Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2014, Article ID 350876, 9 pages
http://dx.doi.org/10.1155/2014/350876

*Research Article*

# Secure eHealth-Care Service on Self-Organizing Software Platform

**Im Y. Jung, Gil-Jin Jang, and Soon-Ju Kang**

*School of Electronics Engineering, Kyungpook National University, Daegu 702-701, Republic of Korea*

Correspondence should be addressed to Gil-Jin Jang; gjang@knu.ac.kr and Soon-Ju Kang; sjkang@ee.knu.ac.kr

Received 8 April 2014; Accepted 30 May 2014; Published 17 July 2014

Academic Editor: Jong-Hyuk Park



There are several applications connected to IT health devices on the self-organizing software platform (SoSp) that allow patients or elderly users to be cared for remotely by their family doctors under normal circumstances or during emergencies. An evaluation of the SoSp applied through PAAR watch/self-organizing software platform router was conducted targeting a simple user interface for aging users, without the existence of extrasettings based on patient movement. On the other hand, like normal medical records, the access to, and transmission of, health information via PAAR watch/self-organizing software platform requires privacy protection. This paper proposes a security framework for health information management of the SoSp. The proposed framework was designed to ensure easy detection of identification information for typical users. In addition, it provides powerful protection of the user's health information.

## 1. Introduction

Self-organization is a process in which the structure and functionality (pattern) of a system at the global level emerge solely from numerous interactions among the lower-level components without any external or centralized control. The system components interact in a local context, either by means of direct communication or through environmental observations, without reference to a global pattern [1].

The self-organizing software platform (SoSp) is a platform designed to actualize the self-organizing function of communication devices [2]. A SoSp is combined IT health devices. Such devices are designed to automatically interact with the physical environment and users based on the necessities and the surroundings of the users [3], for example, wearable healthcare, medical devices, watches, and bicycles, with ubiquitous computing allowing users to take care of their health needs easily regardless of their location or time and to cope with certain types of emergencies. The SoSp and its applications are practical products of IT convergence research for health improvement and are intended to be utilized by elderly users or patients. Ordinarily, people can check their health through periodic measurements and transmit their biosignals to their family doctors. During an emergency, they can call their doctors by pressing an emergency button and transmit their biosignals to them immediately regardless of their location or time [4, 5].

In this paper, an essential security framework to maintain, access, and transmit health information, such as an electrocardiogram (ECG) or other biosignals, is proposed. As sensitive private data, health information needs to be kept secure and should be accessed only by authorized persons. In addition, the users should be identified when their biosignals are acquired and accessed. The proposed framework was designed to ensure easy detection of verification information without the burden of using a smartcard or memorized password, particularly to patients or elderly users. However, it provides powerful protection of health information and a unique identity verification of biometric recognition [6].

The rest of this paper is organized as follows: Section 2 describes previous work related to this topic. Section 3 presents a brief review of the SoSp and its requirements of health information management. The proposed security framework for health information management applied on the SoSp is presented in Section 4. A security analysis and overhead estimation are then demonstrated in Section 5. Finally, some concluding remarks and areas of future work are provided in Section 6.

## 2. Related Works

Research on biometric authentication is actively being conducted as a means for password replacement [7]. Biometric features (fingerprints, faces, irises, hand geometries, palmprints, etc.) can be neither lost nor forgotten. They are neither copied nor shared easily [8]. In addition, they are extremely difficult to forge or distribute. Because they maintain their uniqueness, they are difficult to guess [9]. As powerful mobile devices and the internet are continuously developing, biometric authentication is being grafted into them [10]. Mobile biometric authentication using face and voice recognition simultaneously on a Nokia N900 mobile device was also introduced [11]. An authentication system using multiple biometrics such as face and hand features has also been studied [12, 13].

