Framework for the Telebiometric Systems using Mobile Biometrics

Yong-Nyuo Shin

Dept.of Computer Engineering, Hanyang Cyber University
ynshin@hycu.ac.kr

Abstract

This paper is designed to provide a framework to ensure security and reliability of the flow of biometric information for telebiometric applications using mobile devices. Also, we define twelve telebiometrics authentication models depending on the configuration of the biometric sensor, the mobile device, and the server. It also specifies threat in operating telebiometric systems based on the mobile device and proposes a general guideline for security countermeasures from both technical and managerial perspectives in order to establish a safe mobile environment for the use of telebiometric systems.

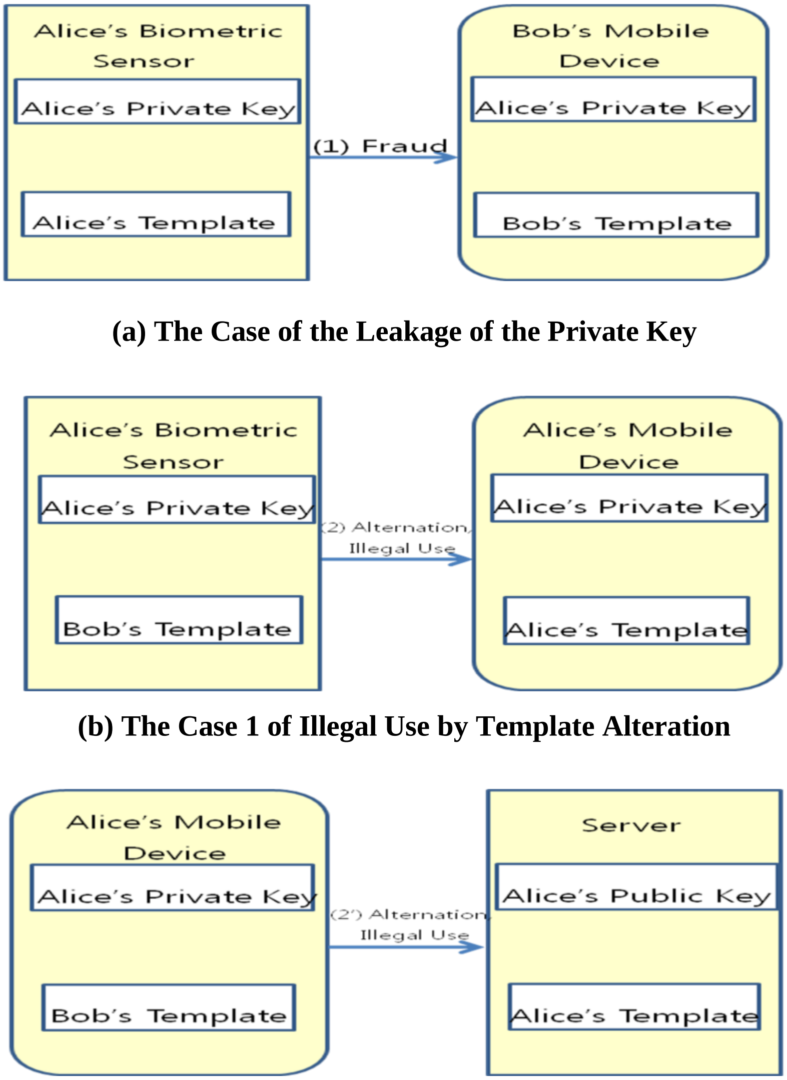
Keywords: *Telebiometric, Mobile device, Biometrics, Threat, Vulnerability*

