the factors that affect fingerprint quality include image resolution, finger area, and clarity of ridge pattern [1]. Most fingerprint scanner processor of today's smartphones ensures clear fingerprint image is generated. If the fingerprint does not meet its predefined threshold, it is rejected. It tries to scan again typically after adjusting exposure time. Different algorithms are employed by different manufacturers to identify distinctive features of the scanned fingerprint.

- ***Biometric data processing*** is the stage in the biometric recognition system by which the raw biometric data acquired from the sensor undergoes certain pre-processing operations to extract feature values of the biometric trait. The steps may involve quality assessment, segmentation, noise reduction, normalisation and enhancement. Extraction of features is generally dependent on the type of biometric trait and the set of available algorithms.

  In the case of iris recognition, preprocessing begins with segmentation after image quality has been assured. Segmentation algorithm is needed to isolate the actual iris boundary from noise in the image. These noise could be in the form of occlusions of eyelashes, off-angle irides, motion blurs, specular reflections, eyeglasses, and poor illuminations. Several algorithms can be employed at this stage to detect the inner and outer boundaries of the iris. Some of the widely used segmentation algorithms are:

  - Integro differential operator (IDO) (that assumes the outer boundary to be circular or elliptical and is ideal for detecting circular edges. This method was first utilised by Daugman in [33] to locate irregular shapes of iris and pupil boundaries. Other works such as [34] extended the IDO technique to improve the speed and efficiency of iris recognition);

  - Hough Transform, is a classical segmentation technique used for iris boundary detection in iris images. By this technique, parameters such as radii and center coordinates of the iris and pupil can be determined through edge map voting in Hough space for the parameters of the circle passing through each edge point. The approach was first introduced by Hough [35] to detect arbitrary shapes like lines or circles in digital images and is utilized by [36] to localize iris and pupil regions in an image.

  - Active contours also known as snake is an energy-minimizing parametric closed curves guided by external constraint forces and influence by image forces that pull it toward features such as lines and edges [37]. Ritter [38] first proposed active contour model that searches pupil and iris boundaries by finding the equilibrium of internal and external forces. Variants of the active contour approach have been proposed in [39], [40]. The technique is ideal for detecting and isolating the actual inner and outer boundaries of the iris that might be occluded by the lower and upper eyelids and eyelashes. The method is dependent on the gradient information in the image and as such the performance of also depends on the edges or gradient information of the image boundary);

  - Geodesic active contour (which is a variant of classical active contour is ideal for detecting irregular contours. The model was first proposed by [41] to detect edges of objects simultaneously in a digital image. It is based on the relation between active contours and the computation of geodesics (minimal length curves). The strategy is to evolve the contour from inside the iris under the influence of geometric properties of the iris boundary in the image. This approach combines geometric active contour curve evolution technique and minimization technique of classical snake). Shah and Ross [42] made use of this approach for iris segmentation;

  - Region growing/Watershed transform methods; The watershed segmentation approach was proposed by Beucher and Lantuejoul in [43] is a non-parametric contour detection technique which treats an image as a height function describing a landscape. The landscape is partitioned into regions or basins separated by watershed lines. It combines features of both edge-based and region-based image segmentation approaches. Pixel grouping lead to the formation of regions whereas edges of regions are as a result of detecting locations of discontinuities between an image. The intuition underlying this approach is that it assumes image as a surface with watershed lines and catchment basins. The watershed lines of the gradient correspond to the contour lines while the catchment basins correspond to the regions in the image that represent the object of interest to be identified. Often watershed transform is applied to morphological gradient of the image instead of the actual image to produce gray value in the image corresponding to the minima of the gradient [44]. Works such as [45], [46] used the watershed transform approach to detect iris boundary in a noisy environment.

  Region growing is region-based image segmentation technique. The method works with the principle that regions should be homogeneous for which pixels satisfying the criterion would be added to the region. The process groups pixels or subregions into larger regions. The

approach is preferred in a noisy environment to edge-based techniques where edges are difficult to be detected. The approach normally starts with an arbitrary seed pixel and compare it with neighbouring pixels. The region is grown from the seed pixel by adding neighbouring pixels that are similar, thus increasing the region's size. Another seed pixel which does not belong to any region is chosen and the process started again when the growth of the previous region stops. Regions are grown from seed points on the basis of region membership criterion such as pixel intensity, color etc. Many works have contributed to iris segmentation using the region growing-based method [47], [48].