However, it is a significant issue how to preserve and to transmit the information for biometric authentication securely as well as the additional cost to adopt the device to acquire biometric data [14]. On the other hand, function creep, which refers to biometric data used outside of the original purpose, exists [15–17]. These days, personal information being sold or passed around without proper consent is a series issue. The unique and permanent nature of biometric information adds a more serious dimension to such a breach of confidentiality, that is, unlike passwords, fingerprints or retinal patterns cannot be changed when an identity theft is suspected [18]. A case involving Emilio Calatayud in the United States shows that systems containing an aggregation of identifiable personal information can be abused [19]. When patients use smartcards or barcodes to protect their privacy, managing such cards and barcodes against theft or loss becomes a double burden. Using cryptography to protect health information can generate complexity in the application, for example, the choice of whose information to encrypt (pharmacist, pharmacy, or group of pharmacies) and which public keys to use [20]. In [9], an efficient biometric-based authentication scheme for a telecare medicine information system (TMIS) with a nonce was proposed. When users are cared for using a TMIS, their mobile devices are connected to the TMIS through a public network, for example, the Internet. The goal is to overcome Internet security risks [20, 21].

On the other hand, the authors in [22] proposed a framework for security management in a self-organized mobile ad hoc network based on the assumption that individual nodes are themselves responsible for their own security level. However, in a network where health information is delivered, authentication and authorization should be further stressed because a node can be misused by another entity, that is to say, another person. The authors in [23] proposed a security protocol for self-organizing data storage through periodic verification. A self-organizing trust model was studied to trust the communications among nodes in P2P systems [24].

Researches into the security of the acquisition and transmission of health information have been conducted. However, there has been no research regarding health information management on internet of things (IoT) [25], especially on SoSp network.

## 3. Health Information Management on SoSp

*3.1. Domain Description.* Figure 1 shows a SoSp domain used to manage health information. The whole environment can be divided into several small spaces such as rooms or floors. Such spaces, called *unit spaces,* are the basic units for assessing location awareness. Communication devices are divided into stationary nodes and mobile nodes. A node means a communication device that is implemented in hardware. Mobile nodes are characterized through low-speed operations and can be attached to a person or physical mobile object in the form of small tags with limited H/W (e.g., 8-bit MCU, 4 K of SRAM, and a coin battery) and communication functionality. Unlike RFID tags, however, mobile nodes can communicate bidirectionally. In Figure 1, a mobile node is a mobile self-organizing software platform router (SoSpR) implemented on a smartphone. It provides a text message connection, emergent calls, and a fixed SoSpR agent. Stationary nodes attached to ceilings or walls of the unit spaces, for example, the fixed SoSpR shown in Figure 1, are characterized by high-speed operations with powerful H/W (e.g., an Arm Cortex A8 MCU with 512 MB of SDRAM, an 8 GB SDCard, and an IEEE 802.15.4 transceiver) compared with a mobile node. They are intended to function as location references and communication access for mobile nodes. A stationary node has a wired network for communication between stationary nodes and a wireless (sensor) network for communication between mobile nodes. The communication between stationary and mobile nodes is limited to a single hop. This approach can help minimize the network congestion and delay problems that take the form of a broadcast storm, packet replication, or routing table overflow in a multihop *ad hoc* sensor network [26, 27].

Figure 2 shows the SW stack of the SoSpR for health information management on the SoSp network [4]. The SW stack is composed of three parts: transportation for real-time streaming of health data, coordination for interaction, and user interface. The transportation part consists of messaging middleware, service broker and discovery, service routing, data processing, and simulation. Messaging middleware supports streaming transmission through publish and subscribe service. In Figure 2, Service Broker & Discovery creates or searches for new services. The coordination part provides cooperation among distributed services based on the consensus, group management, leader election, and presence protocol. This paper focuses on a security module of the SoSpR and distributed personal health record storage.

*3.2. Healthcare via SoSp. Connected Patient in Home* [4] states the service and its infrastructure, which can monitor patients or the aged at home in real-time and transmit the data monitored to their doctors using mobile technology [28]. One of the applications is the control of medicine dispersal. Not only the service and its infrastructure can reduce the user's medical expenses, but also they can improve the interaction between patients and doctors.