1. Introduction

To service the demand mobile communications and transactions need to be protected in order to safeguard personal privacy. Identity authentication is a vital part of this and biometric authentication can provide assurance that the person is who they insist they are rather better than other forms of authentication such as passwords and tokens because biometric characteristics are linked or bound more closely to the person than the passwords and tokens[1-2]. Also, biometric handles the sensitive personally identifiable information (PII), some of privacy issues for biometric in the mobile device should be considered [7]. To provide a telebiometric framework to ensure security using mobile devices, we provide the 12 telebiometric authentication models. The range of mobile devices and communication channels involved in mobile transactions is large and variable. Smartphones, tablets and laptops are common examples of mobile devices and the internet and wireless are examples of communication channels. This paper cover the threats in operating telebiometric systems based on the mobile device and guideline for security countermeasures from both technical and managerial perspectives in order to establish a safe mobile environment for the use of telebiometric systems. Chapter 2 explains the environment of the telebiometirc applications using mobile devices. Chapter 3 specifies the security threats allowing illegal use by an unauthorized user and possible counter measures for each model. Finally, a conclusion is drawn and future study tasks are reviewed.

2. Environment for the telebiometric applications using mobile devices

Figure 1 illustrates specific threats for cooperation of PKI, and a biometric authentication, such as the environment of this paper. For a model that incorporates PKI, there remains the threat of a private key leaking out, and that somebody may uses it illegally, such as case (a). Even without private key leakages, such as case (b), relation between PKI information and biometric template information may not be guaranteed. Therefore, the biometric template information should require the identifying information of the PKI Certificate and the validity information for itself. This paper assumes the use of a Biometric Certificate (BC) of [ITU-T X.1089] as the biometric template.



(a) The Case of the Leakage of the Private Key

(b) The Case 1 of Illegal Use by Template Alteration

(c) The Case 2 of Illegal Use by Template Alteration

Figure 1. Risk of illegal use by falsification of the template

Vulnerabilities mean weakness of mobile devices and their inabilities to withstand hostile environment effects. Attacks are any attempts to intentional destroy, unauthorized use, malicious modify or illegally obtain mobile devices assets. In other words, vulnerabilities are the internal attributes of mobile devices, while attacks are the external offensive activities to mobile devices. Telebiometric security reference models in operating telebiometric systems using a mobile device including cloud computing and big data environment. The environment of the telebiometirc applications using mobile devices is depicted in Figure 2.

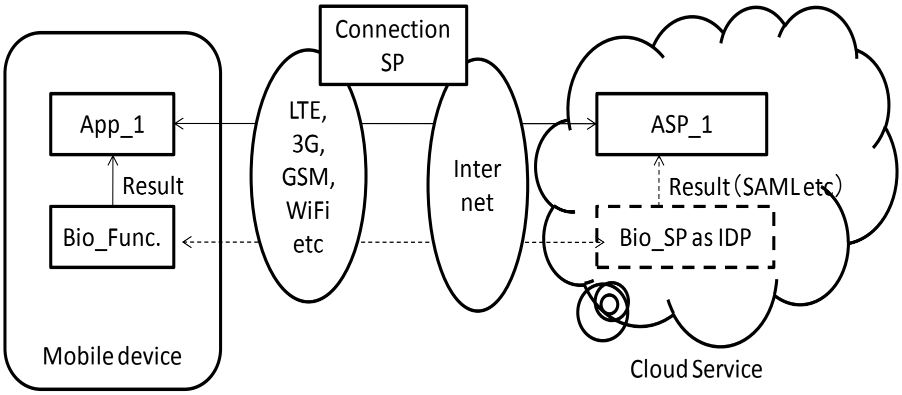


Figure 2. Environment of the telebiometirc applications using mobile devices

3. Authentication Models

In this paper, we takes into account of the three perspectives below, dividing models into eleven categories

