Enhanced Authentication for Self-organizing Software platform using Smart SSD

Im Y. Jung, Gil-Jin Jang, Jung-Min Yang

School of Electronics Engineering, Kyungpook National University, Republic of Korea
iyjung@ee.knu.ac.kr, gjang@knu.ac.kr, jmyang@ee.knu.ac.kr

Abstract: This paper proposes an enhanced biometric authentication using Smart SSD. In addition to data storing, almost all data processing, including feature extraction and feature matching, is performed in Smart SSD. Therefore, biometric authentication can be secure and efficient without biometric data leakage.

[Jung I, Jang GJ, Yang JM. **Enhanced Authentication for Self-organizing Software platform using Smart SSD**. *Life Sci J* 2014;11(7):582-587] (ISSN:1097-8135). http://www.lifesciencesite.com. 80

Keywords: Biometric Authentication; Security Enhancement; Smart SSD; Self-organizing Software platform

1. Introduction

Research into biometrics has led to the advent of biometric authentication, which refers to the identification of humans on the basis of their characteristics or traits [1]. For the same level of security, biometrics is preferred to passwords on account of user convenience alone [2].

The development of information systems and the Internet has engendered an apprehension of information leakage. Moreover, because of the rapid dissemination of information systems and the expansion of their functionalities, there is a possibility for the data collected for a certain purpose to be utilized differently than originally intended. For example, the keywords that users enter into a web search engine are often used for marketing. Biometric data can be utilized for genetics research, medical monitoring, ethnic categorization, as well as identification. There is a serious risk for discrimination based on what is measured from the human body [3].

On the other hand, Smart SSD is storage that is more advanced than Solid State Drive (SSD), with powerful Central Processing Units (CPUs) and Random Access Memory (RAM) where downloaded programs can be executed.

This paper addresses the security issue of biometric authentication and proposes an enhanced biometric authentication with Smart SSD on the Self-organizing Software platform (SoSp) [4]. One of the applications for SoSp is in health care services, especially for the elderly and patients. Health management on the SoSp domain requires convenient, easy, and secure authentication. Therefore, the proposed biometric authentication satisfies requirements with Smart SSD.

2. Biometric Authentication

Biometrics is the science of establishing or determining an identity based on the physiological or behavioral traits of an individual. These traits include fingerprints, facial features, iris, hand geometry, voice, signature, and more. In conjunction with traditional authentication schemes, biometrics is a potent tool for establishing identity [5].

The merits of Biometric Authentication are efficiency, convenience, improved access, and enhanced security. On the other hand, its limitations include unique identifiers, support of unwarranted surveillance, difficulty with storage, and questionable security. The security feature of Biometric Authentication is both an advantage and a disadvantage.

Protecting personal data and sensitive biometric information is critical and must be done in a convenient way.

2.1. Vulnerability of Biometric Authentication System

Figure 1 introduces a biometric system and shows the vulnerabilities found in the system.

In general, there are several modules for biometric authentication. The *sensor* acquires the raw biometric data in the form of an image, video, audio, or other signal. The *feature extractor* extracts a salient set of features for the acquired biometric signal. A template, the extracted feature set labeled with the user's identity, is stored in safe storage during user enrolment. The *matcher* compares the feature set extracted during authentication with the enrolled template(s) and generates match scores. The *decision module* processes these match scores in order to either determine or verify the identity of an individual.