The SoSp as a self-organizing middleware platform for real-time biosignal transmission acquires various biosignals (e.g., ECG streaming data) from their measuring devices,

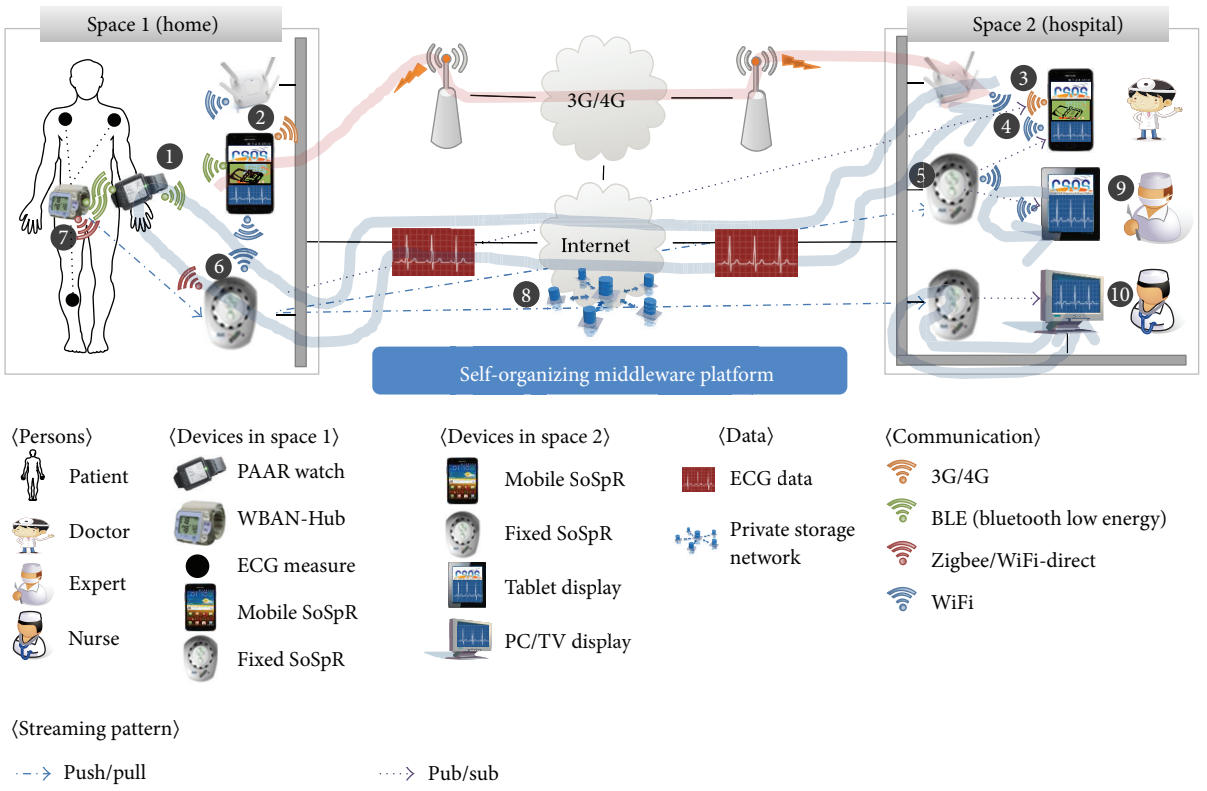


Figure 1: Domain description of SoSp for health information management [4].