3.1. Model 1

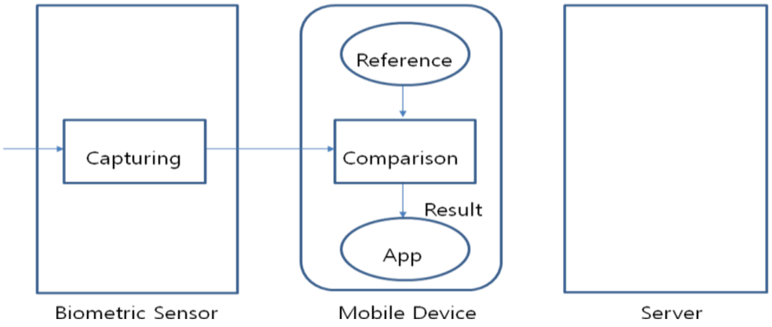


Figure 3. Model 1

The mobile device takes the request from the App; it acquires sample data, compares it with the registered user's template, and transfers the result to the App. Template ID information is required, which is the comparison result. For the model1, we assume the mobile device has a difficult situation to telecommunicate with server including wireless environment and the mobile device-side is given sufficient processing resources such as smartphones. (The processing resources must be sufficient to acquire sample data and compare). External biometric sensor communicates with the mobile device using Near Field Communication when the mobile device cannot bear the sensor because of a characteristic of a modality or applicability. This model can be used when the server side trusts the mobile device-side processing procedures.

3.2. Model 2

The App requests of verification to the server. The server sends the registered user's template. It compares the acquired sample data with the received template, sending the result to the App. The model 2 has the same sequence as the model1, excluding the transfer template from the server. Template ID information is required. This then forms the comparison result. Under this structure, it is practical to use many terminals. This is suitable for the web-verification model, as users can connect to the server from any mobile device. This model 2 requires registration of the biometric reference template to the server. This model also requires the server to trust the mobile device processing procedure.

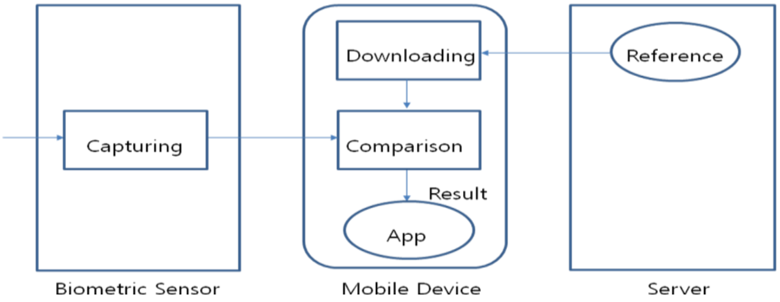


Figure 4. Model 2

3.3. Model 3

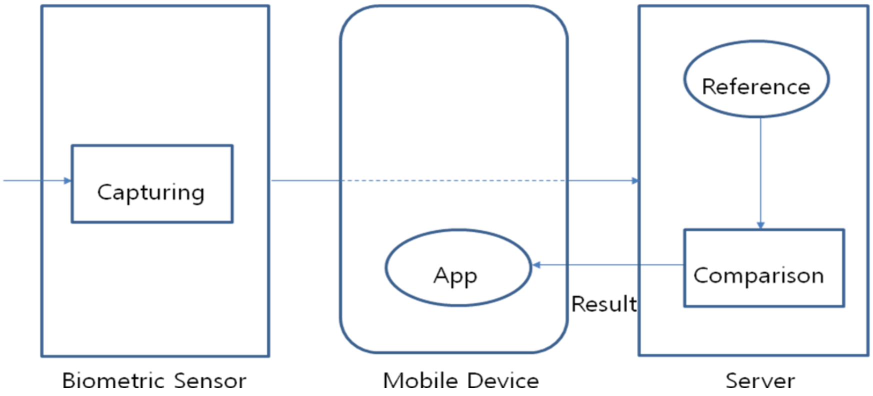


Figure 5. Model 3

The server requests the sample data required for verification, the biometric sensor acquires sample data and transfers it to the server through the mobile device, and the server finally compares it with the user’s template. For the model 3, we assume the mobile device-side cannot guarantee sufficient resources in terms of processing power, memory, security etc. That is the reason mobile device is used for only telecommunication methods. External biometric sensor communicates with the mobile device using Near Field Communication when the mobile device cannot bear the sensor because of a characteristic of a modality or applicability. The user registers their biometric reference in advance with a server that has a trusted biometric reference template. This model requires that the server trusts the data captured from a biometric sensor.