Several attacks against biometric systems have been identified [2]. 1) Fake biometrics such as a fake fingerprint, a forged signature, or a facemask can be captured by the sensor. 2) Old digital biometric data acquired and stored illegally can be

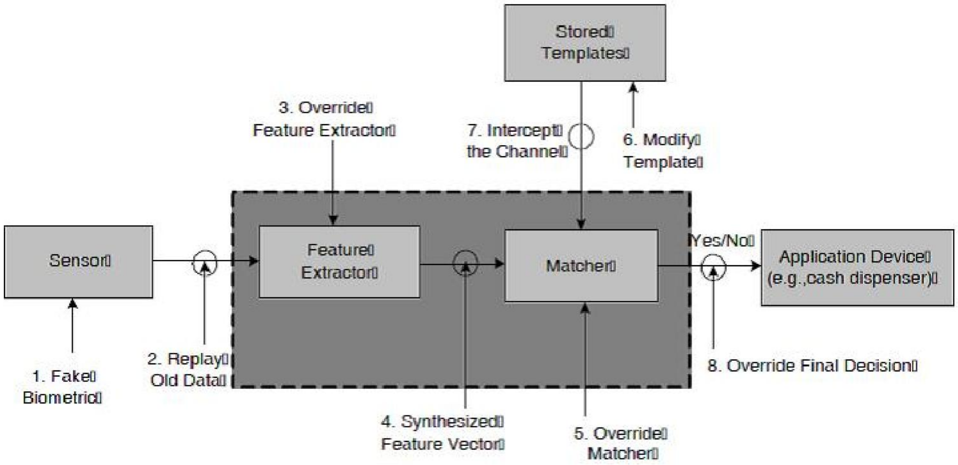

Figure 1. Vulnerabilities in a Biometric System (Adopted from [6])

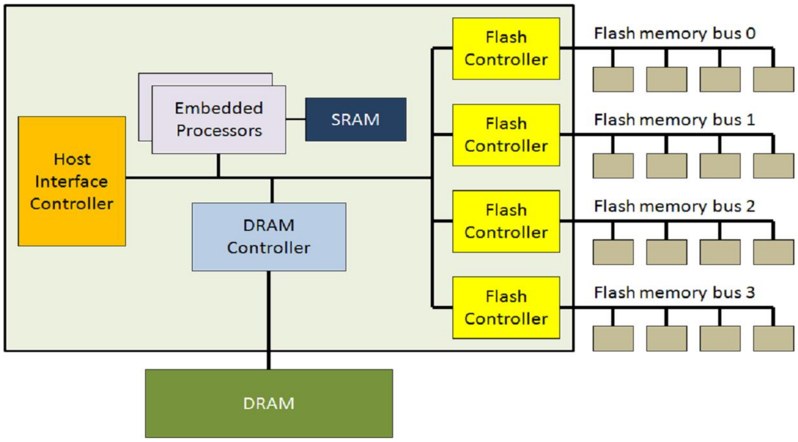

Figure 2. Modern SSD-Equipped Processors and RAM (Adopted from [7])

replayed. 3) A hacker might override the feature extractor with a Trojan horse program. 4) After features have been extracted from an input signal, they can be replaced with a different synthesized feature set. 5) The matcher can be replaced by a Trojan horse program that always produces an artificially high or low match score. 6) The stored templates can be modified such that they result in the authorization of a fraudulent individual. 7) The templates from the stored database can be sent to the matcher through a channel that could be attacked to change the template content before reaching the matcher. 8) A hacker can override the final result.

2.2. Enhanced Biometric Authentication on SoSp

There is a need for a scheme that enhances the security and addresses the drawbacks of biometric authentication.

This paper proposes enhanced biometric authentication that is related to health care applications on the SoSp domain. Self-organization is a process in which structure and functionality (pattern) at the global level of a system emerge solely from numerous interactions among the lower-level components of the system without any external or centralized control [8]. Because the SoSp network is the Internet of Things (IoT), SoSp combines Wellbeing Devices[1] with ubiquitous computing to