- Deep-learning based methods. Due to the popularity of deep learning in computer vision tasks, there has been much attention on using deep learning techniques in exploring iris recogniton. Recent approaches such as [49], [50] have investigated deep learning frameworks for iris recognition. The network learn features that can be used for various image processing tasks. In such frameworks, the network finds the best way to combine image pixels for recognition by supplying images as input to its multi-layer neural network. Considering iris segmentation, one of the most popular among deep learning methods in computer vision applications is Convolutional Neural Networks (CNN). Liu et al. [51] employed fully convolutional networks (FCN) to detect iris boundaries in non-cooperative environment. Some of the standard deep neural networks that have made significant contributions in the field of computer vision and used as a basis for image segmentation include AlexNet, ResNet, VGG-16, and GoogLeNet. Iris prints encode mapping of furrows and striations in the iris.

In the case of fingerprints, extraction of features may involve ridge orientation and frequency estimation, ridge extraction, singularity extraction and minutiae extraction [1]. Fingerprint features are widely categorized into:

- Level 1 features (Global characteristics), which refers to the local ridge orientation and frequency at each location of the fingerprint. Ridges assume distinctive shapes at this level which are collectively defined as singular regions and commonly classified into loop, delta, and whorl [31]. Level 1 features are widely used for fingerprint classification since fingerprint classes could inherently be defined from singular point features.
- Level 2 features (Local characteristics), which represents ridge skeleton and features constituting minutiae details of the fingerrint. Minutiae features are most commonly used for automatic fingerprint matching.
- Level 3 features (Finest details), captures fine details which includes intra-ridge details such as ridge contours, breakes, sweat pores, scars and creases. These type of features are highly distinctive and more useful for latent fingerprint examiners [31].

Generally, Level 1 and 2 features (global and local features respectively) are mainly employed for commercial fingerprint recognition systems by first extracting level 1 features followed by level 2 features [1].

- ***Biometric data storage*** is the repository of the biometric information in that it stores unique and identifying features extracted from users. The unique biometric features are converted into a mathematical file known as biometric template. The template represents a digital reference of the specific characteristics of the biometric trait. There are several biometric data storage strategies that are employed. The main strategies that are often considered are centralized storage, portable-token, on-device, hardware-based, and distributed data storage approaches. Portable devices have no centralized storage system. The biometric data is stored on devices such as smart cards. Even though it is costly to implement such strategy, the user has control of the biometric data and would have to present the biometric smart card during authentication. On the contrary, centralized storage approach is less costly and enables biometric data to be accessed from multiple locations. It puts organizations or data controllers in full control of end-users' biometric data and therefore assume responsibility of the storage and management of the data. The distributed data storage system ensures that users' biometric data is stored both on a server and a device. The biometric data is split and stored separately on centralized storage and the authentication device. In this way, both the user and organization have responsibility to maintain control of its biometric data. Hardware based storage is when the biometric data is stored on a piece of hardware (control board). It is integrated with the recognition device to recognize the data but the data is not stored on the device itself.

  Smartphone manufacturers are known to store biometric information locally on the mobile devices instead of a centralized database. This is where the on-device approach comes into play. Here, the biometric data is stored on end-users' device which could be by a chip where the biometric data is kept separate from the device's network.
- ***Biometric data usage/dissemination*** Dissemination is a planned process that involves transfer of data or information to key actors to make best use of it. Processing of biometric data is essential for a variety of reasons in mobile devices. Most important of all is for recognition purposes. Under the GDPR, processing means any operation or set of of operations which could be performed on personal data or sets of personal data. The wide-ranging term can include the use and dissemination of data. Biometric data is also considered sensitive personal data under the GDPR and as such biometric data use and dissemination should be determined under the GDPR framework. Generally, GDPR disallows the processing of biometric data, however at the same time it provides certain exceptions to justify its processing. Chief among GDPR biometric data processing exemptions are informed consent of the data subject and other legal grounds proportionate for specific legitimate purpose can permit its processing. Processing is further dependent on legislation of EU member countries who have the right to introduce other conditions or

restrictions with regard to the processing of biometric data. As such, legal requirements vary across member EU countries for the processing of biometric data. The GDPR (recital 32) specifies that consent should be freely given and unambiguous indication to the processing of the data subject's personal data. Chapter 5, (Art. 44 - 50) of the GDPR provides provisions such as appropriate safeguards, binding corporate rules for processing or transfer of personal data to third countries or international organisations. Moreover, when processing is likely to result in a high risk to the rights and freedoms of data subjects, the GDPR (Art. 35) introduces requirement of data protection impact assessment to be conducted by data controllers. Particularly so is processing of personal data that involves the use of new technologies. Personal information transferred to controllers or service providers in other non-EU countries involves a lot of legal and ethical provisions under chapter 5 of the GDPR.