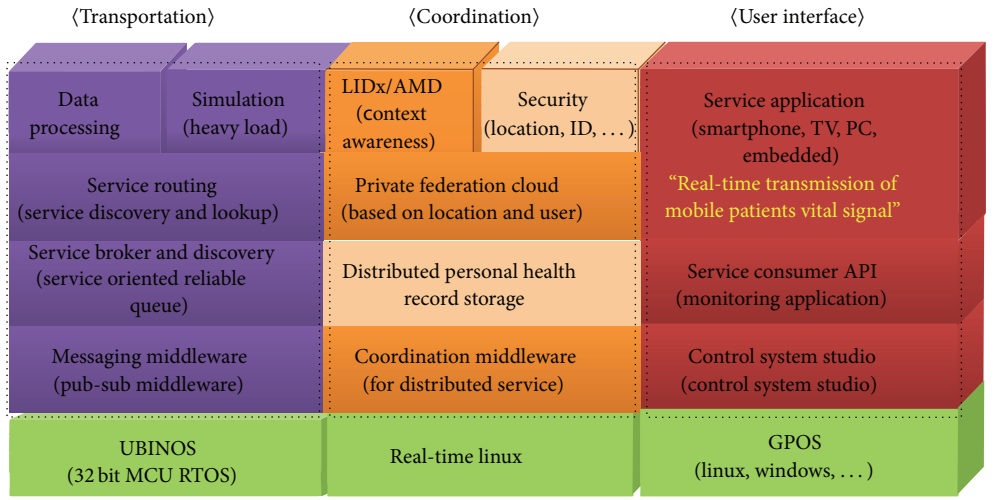


Figure 2: SW stack of SoSpR for health information management on SoSp [4].

transmits them to the SoSpR, and saves them in safe storage in real-time. Several devices can receive the signals from the SoSpR and display them. That is to say, the devices operated and managed by patients or the aged can interact with each other on the SoSp network and provide context-aware services for healthcare without any presetting. A flexible handover while moving and a predefined protocol can be used to handle emergencies.

Figure 1 shows the SoSp domain for health information management [4].

(1) When a patient or elderly user, wearing an ECG sensor, WBAN-Hub, and PAAR watch, presses the emergency button

in the PAAR watch, the PAAR watch notifies the mobile SoSpR (e.g., a smartphone) of the emergent state through bluetooth low energy (BLE) communication.

(2) The mobile SoSpR sends an SMS to a predefined person such as a doctor, medical team worker, or other family members.

(3, 4) When a doctor receives the emergency SMS, they request the biosignal of the patient or elderly user from a fixed SoSpR near in space 2, shown in Figure 1, if necessary.

(5) The fixed SoSpR in space 2 delivers a request to the fixed SoSpR, which can provide streaming service of the biosignal of the patient or elder user in space 1.

(6) The fixed SoSpR in space 1 sends a message to a WBAN-Hub allowing it to start measuring the ECG signal of the patient or elderly user.

(7) As WBAN-Hub measures the ECG signal, it sends the signal data to the fixed SoSpR in space 1 using a push-pull streaming pattern [29].

(8) The biosignal is saved in a private storage network and simultaneously sent to the client device that requested the signal. If the client device is a smartphone, the signal is transmitted through WiFi using a publish-subscribe pattern [30]. If the devices cannot be accessed through WiFi, the signal is sent to the fixed SoSpR near the devices using a push-pull streaming pattern.

(9, 10) Other authorized medical team workers or family members can monitor the biosignal of the patient or elderly user using a tablet PC, desktop PC, or TV located near the fixed SoSpR, which provides streaming service.

*3.3. Requirements of Health Information Management on SoSp.* At the domain handling the health information including the biosignal, privacy protection, authentication, and authorization are very important. This section describes the domain requirements for health information management on the SoSp including the security requirements.

The overlay network constructed by the SoSp is vulnerable to the same threats as any wireless network. However, the SoSp has the following additional threats and vulnerabilities owing to its basic nature [22].

(i) There is a lack of central administration, and neither central control nor prior contact is assumed.

(ii) The routing mechanisms are more vulnerable than in conventional networks because each node can act as a relay.

(iii) In terms of cooperation, if a node does not respect the cooperation rules, that is, it is selfish, the performance of the network can be severely affected.

(iv) There is a variation in memory and computation resources, in which many of the nodes are expected to be low-priced consumer electronics with cheap and slow computation capability and a limited storage size.

(v) Finally, there is an energy constraint during operation, in which many of the nodes are expected to operate on battery power. Sleep or standby modes are used to conserve energy, during which they may not be reachable. A sleep deprivation torture (exhausting the battery power) attack may be implemented by attackers.