3.4. Model 4

The App requests verification, the biometric sensor acquires sample data, and requests the user’s template to server. Then the biometric sensor compares the template which is transferred from server with the captured sample data, and transfers the result data to the mobile device. In this model, a biometric sensor could be a hardware security module. They are physical devices that traditionally come in the form of smartcard or some other USB type security token that can provide tamper proof against penetration or modification of an internal operation and/or insertion of active or passive tapping mechanism to disclosure secret data or to alter the operation of devices. For the model 4, we assume the mobile device-side cannot guarantee sufficient resources in terms of processing power, memory, security etc. That is the reason mobile device is used for only telecommunication methods.

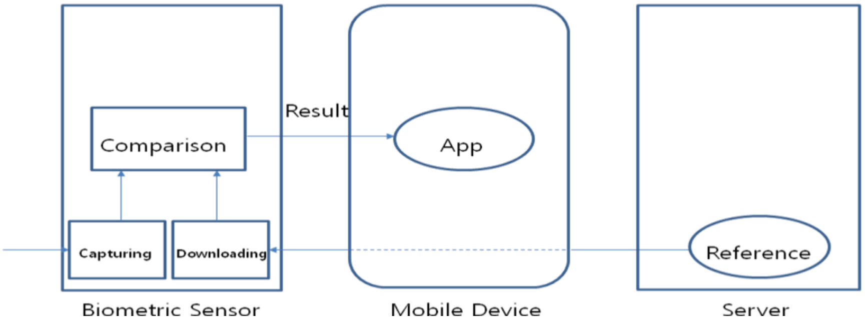


Figure 6. Model 4

3.5. Model 5

Figure 7 illustrates a model 5. The biometric sensor compares the template which is transferred from server with the captured sample data, and transfers the result data to the mobile device. The model5 has the same sequence as the model4, excluding the transfer template from the mobile device. In this model, a biometric sensor could be a hardware security module. For the model5, we assume the mobile device has a difficult situation to telecommunicate with server including wireless environment.

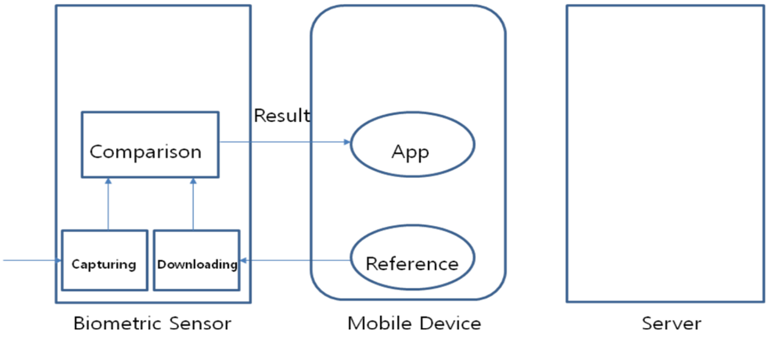


Figure 7. Model 5

3.6. Model 6

Figure 8 illustrates a model 6. The biometric sensor takes the request from the App; it acquires sample data, compares it with the registered user’s template, and transfers the result to the App. Template ID information is required, which is the comparison result. External biometric sensor communicates with the mobile device using Near Field Communication when the mobile device cannot bear the sensor because of a characteristic of a modality or applicability. In this model, a biometric sensor could be a hardware security module. They are physical devices that traditionally come in the form of smartcard or some other USB type security token that can provide tamper proof against penetration or modification of an internal operation and/or insertion of active or passive tapping mechanism to disclosure secret data or to alter the operation of devices. For the model6, we assume the mobile device-side cannot guarantee security. This is practical when put to use for national infrastructure systems that need for a high level of security.