- ***Biometric data update*** Biometric traits being biological characteristic are affected by ageing. A biometric authentication system operates by comparing new input biometric data against template data collected during enrollment phase and stored in a database for user identification or verification of claimed identity. The enrollment phase mostly involves capturing new biometric data, processing to extract salient features and storing as template in a controlled environment. Generally, biometric characteristics are considered to be unique and stable (permanence). The performance of a biometric authentication system is dependent largely on the matching accuracy which also relies on stability of the biometric data over time. However, biometric data tend to exhibit uncertainty and variations (intra-class variability) due to:
  - Variations within persons: Input biometric data may be affected by factors such as changes in environment, age, expression, pose, scars, stress especially to face image, disease etc.
  - Sensors: Noise introduced at the sensor as users interact with the system can lead to intra-user variations. Again variations could be introduced as a result of the type sensor used in terms of its calibration, age and performance in general.
  - Feature extraction and matching algorithms: Feature extraction algorithms that are not able to extract significant features as well as matching algorithms that are not robust can cause variations in the biometric template.

  Ageing within the context of biometrics can be classified into two [52]:
  - Biological age, where absolute age of the individual directly affects the available biometric data.
  - Template age; which refers to the time lapse between which the biometric system actually undertakes a matching decision against the biometric template stored.

  In order to account for time and intra-class variability calls for periodic update of the stored biometric template. Template update which is the process by which existing templates are either replaced or modified consist of the following [53]:
  - Template ageing: This refers to the situation where the biometric trait of the individual undergoes constant change with age. For instance, the hand geometry of a child changes especially during early years of growth. In such situations old templates have to be constantly be replaced with new ones.
  - Template improvement: This a situation when already existing template is updated to include variations obtained at more recent time.

  Effects of template ageing is not only dependent on time lapse between enrollment and authentication but to some extent on absolute age of the individual within the time frame [52]. It is well established in literature, ageing and other factors such as environment affect or causes variations in biometric features such fingerprint, face, iris, voice and other traits used for biometric authentication system. Various template update strategies have been proposed in [53]–[55]. In [54], authors proposed cache replacement strategies namely; First In First Out, Least frequently Used, and Least Recently Used to replace biometric reference. Authors in [55] presented three different supervised template update strategies; model-level adaptation, score-level adaptation, and compound adaptation. Model adaptation is adjusted to the user to provide user specific model. Score-level adaptation normalises acquisition scores in a condition dependent way while the compound strategy combines the two approaches. Authors in [56] presented overview of template update strategies for biometric systems.

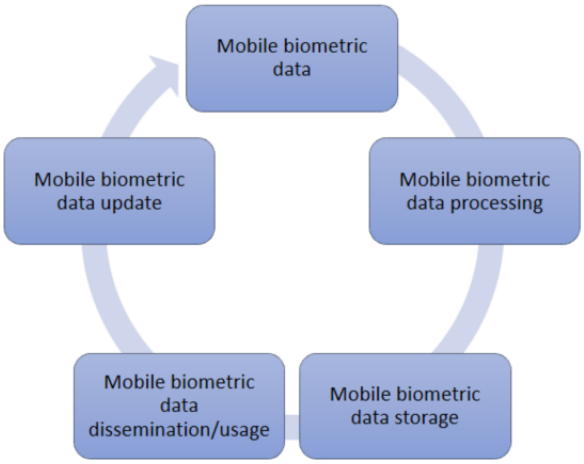

Fig. 4: Taxonomy of privacy adapted from [29]

IV. Security and privacy opportunities in mobile devices

A. Security opportunities in biometric-based mobile platforms

B. Privacy opportunities in biometric-based mobile platforms

V. Information Security Evaluation Process

Security evaluation is a crucial part of system development and is needed to provide evidence of performance or information security level of the system. Security evidence can be useful for both quantitative and qualitative analysis. Information security procedures and process can be quantified in terms of the information usage which could serve as evidence of conformance to a certain standard. The principal goal of security evaluation process is to identify vulnerabilities and threats whiles taking into account the capabilities of an adversary [57]. It is assumed attackers have various levels of resources, expertise and motivation. Generally, security evaluation can be performed in two ways: to determine if a security condition has been met; and to compare security criteria of a system against predefined set of criteria or standards. Among some of the well known internal security standards or frameworks are; Common Criteria (ISO/IEC, 15408), ISO/IEC 17799, and ISO/IEC 24745.