These threats place great demand for flexibility of the security system because one must be capable of tailoring the range of supplied security services toward a wide variety of network topologies and application requirements, rather than fixing them. Further, each application imposes cost, performance, complexity, flexibility, and ease-of-use constraints, which affect the feasibility of a particular security solution [31].

In addition, node security, secure information handling, authentication, and authorization are needed. In particular, easy human computer interaction (HCI) and an efficient and simple sequence of security mechanisms should be seriously considered for elderly users and patients.

A security framework for health information management on the SoSp was proposed that satisfies the requirements mentioned in this section.

## 4. Security Framework for Health Information Management on SoSp

*4.1. System Architecture.* Figure 3 shows the proposed system architecture of security framework for health information management on the SoSp. The health information of the patients, authorization information of the doctors who can access the information, and the biometric recognition information of the patients and doctors are saved in secure storage. Biometric recognition devices can be equipped in a PAAR watch [4] worn by the patients or doctors. Multiple biometric recognition devices can be equipped in one PAAR watch. Through such devices, biometric recognition information, such as fingerprint, face, voice, and iris information, can be easily acquired. Several types of biometric recognition information can be combined to improve the exactness of verification.

*4.2. Service Management.* The fixed SoSpR, which loads the streaming service of a biosignal, can provide streaming service for mobile nodes or devices that have registered for a service subscription. However, data leakage during transmission is one weak point in an overlay network because there is no central server that manages all of the nodes providing streaming service, or the paths that the data are delivered upon. Any security scheme should be lightweight so that it does not cause a delay in streaming.

Figure 4 shows the security scheme used to protect health information delivered on the SoSp.

When a doctor requests the streaming of a patient's biosignal, he/she issues one ID of the patient, $\mathrm{id}_{\mathrm{temporary}}$, and send $\mathrm{ID}_{\mathrm{patient}}$, which is composed of $\mathrm{id}_{\mathrm{temporary}}$ and the issuing timestamp, $T$, to the mobile SoSpR of the patient directly. Consider

$$\mathrm{ID}_{\mathrm{patient}} = \mathrm{id}_{\mathrm{temporary}} \,||\, T. \tag{1}$$

If the issuing time is 2014-01-20 15:30, $T$ will be a string of 201401201530.

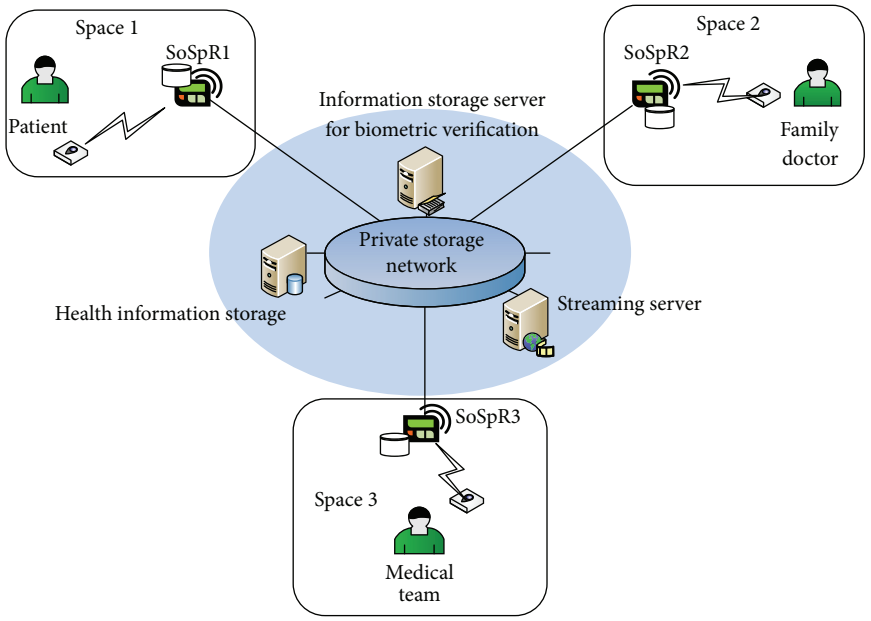


FIGURE 3: System architecture of security framework for health information management on SoSp.