[1] Devices designed to automatically interact with the

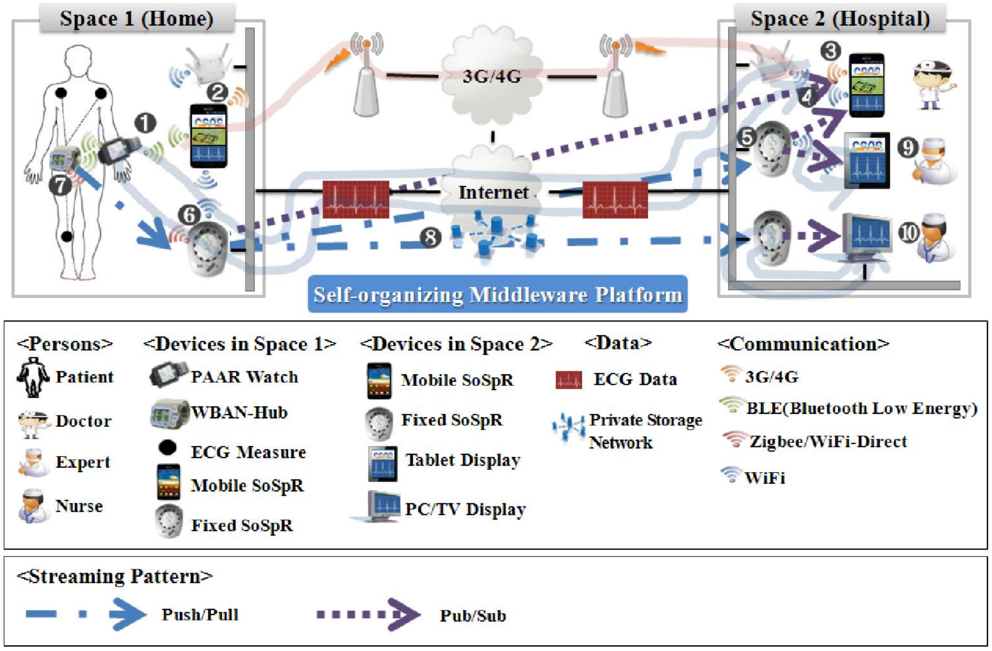

Figure 3. Health Care Application on SoSp [4]

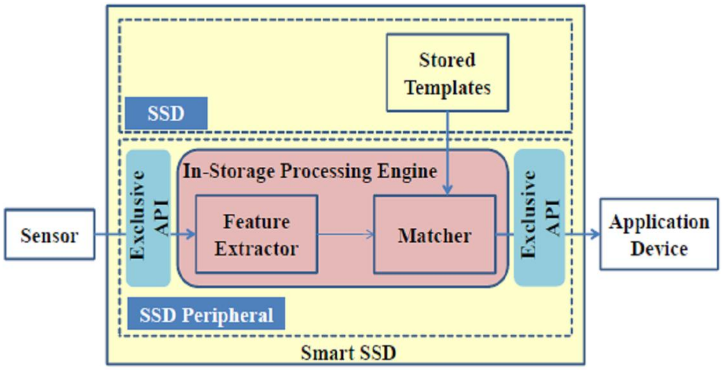

Figure 4. Architecture for Enhanced Biometric Authentication with Smart SSD

allow people to tend to their health easily regardless of location or time, and to cope with any emergencies.

Figure 3 shows a health care application on SoSp [4]. The emergency state of a person who wears a Personal Activity Assistance and Reminder (PAAR) watch and a Wireless Body Area Network (WBAN)-Hub is notified to the medical team or the family doctor pre-appointed by the emergency room (ER) button of the PAAR watch. Upon receiving the notification, the doctor requests an Electrocardiography (ECG) signal from the person via the WBAN-Hub. The ECG signal is displayed in real-time on a smartphone, tablet, or PC/TV through the streaming service installed on the SoSp domain. Usually, the patient's signal can be delivered to his/her doctor periodically. There are two types of core devices in SoSp, mobile SoSp-Router (SoSpR) and fixed SoSpR. As an identifiable node, SoSpR can communicate with other SoSpRs and provide many services. Fixed SoSpR attached on the ceiling or the wall of a unit space, communicates the things in the unit space.