Information security evaluation process results in evidence of assurance which leads to a measure of trust and also indicate how well a system performs based on a certain criteria. The process requires tools or metrics to be able to measure the performance of a system based on a criteria to allow meaningful comparison to be made. It is also essential the measure of trust on a system is measurable and quantifiable which ultimately is critical to achieving security assurance of the system. Trust relies on evidence to determine the level of trustworthiness. Trustworthiness in the context of information security relates to evidence that a system meets requirements of a certain criteria. It is noted that security assurance is a feature of trust which gives rise to measures to ensure systems conform to security standards or framework.

VI. Security and privacy assessment of template protection

Privacy and security analyses of template protection must begin with a clear definition of protection goals to clarify the objectives of the evaluation criteria as well as the security and privacy aspects to be assessed. Next, is to determine threat models to identify capabilities of the adversary by determining information and resources available to him/her. Final step involves the actual evaluation which could be theoretical or empirical. In this section, we define threat models, protection goals, and evaluation metrics shown in figure 5 and adapted from [58].

As a first step to evaluation process, protection goals should be defined to clarify the aim of the evaluation. In essence, it is to be able to determine the objectives of the evaluation as well as template protection property requirements. One of the most important property of template protection method is to achieve randomness and one-wayness. With these properties achieved, protection goals such as security, privacy, unlinkability and

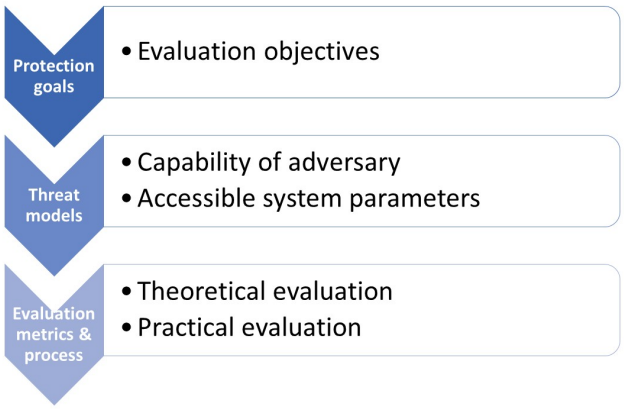

Fig. 5: Generalized security and privacy evaluation framework adapted from [58]

randomness can be evaluated. More so, these properties are the basis for security and privacy requirements of protected templates such as renewability, unlinkability, revocability, confidentiality and data minimization.

Generally, as a prerequisite to security and privacy assessment of biometric template protection, it is important to identify threat models for the evaluation. Threat models makes it possible to identify and access information about biometric data, system parameters and functions during the evaluation [58]. Essentially, threat model process helps to determine:

- Capabilities of the adversary
- Information and system parameters accessible to an adversary
- Computational power within easy reach by an adversary

Three threat models are defined as follows:

- Naive model: This is the basic threat model where it is assume the adversary has no knowledge of underlying algorithm of template protection system. It is also assumed the adversary does not own large biometric database. The whole system is considered black box to the adversary and has access only to the output of the system, which is protected template.
- Advanced model: In this model, it is assumed an adversary has full knowledge of the underlying algorithm as stated in Kerckhoffs principle of cryptology. It is also assumed the adversary understands statiscal properties of biometric features. For security assessment of a secret-based biometric protection system, it could be assumed an adversary has access to all system parameters except the secret information. However, for privacy assessment, it could be assumed the adversary has access to the secret information to help determine if biometric information leakage exists and how much of biometric information is leaked.
- Collision model: This model infers that an adversary has large amount of biometric data and can gain enough information from the data. The adversary has the capability of exploiting vulnerabilities of the biometric template protection system. By undertaking an exhaustive search

of the biometric database, the adversary can create a link between biometric data and that of a target user.