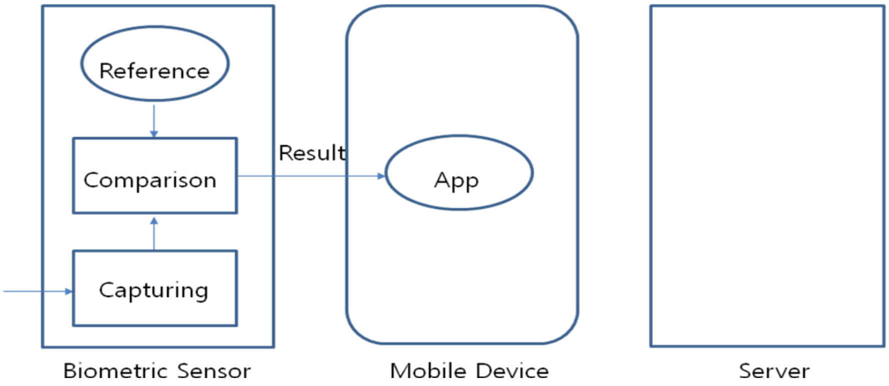


Figure 8. Model 6

3.7. Model 7

The mobile device requires the comparison function, which is needed for template and captured sample data. The biometric sensor transfers the acquired sample data and template to the mobile device, and the comparison is ultimately conducted within the mobile device. The mobile device trusts biometric sensor capture-data. This is practical for use in credit authorization systems, as a comparison algorithm is not required for the biometric sensor.

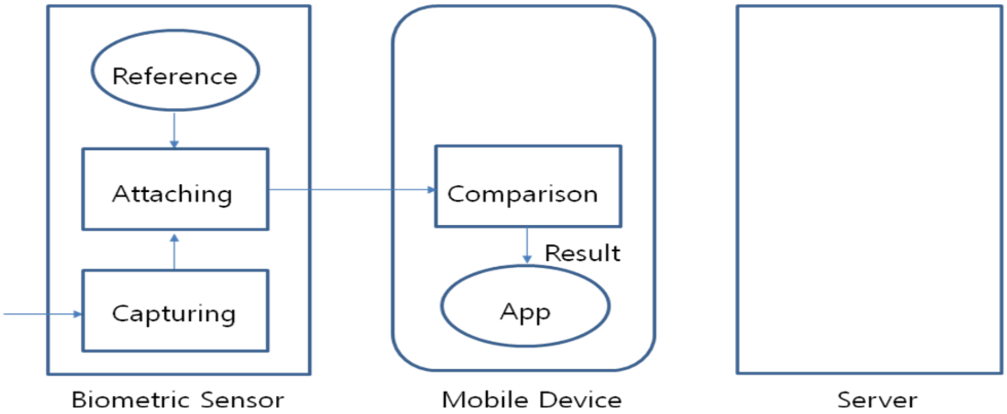


Figure 9. Model 7

3.8. Model 8

The biometric sensor takes the request from the App; it acquires sample data. The model8 has the same sequence as the model 7, excluding the comparison location.

The biometric sensor transfers the acquired sample data and template to the server through the mobile device, and the comparison is ultimately conducted within the server. The mobile device is used for only telecommunication methods. This model requires that the server trusts the data captured from a biometric sensor.