Sensitive private data, such as biosignals or health information, should be stored securely and made accessible to authorized individuals only [15]. Therefore, the person sending such private data should be identified when his/her biosignal is acquired and accessed. The doctors who request and access the transmitted signals or any other health

physical environment. Examples are wearable healthcare and medical devices, watches, bicycles.

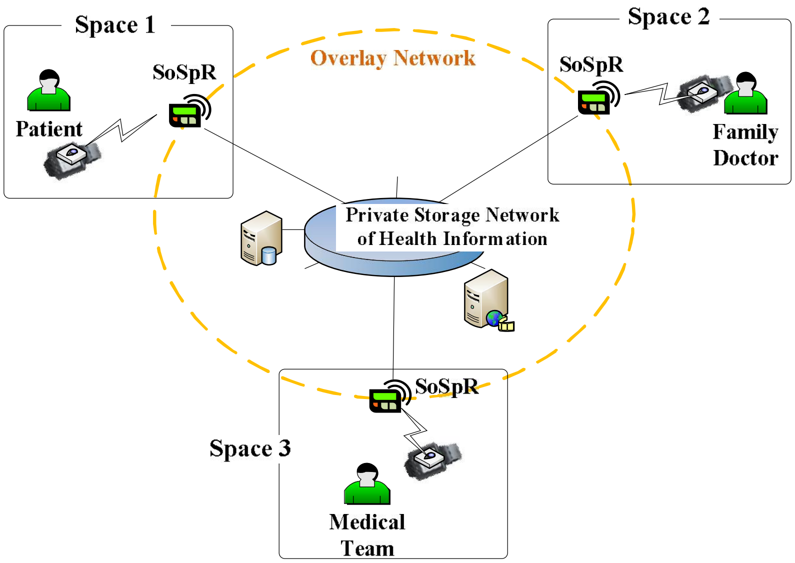

Figure 5. System Architecture for Health Care Services on SoSp Domain

information should be identified before they can process the signal.

Considering users, especially the elderly or patients, the authentication scheme should provide an easy interface to verify such users without the burden of managing smartcards or memorizing codes such as passwords. Biometric authentication provides easy user interface and unique identity verification of biometric recognition [9]. The biometric recognition devices, that is, sensors, can be equipped on the PAAR watch [4] that patients or doctors wear. Multiple biometric recognition devices can be equipped on one PAAR watch. Through the devices, biometric recognition information such as fingerprints, face, voice, iris, and so on can be acquired easily. Several biometric recognition schemes can be combined to improve the exactness of verification.

3. Why Smart SSD

SSD is large capacity storage that uses Negated AND (NAND) Flash Memory. Because SSD shows impressive performance compared with hard disk drives, it has received attention as cost-effective secondary storage. In addition to demonstrating high performance on concurrent random writes, modern SSDs have powerful processors, memory, and multiple input/output (I/O) channels for flash memory, enabling In-Storage Processing (ISP) [10] with almost no hardware changes. Figure 2 shows a modern SSD, also called Smart SSD because of ISP. In Smart SSDs, special-purpose computing modules can be deployed using System-on-Chip technology. This technology furthers energy conservation by reducing data transfer and by efficiently processing data [14].

In Figure 2, the host interface controller implements a bus interface protocol such as Serial Advanced Technology Attachment (SATA), Serial Attached SCSI[2] (SAS), or Peripheral Component Interconnect Express (PCIe). Typically, 32-bit Reduced Instruction Set Computing (RISC) processors such as the ARM series are used as embedded processors [10]. The flash controller (or Flash Memory Controller-FMC) ensures reliable data transfer between flash memory and Dynamic RAM (DRAM). NAND flash memory is composed of blocks, each of which consists of pages. A block is the unit of erase, whereas a page is the unit of read and write. Flash memory arrays typically have multiple channels, allowing for a high degree of parallelism.