Evaluation metrics are needed to quantify protection goals. In this section, we borrow metrics from information theory domain which are well suited for security and privacy assessment of template protection. Here, we look at metrics of information theory such as entropy, conditional entropy, and mutual information. Entropy is the expected number of bits of information contained in a random variable. Entropy is more useful as a metric in the naive threat model as no additional information is available. Moreover, no parameters and variables are taken into account. Conditional entropy quantifies the amount of information needed to describe the outcome of a random variable Y given that the value of another variable X is known. In this context, it is suitable in the advance threat model for quantifying the security and irreversibility of biometric data. Here, we define the entropy of a secret S conditioned on an auxiliary data AD as $H(S|AD)$. Mutual information of two random variables is a measure of how much one variable tell us about the other or measure of mutual dependence between the two variables. It is a suitable metric to measure privacy leakage in the advance model. For two discrete variables X and AD, mutual information between them can be defined as $I(X;AD)$.

Other metrics such as min-entropy, average min-entropy, guessing entropy, and statistical distance assess security and privacy from different perspective. Theory of min-entropy measures uncertainty in terms of random variable's vulnerability to being guessed in one try by an adversary. A random variable X has min-entropy defined as $H\infty(X) = k$, if

$$\underset{x}{max}\Pr[X = x] = 2^{-k}$$

In this context, min-entropy is useful in measuring irreversibility in the advance model without considering AD. Given a pair of random numbers (X, Y), average min-entropy like min-entropy is the logarithm of the probability that an adversary given the value of one (e.g. Y) will be able to guess the value of X in a single attempt. In this context, it also quantifies security and irreversibility in the advance model. The average min-entropy of biometric data X conditioned on auxiliary data AD is given by:

$$\begin{aligned}\tilde{H}\infty(X|AD) &\stackrel{\text{def}}{=} -log\underset{z\leftarrow AD}{\mathrm{E}}\underset{x}{\max}\Pr[X = x|AD = z] \\ &= \log[\underset{z\leftarrow AD}{\mathrm{E}}(2^{H\infty(X|AD=z)})].\end{aligned}$$

Guessing entropy is a measure of the difficulty an attacker has to guess the value of taken on by discrete random variable X in one trial of a random experiment. Guessing entropy measures the average number of attempts required to retrieve target data with or without the help of AD. Statistical distance metric is required to measure the distance between two distributions in template protection methods. Typically, it measures randomness of extracted secrets with reference to ideal uniform distribution.

These evaluation analyses can be determined in two ways; empirical and theoretical. The goal of the analyses is to quantify security and privacy requirements which can lead to empirical assessment.

Biometric template protection methods are designed as security and privacy enhancing techniques of biometric data. The International Organization for Standardization, ISO defines criteria and metrics in the ISO reference architecture for template protection ISO/IEC 24745 [59]. The generic model is applicable to various methods and consists of the following functions:

- Pseudonymous Identifier Encoder, PIE: This generates a pseudonymous identifier, PI and auxiliary data, AD from a biometric data, B during enrolment, i.e. $[PI; AD] = PIE(B)$. PI represents the protected identity of the individual used as a reference for verification. AD is user-specific data, part of the protected template, PT which helps to reconstruct PI during verification. Both PI and AD are stored as secured template. Both are not necessarily stored together but are needed during verification.
- Pseudonymous Identifier Recorder, PIR: During verification, PIR computes pseudonymous identifier PI^* from a newly captured biometric data, B^* and auxiliary data AD. This can be written as: $[PI^*] = PIR(B^*; AD)$.
- Pseudonymous Identifier Comparator, PIC: During the decision making process, the computed PI^* is compared with the stored reference PI with the help of PIC. The operation outputs a comparison score, s which could be similarity score or yes/no decision. This can be given as $s = PIC(PI; PI^*)$.

The auxiliary data AD is generally encouraged to be public in most implementations. This is because the protected template, PT within the context of biometric security is generally considered to be public. However, since its not a strict requirement by the standard, some schemes have it as a secret parameter. In terms of template protection approaches, PI is either transformed feature generated from the transformation function or hash secret generated from the cryptographic framework. The AD can be a parameter for the transformation function or helper data neeeded to extract cryptographic key from biometric features during matching. AD is responsible for handling intra-user variation and renewing PI. Ideally, protected template as already been mentioned should possess properties such as noninvertibility, robustness, renewability and unlinkability(diversity). We explain these properties in the context of the ISO reference model:

- Noninvertibility: It should be computationally hard or impossible to obtain the original biometric template from the extracted PI.
- Robustness: The generated PIs should be robust against variations and uncertainties exhibited by the input biometric data. This enables PIC to compare PIs directly. The applied template protection scheme should not degrade the recognition performance of the biometric system.
- Renewability: It should be computationally difficult to obtain the original biometric template from multiple instances PIs derived from the same biometric trait of an

individual. This makes it possible to revoke and reissue new instances of compromised PI.