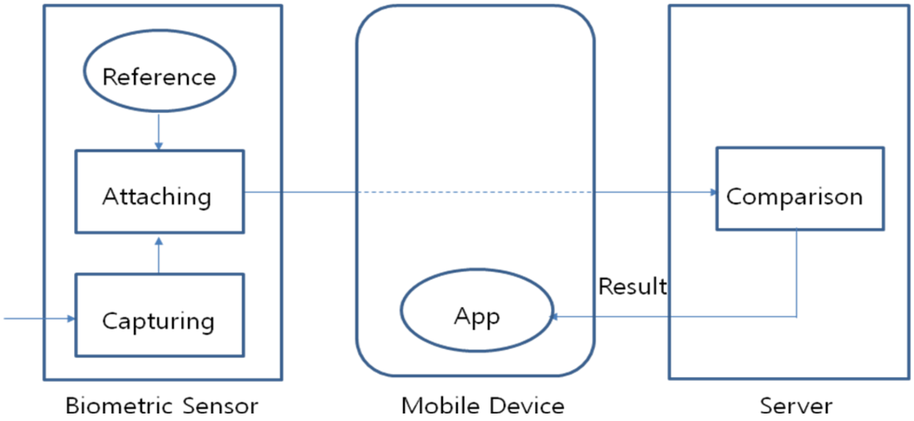


Figure 10. Model 8

3.9. Model 9

The server requests the sample data required for verification, the biometric sensor acquires sample data and transfers it to the server through the mobile device, and the server finally compares it with the user's template. This model requires that the server trusts the data captured from a biometric sensor.

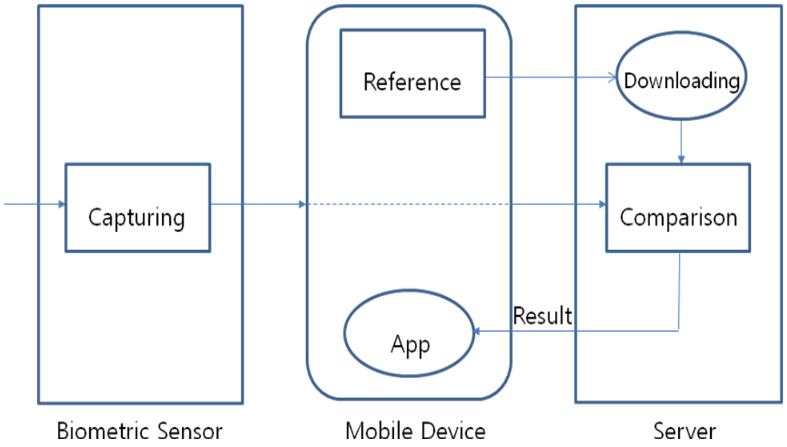


Figure 11. Model 9

3.10. Model 10

The mobile device acquires sample data, compares it with the registered user's template, and transfers the result to the App in the mobile device. Template ID information is required, which is the comparison result. For the model 10, we assume the mobile device can bear the biometric-processing load, and it is given sufficient processing resources (The processing resources must be sufficient to acquire sample data and compare).

3.11. Model 11

For this model, we assume that mobile device resources, (memory, disk etc.), are insufficient. The App requests verification from the mobile device. The mobile device captures the sample data, and requests verification result from a server with the captured sample data. Therefore, the server compares sample data with the registered user's template, and transfers the result to the App. A user registers their biometric reference template in advance with a server. Template ID information is required in the comparison result.

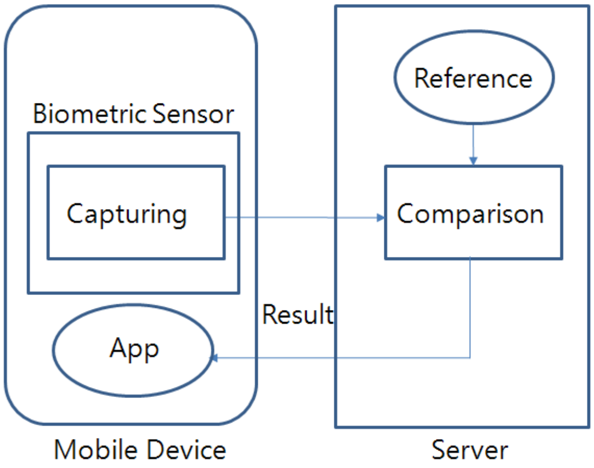


Figure 12. Model 11

3.12. Model 12

The model12 has the same sequence as the model10, excluding the transfer template from the server. Template ID information is required, which is the comparison result. For the model 12, we assume the mobile device can bear the biometric-processing load, and it is given sufficient processing resources (The processing resources must be sufficient to acquire sample data and compare).