The authentication module used for SoSp application needs to be protected securely. Smart SSDs can provide secure authentication with their embedded components and ISP.

4. Enhanced Biometric Authentication using Smart SSD on SoSp domain

This section describes the software (SW) architecture and the Application Program Interface (API) definition of the proposed biometric authentication with Smart SSD.

[2] Small Computer System Interface

4.1. SW Architecture

Biometric authentication is executed on the PAAR watch worn by patients (including the elderly) or appointed doctors. Biometric signatures for authentication are acquired via the equipment or the sensor installed in the PAAR watch. Biometric authentication can be performed on other devices with Smart SSD, apart from the PAAR watch.

Figure 4 shows the architecture for the enhanced biometric authentication with Smart SSD. In Figure 4, almost all the vulnerabilities of the biometric system described in Figure 1 can be addressed because Smart SSD accommodates data processing such as feature extraction and matching for biometric authentication and biometric data. Because only exclusive APIs are exposed, direct access to the original biometric data and the intermediate processed data, such as extracted features, is blocked. Direct access to the modules in the biometric system is also blocked. Because ISP can reduce data transfer, biometric authentication can be fast and efficient. Attacks such as fake biometrics and overridden final decisions cannot be addressed with the proposed scheme (points 1 and 8 of the types of attacks listed in Section 2.1 and Figure 1). However, because the equipment required for obtaining biometric features is usually installed on private devices such as the PAAR watch on the SoSp domain, the risk of attacks is significantly reduced.

4.2. API Definition

The exclusive essential APIs that are exposed are two.

- Get_Feature()
  The biometric feature acquired by the sensor or the equipment installed in the PAAR watch is transmitted to the Smart SSD.
- Send_Result()
  The final decision of biometric authentication by the matcher is sent from the Smart SSD.

Additional APIs might include those of error handling and fault management during the biometric authentication process.

4.3 Authentication on SoSp domain

Authentication for health care applications on the SoSp domain means that sensitive data from health care applications are protected, and the person using the application is identified. Secure authentication is of utmost importance for this type of application because such authentication is the first obstacle to using the application and accessing the data.

Figure 5 shows the system architecture for health care services on the SoSp domain. After the user is authenticated via the biometric sensor installed on the PAAR watch that he/she wears, he/she can use the health care services on the SoSp domain. Because biometric authentication is easy, fast, and secure with Smart SSDs, it is appropriate for the SoSp domain. The SoSp domain has the same security problems of the wireless domain constructed on overlay networks, such as secure authentication, secure communication, secure data access, low overhead, and lightweight schemes. In this paper, the issue of secure and lightweight authentication is studied. However, the degree of exactness and error rate of the biometric authentication itself is not considered.

5. Contribution

The contributions of the proposed biometric authentication with Smart SSD are as follows.

- Biometric authentication with easy interface is provided for disabled users of health care services via the SoSp domain.
- Secure authentication is ensured with Smart SSD. The ISP of Smart SSD functions as a defense against the attacks described in Figure 1.
- The proposed scheme is practical because it is simple and lightweight without special requirements. The scheme depends solely on the ISP, one characteristic of Smart SSDs. The development of Smart SSD is underway, and compact sized Smart SSD will be launched in the market shortly.

6. Related Works

There are several studies on biometric system security. Attacks that consist of a replay of old data were addressed for authentication with face recognition [11]. A study devised a Synthetic Template Generator (STG) to prevent the synthesized feature vector attack [12]. A masquerade attack wherein the fingerprint structure is determined using the minutiae template alone was addressed [13]. A technique was introduced to elicit the fingerprint structure from the minutiae template. These studies are relevant to the channel intercept attack shown in Figure 1. Most attacks described in Figure 1 occur because components of the biometric system are distant and need to communicate via certain exposed paths. The proposed scheme with Smart SSD solves this problem.

To the best of our knowledge, there is no research on SoSp security, especially on biometric systems on SoSp with Smart SSD.