- Unlinkability: It should be computationally difficult to know whether two or more instances of PIs were generated from the same biometric trait of a user. This prevents cross-matching across different applications.

In this work, to deal with template protection schemes in mobile environments, we analyse most of the template protection schemes and settle on the one deemed suitable for such platform. Considering mobile platform constraints, we focus on bloom filter template protection schemes.

VII. Discussion

The purpose of this paper is to make privacy and security assessment of different biometric modalities on mobile platforms. In all of these assessments, we employ the advanced threat model. The modalities we looked at are fingerprint, face and iris. In this report, we measure the security and privacy protection capability of protected biometric templates on mobile platforms. We looked at the security and privacy issues of the selected biometric modalities before and after transformation of the biometric template.

Before transformation of the biometric template, we analyse the statistical properties of the selected biometric features. We carry out this by analysing the distributions of the intra-class and inter-class errors. The intra-class distributions measure the biometric features and their variability with regards to an individual. It helps to measure the error probability at every bit position. The inter-class distributions measure the variability of features across the whole dataset. It helps to analyse the discriminative power of the biometric features. By the various distributions, information of the biometric features is analysed using information theoretical metrics. We are thus able to calculate the number of bits in the biometric features that have discriminative entropy. We make use of mutual and conditional entropy in our assessment of protected biometric template. Thus, we are able to calculate entropy of the biometric template space prior and post template protection application.

As part of the assessment process we evaluate unlinkability of the protected biometric template in relation to cross matching and leakage amplification. This helps us to analyse the vulnerability of the template protection system regarding risks related to unlinkability. A principal criteria of template protection scheme is its impact on recognition performance of the biometric system. As a result, we analyse the recognition performance of the biometric system before and after application of the template protection scheme.

VIII. Conclusion

In this paper, we adapted security and privacy evaluation framework and applied to biometric template scheme, bloom filters in mobile environment. We then assess the security and privacy implications of the protected biometric template on such platforms. By that analyse the biometric template space and the biometric system performance.

We looked at three biometric modalities in fingerprint, iris, and facial recognition systems on mobile devices. We make an estimate of the probability distribution of fingerprint, facial and iris features and determine the correlation with the calculated entropy of respective features. In terms of security and irreversibility, we analyse size of the secret used in the template protection scheme. We look at its impact on the performance of security as well as privacy leakage. In the same vein, we estimate reliability and entropy of selected biometric features and its impact on security. To quantify security and privacy protection potential of the template protection scheme, we use metrics from the field of information theory.

REFERENCES

[1] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to biometrics*. Springer Science & Business Media, 2011.

[2] S. Egawa, A. I. Awad, and K. Baba, "Evaluation of acceleration algorithm for biometric identification," in *International Conference on Networked Digital Technologies*. Springer, 2012, pp. 231–242.

[3] A. I. Awad and A. E. Hassanien, "Impact of some biometric modalities on forensic science," in *Computational intelligence in digital forensics: Forensic investigation and applications*. Springer, 2014, pp. 47–62.

[4] C. M. Most, *ACUITY: Market Intelligence, Biometrics Market Development: MegaTrends and Meta*, 2007.

[5] B. Schouten and B. Jacobs, "Biometrics and their use in e-passports," *Image and Vision Computing*, vol. 27, no. 3, pp. 305–312, 2009, Special Issue on Multimodal Biometrics.

[6] D. Lowrence, "Biometrics and retail: moving towards the future," *Biometric Technology Today*, vol. 2014, no. 2, pp. 7–9, 2014.

[7] R. R. Jillela and A. Ross, "Segmenting iris images in the visible spectrum with applications in mobile biometrics," *Pattern Recognition Letters*, vol. 57, pp. 4–16, 2015.

[8] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, p. 113, 2008.

[9] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of biometrics*. Springer Science & Business Media, 2007.

[10] I. O. for Standardization, "ISO/IEC 27000:2016 - Information technology – Security techniques – Information security management systems – Overview and vocabulary." [Online]. Available: https://www.iso.org/standard/66435.html

[11] A. Adler and S. Schuckers, "Biometric vulnerabilities, overview," in *Encyclopedia of Biometrics*. Springer, 2009, pp. 160–168.

[12] C. Roberts, "Biometric attack vectors and defences," *Computers & Security*, vol. 26, no. 1, pp. 14–25, 2007.