4. Security threats for each models

Table 1 shows security threats allowing illegal use by an unauthorized user and possible counter measures for each model.

Table 1. Security threats and countermeasures

Model	Threats allowing illegal use by unauthorized users	Possible countermeasures
Model1	− They may replace illegal capture data, such as stolen or altered data − They may use an illegal biometric reference template data − They may use an illegal comparison program − Template can be leaked through the loss of the mobile devices	− Mutual authentication between sensor and mobile device − Encryption for the reference data
Model2	− They may replace illegal capture data, such as stolen or altered data − They may alter illegally when the captured data is transfered − They may use an illegal biometric reference template	- Authentication for the sensor, mobile device and server Ex. Process key generation and digital signature generation inside of the USIM card, when encryption operation is performed.

Model	Threats allowing illegal use by unauthorized users	Possible countermeasures
	data − They may use an illegal comparison program − Leakage for the reference − They may transfer data to illegal server − Template can be leaked through the loss of the mobile deviceTemplate is leaked by having a central server lost or stolen	− Encryption for the transmission channel − Encryption for the reference data − Encryption for the transmission channel
Model3	− They may replace illegal capture data, such as stolen or altered data − They may alter illegally when the captured data is transfered − They may attack the transmission channels − They may transfer data to illegal server − Template is leaked by having a central server lost or stolen	− Authentication for the sensor and server Encryption for the transmission channel − Encryption for the transferred data
Model4	− They may replace illegal capture data, such as stolen or altered data − They may use an illegal biometric reference template data − They may use an illegal comparison program − Template is leaked by having a sensor lost or stolen − They may attack the transmission channels − Template is leaked by having a central server lost or stolen	− Authentication for the sensor and server Encryption for the reference data − Encryption for the transmission channel − Encryption for the transferred data
Model5	− They may replace illegal capture data, such as stolen or altered data − They may use an illegal biometric reference template data − − They may use an illegal comparison program − Template is leaked by having a sensor lost or stolen	− Authentication for the sensor and mobile device − Encryption for the reference data
Model6	− They may replace illegal capture data, such as stolen or altered data − They may use an illegal biometric reference template data − They may use an illegal comparison program − Template is leaked by having a sensor lost or stolen	− Encryption for the reference data
Model 7	− They may replace illegal capture data, such as stolen or altered data − They may alter illegally when the captured data is transfered − They may use an illegal biometric reference template data − They may use an illegal comparison program − Template can be leaked through the loss of the mobile	− Authentication for the sensor and mobile device − Encryption for the reference data

Model	Threats allowing illegal use by unauthorized users	Possible countermeasures
	device	
Model8	− They may replace illegal capture data, such as stolen or altered data − They may alter illegally when the captured data is transfered − They may attack the transmission channels − They may transfer data to illegal server	− Authentication for the sensor and server − Encryption for the transmission channel
Model9	− Misuse for the sensor (Irrelevant App use the sensor) − Irrelevant App attacks the sensor such as man-in-the-middle-attack, so irrelevant App use the captured data − They may use an illegal biometric reference template data − They may use an illegal comparison program − Template can be leaked through the loss of the mobile device	− Authentication for the sensor and App Encryption for the reference data
Model10	− Misuse for the sensor (Irrelevant App use the sensor) − Irrelevant App attacks the sensor such as man-in-the-middle-attack, so irrelevant App use the captured data − They may attack the transmission channels − They may transfer data to illegal server − Template is leaked by having a central server lost or stolen	− Authentication for the sensor and App Authentication for the App and server − Encryption for the transmission channel − Encryption for the transferred data
Model11	− Misuse for the sensor (Irrelevant App use the sensor)) − Irrelevant App attacks the sensor such as man-in-the-middle-attack, so irrelevant App use the captured data − − They may use an illegal biometric reference template data − They may use an illegal comparison program − Template can be leaked through the loss of the mobile deviceThey may attack the transmission channels − They may transfer data to illegal server − Template is leaked by having a central server lost or stolen	− Authentication for the sensor and App Authentication for the App and server − Encryption for the reference data − Encryption for the transmission channel − Encryption for the transferred data
Model12	− Misuse for the sensor (Irrelevant App use the sensor) − Irrelevant App attacks the sensor such as man-in-the-middle-attack, so irrelevant App use the captured data − They may attack the transmission channels − They may transfer data to illegal server	− Authentication for the sensor and App Authentication for the App and server − Encryption for the transmission channel