7. Conclusion and Future Works

This paper proposes an enhanced biometric authentication with Smart SSD on the SoSp domain. In addition to data storing, almost all data processing, including feature extraction and matching, is performed in Smart SSD. In addition, biometric authentication is one of the easier authentications for users because users are not required to memorize secret codes or patterns. Because health care applications on the SoSp are directed mainly to patients, the elderly, or the disabled, an easy human interface should be provided. At this point, biometric authentication can be a good choice.

There is a problem of cost: the price of the sensor required for obtaining biometric features and that of Smart SSDs is not insignificant. However, such limitation will be overcome as the hardware is developed; it has been witnessed that hardware devices with the same specification become less expensive with time.

In the future, the type of attack that overrides final decisions on the SoSp domain will be addressed. The problem of fake biometrics is somewhat beyond the technology area; the solution for such attacks might be delivered through social engineering or other actions to obtain the real biometrics. Secure communication between the components of the SoSp domain will be studied as well.

Acknowledgements:

This work was supported by the IT R&D program of MSIP/KEIT. [10041145, Self-Organizing Software platform (SoSp) for Welfare Devices]

Corresponding Author:
Prof. Gil-Jin Jang, Prof. Jung-Min Yang
School of Electronics Engineering
Kyungpook National University
Republic of Korea
E-mail: gjang@knu.ac.kr, jmyang@ee.knu.ac.kr

References

1. Jain A. K., Ross A. Introduction to Biometrics. In Jain, AK; Flynn; Ross, A. *Handbook of Biometrics*. Springer. pp. 1–22. ISBN 978-0-387-71040-2. 2008.
2. Ratha N. K., Connell J. H., Bolle R. M. An analysis of minutiae matching strength. Audio and Video-based Biometric Person Authentication (AVBPA) 2001; 223–228.
3. Mordini E. Ethics and Policy of Biometrics. Handbook of Remote Biometrics 2009.
4. Kang H., et al. Self-Organizing Middleware Platform Based on Overlay Network for Real-Time Transmission of Mobile Patients Vital Signal Stream. THE JOURNAL OF KOREA INFORMATION AND COMMUNICATIONS SOCIETY (J-KICS) 2013; 38C(7):630-642.
5. Jain A. K., et al. Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers 1999.
6. Jain A. K., Ross A., Uludag U. BIOMETRIC TEMPLATE SECURITY: CHALLENGES AND SOLUTIONS. European Signal Processing (EUSIPCP) 2005.
7. Kang Y., et al. Enabling Cost-effective Data Processing with Smart SSD. IEEE Symposium on Massive Storage Systems and Technologies (MSST) 2013.
8. Dressler F. A study of self-organization mechanisms in ad hoc and sensor networks. Computer Communications 2008; 31(13):3018-3029.
9. Jain A. K., Ross A., Prabhakar S. An Introduction to Biometric Recognition. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY 2004; 14(1).
10. Kim S., et al. Fast, Energy Efficient Scan inside Flash Memory SSDs. International Workshop on Accelerating Data Management Systems using Modern Processor and Storage Architectures (ADMS) 2011.
11. Adler A. Can images be regenerated from biometric templates?. Biometrics Consortium Conference 2003.
12. Uludag U., Jain A. K. Attacks on biometric systems: a case study in fingerprints. SPIE, Security, Seganography and Watermarking of Multimedia Contents VI 2004; 5306: 622–633.
13. Hill C. J. Risk of masquerade arising from the storage of biometrics. B.S. Thesis, Australian National University 2011; http://chris.fornax.net/biometrics.html.
14. Do J., et al. Query Processing on Smart SSDs: Opportunities and Challenges. SIGMOD'13
15. Al-Assam H., et al. A Lightweight approach for biometric template protection. SPIE, Mobile multimedia/image processing, security, and applications 2009.

5/26/2014