[13] S. Vidalis, A. Jones *et al.*, "Using vulnerability trees for decision making in threat assessment," *University of Glamorgan, School of Computing, Tech. Rep. CS-03-2*, 2003.

[14] M. B. Salem, S. Hershkop, and S. J. Stolfo, "A survey of insider attack detection research," *Insider Attack and Cyber Security*, pp. 69–90, 2008.

[15] J. L. Wayman, "Technical testing and evaluation of biometric identification devices," in *Biometrics*. Springer, 1996, pp. 345–368.

[16] B. Cukic and N. Bartlow, "The vulnerabilities of biometric systems-an integrated look and old and new ideas," *West Virginia University, Tech. Rep*, 2005.

[17] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *International Conference on Audio-and Video-Based Biometric Person Authentication*. Springer, 2001, pp. 223–228.

[18] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 88–100, 2015.

[19] www.statista.com, "global digital population 2018 statistic." [Online]. Available: https://www.statista.com/statistics/617136/digital-population-worldwide/

[20] "Fingerprint scanner on Phones: History and Evolution, but do we really need that? | iGadgetsworld," Apr. 2016. [Online]. Available: https://www.igadgetsworld.com/fingerprint-scanner-history-evolution-but-do-we-really-need-that/

[21] "Two in five shoppers use their phones to pay in store, url = https://mobileecosystemforum.com/2017/01/30/two-in-five-shoppers-use-their-phones-to-pay-in-store/, language = en-GB, urldate = 2018-11-23, journal = MEF, month = jan, year = 2017."

[22] "Press Releases & News | Kaspersky Lab," 2016. [Online]. Available: https://www.kaspersky.com/about/press-releases/2016_mobile-devices-become-a-new-target-for-spam-and-malware-attacks

[23] A. K. Jain and D. Shanbhag, "Addressing security and privacy risks in mobile applications," *IT Professional*, vol. 14, no. 5, pp. 28–33, 2012.

[24] GReAT, "IT threat evolution Q1 2017. Statistics," *Securelist - Information about Viruses, Hackers and Spam*, 2017. [Online]. Available: https://securelist.com/it-threat-evolution-q1-2017-statistics/78475/

[25] T. Feng, X. Zhao, B. Carbunar, and W. Shi, "Continuous mobile authentication using virtual key typing biometrics," in *Trust, security and privacy in computing and communications (TrustCom), 2013 12th IEEE international conference on*. IEEE, 2013, pp. 1547–1552.

[26] C. Beek *et al.*, "Mcafee labs threats report," *McAfee, Santa Clara, CA, USA, Tech. Rep*, 2017.

[27] Y. Kaga, Y. Matsuda, K. Takahashi, and A. Nagasaka, "Biometric authentication platform for a safe, secure, and convenient society," *Hitachi Review*, vol. 64, no. 8, p. 473, 2015.

[28] J. W. DeCew, *In pursuit of privacy: Law, ethics, and the rise of technology*. Cornell University Press, 1997.

[29] D. J. Solove, "A taxonomy of privacy," *U. Pa. L. Rev.*, vol. 154, p. 477, 2005.

[30] M. Gao, X. Hu, B. Cao, and D. Li, "Fingerprint sensors in mobile devices," in *Industrial Electronics and Applications (ICIEA), 2014 IEEE 9th Conference on*. IEEE, 2014, pp. 1437–1440.

[31] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.

[32] S. Orandi, *Mobile ID Device Best Practice Recommendation, Version 1. 0*. DIANE Publishing, 2010, vol. 500, no. 280.

[33] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE transactions on pattern analysis and machine intelligence*, vol. 15, no. 11, pp. 1148–1161, 1993.

[34] A. Radman, K. Jumari, and N. Zainal, "Fast and reliable iris segmentation algorithm," *IET Image Processing*, vol. 7, no. 1, pp. 42–49, 2013.

[35] P. V. Hough, "Method and means for recognizing complex patterns," Dec. 18 1962, uS Patent 3,069,654.

[36] R. P. Wildes, "Iris recognition: an emerging biometric technology," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1348–1363, 1997.

[37] M. Kass, A. Witkin, and D. Terzopoulos, "Snakes: Active contour models," *International journal of computer vision*, vol. 1, no. 4, pp. 321–331, 1988.

[38] N. Ritter, R. Owens, J. Cooper, and P. P. Van Saarloos, "Location of the pupil-iris border in slit-lamp images of the cornea," in *Image Analysis and Processing, 1999. Proceedings. International Conference on*. IEEE, 1999, pp. 740–745.