5. Conclusion

To define the framework for the telebiometrics system using mobile devices, the basic component are needed such as capture of a biometric sample, storage of a biometric reference and comparison of a biometric sample with a biometric reference. For the respective three components, we categorized twelve telebiometrics authentication models depending on the configuration of the biometric sensor, the mobile device, and the server. It also specifies threat in operating telebiometric systems based on the mobile device and proposes a general guideline for security countermeasures from both technical and managerial perspectives in order to establish a safe mobile environment for the use of telebiometric systems. Possible threats to private information protection on a sensor, mobile device or with a trusted server are listed such as biometric and private information fraud through an illegal sensor, mobile device, server and network. Counter measures are listed such as authenticate a sensor, mobile device and trusted server using the PKI [6]. Encrypt the session key exchange by use of TLS protocol as specified in IETF RFC 4346. Future work will specify more detailed threats for cooperation of PKI, and a biometric authentication. Also we plan to standardize on this topic in ITU-T SG17 Q.9.

References

[1] Why Apple really bought AuthenTec: It wanted “new technology” for upcoming products, and quickly, http://thenextweb.com/apple/2012/08/16/the-real-reason-apple-acquired-authentec-because-needed-new-technology-quickly-products/ **(2012)**.

[2] M. Soltane, N. Doghmane and N. Guersis, “Face and Speech Based Multi-Modal Biometric Authentication”, IJAST, vol. 21, **(2010)**, pp. 41-56.

[3] M. Soltane and M. Bakhti, “Multi-Modal Biometric Authentications: Concept Issues and Applications Strategies”, IJAST, vol. 48, **(2004)**, pp.23-60.

[4] R. Sharanabasappa and M. B. Sanjaypande, “A Unique Document Security Technique using Face Biometric Template”, IJAST, vol. 50, **(2013)** January, pp. 23-40.

[5] J. Claessens, V. Dem and J. Vandewalee, “On the security of Today’s Online Electronic Banking Systems”, Computers & Security, Elsevier advanced Technology, vol. 21, no. 3, **(2002)**, pp. 257-269.

[6] Y. -N. Shin and W. C. Shin, “A Security Reference Model for the Construction of Mobile Banking Services based on the SmartPhone”, International Journal of Fuzzy Logic and Intelligent Systems, vol. 11, no. 4, **(2011)**, pp. 229-237.

[7] Y. -N. Shin, “Standard Implementation for Privacy Framework and Privacy Reference Architecture for Protecting Personally Identifiable Information”, International Journal of Fuzzy Logic and Intelligent Systems, vol. 11, no. 3, **(2011)**, pp. 197-203.

Author

Yong-Nyuo Shin received her PhD degree in computer science from Korea University in 2008, Republic of Korea. Currently, she is a professor at Department of Computer Science, Hangyang Cyber University. Also, she is an editor for efforts and continued support in progressing the many standardizations such as ITU-T SG17, ISO/IEC JTC1 SC27 and SC37. Her current research interests are telebiometrics, authentication technologies and privacy.