[39] E. M. Arvacheh and H. R. Tizhoosh, "Iris segmentation: Detecting pupil, limbus and eyelids," in *Image Processing, 2006 IEEE International Conference on*. IEEE, 2006, pp. 2453–2456.

[40] J. Daugman, "New methods in iris recognition," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 37, no. 5, pp. 1167–1175, 2007.

[41] V. Caselles, R. Kimmel, and G. Sapiro, "Geodesic active contours," *International journal of computer vision*, vol. 22, no. 1, pp. 61–79, 1997.

[42] S. Shah and A. Ross, "Iris segmentation using geodesic active contours," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 4, pp. 824–836, 2009.

[43] S. Beucher, "Use of watersheds in contour detection," in *Proceedings of the International Workshop on Image Processing*. CCETT, 1979.

[44] F. Meyer and S. Beucher, "Morphological segmentation," *Journal of visual communication and image representation*, vol. 1, no. 1, pp. 21–46, 1990.

[45] A. F. Abate, M. Frucci, C. Galdi, and D. Riccio, "Bird: Watershed based iris detection for mobile devices," *Pattern Recognition Letters*, vol. 57, pp. 43–51, 2015.

[46] M. Frucci, M. Nappi, D. Riccio, and G. S. di Baja, "Wire: Watershed based iris recognition," *Pattern Recognition*, vol. 52, pp. 148–159, 2016.

[47] T. Tan, Z. He, and Z. Sun, "Efficient and robust segmentation of noisy iris images for non-cooperative iris recognition," *Image and vision computing*, vol. 28, no. 2, pp. 223–230, 2010.

[48] H. Patel, C. K. Modi, M. C. Paunwala, and S. Patnaik, "Human identification by partial iris segmentation using pupil circle growing based on binary integrated edge intensity curve," in *Communication Systems and Network Technologies (CSNT), 2011 International Conference on*. IEEE, 2011, pp. 333–338.

[49] K. B. Raja, R. Raghavendra, V. K. Vemuri, and C. Busch, "Smartphone based visible iris recognition using deep sparse filtering," *Pattern Recognition Letters*, vol. 57, pp. 33–42, 2015.

[50] A. Gangwar and A. Joshi, "Deepirisnet: Deep iris representation with applications in iris recognition and cross-sensor iris recognition," in *Image Processing (ICIP), 2016 IEEE International Conference on*. IEEE, 2016, pp. 2301–2305.

[51] N. Liu, H. Li, M. Zhang, J. Liu, Z. Sun, and T. Tan, "Accurate iris segmentation in non-cooperative environments using fully convolutional networks," in *Biometrics (ICB), 2016 International Conference on*. IEEE, 2016, pp. 1–8.

[52] M. Fairhurst, M. Erbilek, and M. Da Costa-Abreu, "Selective review and analysis of aging effects in biometric system implementation," *IEEE transactions on human-machine systems*, vol. 45, no. 3, pp. 294–303, 2015.

[53] U. Uludag, A. Ross, and A. Jain, "Biometric template selection and update: a case study in fingerprints," *Pattern recognition*, vol. 37, no. 7, pp. 1533–1542, 2004.

[54] T. Scheidat, A. Makrushin, and C. Vielhauer, "Automatic template update strategies for biometrics," *Otto-von-Guericke University of Magdeburg, Magdeburg, Germany*, 2007.

[55] N. Poh, J. Kittler, S. Marcel, D. Matrouf, and J.-F. Bonastre, "Model and score adaptation for biometric systems: Coping with device interoperability and changing acquisition conditions," in *2010 20th International Conference on Pattern Recognition*. IEEE, 2010, pp. 1229–1232.

[56] A. Rattani, B. Freni, G. L. Marcialis, and F. Roli, "Template update methods in adaptive biometric systems: A critical review," in *International Conference on Biometrics*. Springer, 2009, pp. 847–856.

[57] R. Savola, "Information security evaluation based on requirements, metrics and evidence information," in *Proceedings of the 6th Annual Security Conference*, 2007.

[58] X. Zhou, "Privacy and security assessment of biometric template protection," *it-Information Technology Methoden und innovative Anwendungen der Informatik und Informationstechnik*, vol. 54, no. 4, pp. 197–200, 2012.

[59] I. O. for Standardization, "ISO/IEC 24745:2011 - information technology - security techniques - biometric information protection." [Online]. Available: https://www.iso.org/standard/52946.html