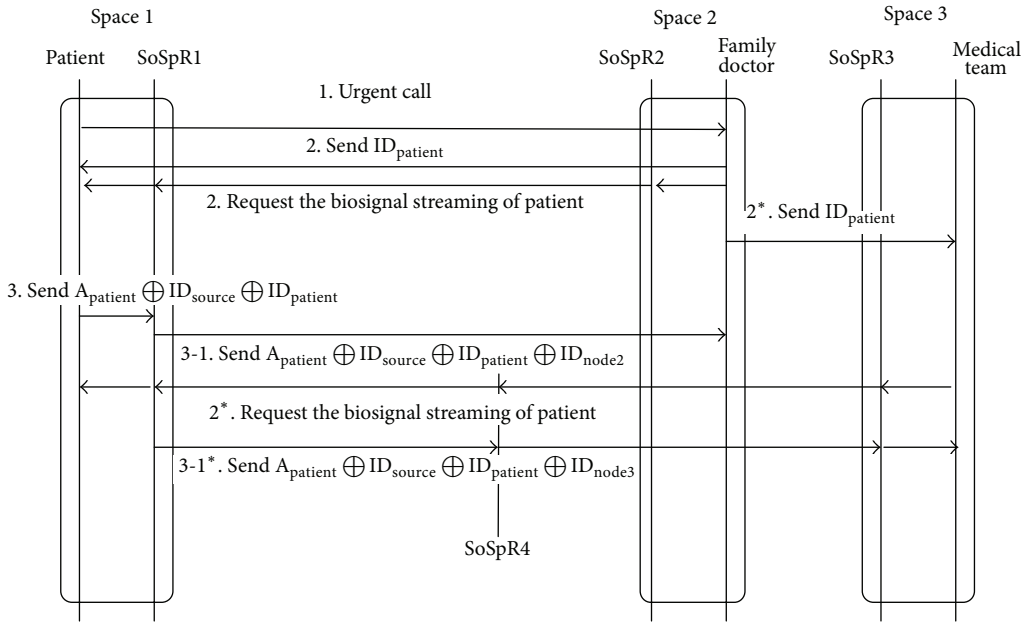


FIGURE 4: Health information protection on SoSp.

When the biosignal of the patient is $A_{\text{patient}}$, and the ID of the equipment used to measure the biosignal is $\text{ID}_{\text{source}}$, the streaming data includes the XOR results of $A_{\text{patient}}$, $\text{ID}_{\text{source}}$, and $\text{ID}_{\text{patient}}$. Consider

$$A_{\text{patient}} \oplus \text{ID}_{\text{source}} \oplus \text{ID}_{\text{patient}}. \tag{2}$$

An XOR operation is very fast and lightweight.

If the destination identity, $\text{ID}_{\text{node}}$, is added,

$$A_{\text{patient}} \oplus \text{ID}_{\text{source}} \oplus \text{ID}_{\text{patient}} \oplus \text{ID}_{\text{node}}. \tag{3}$$

Only the node whose identity is $\text{ID}_{\text{node}}$ can know $A_{\text{patient}} \oplus \text{ID}_{\text{source}} \oplus \text{ID}_{\text{patient}}$. This prevents eavesdropping during transmission in an overlay network and ensures exact delivery to the destination.

In addition, only the doctor who knows $\text{ID}_{\text{source}}$ and $\text{ID}_{\text{patient}}$ can see $A_{\text{patient}}$. Therefore, when cooperative medical treatment is needed, the doctor notifies the medical team members of $\text{ID}_{\text{source}}$ and $\text{ID}_{\text{patient}}$ through another communication channel, not the SoSp network. $\text{ID}_{\text{source}}$ is permanent and $\text{ID}_{\text{patient}}$ is temporary. Because $\text{ID}_{\text{patient}}$ is a temporary identity issued by a doctor, anonymity is guaranteed and the

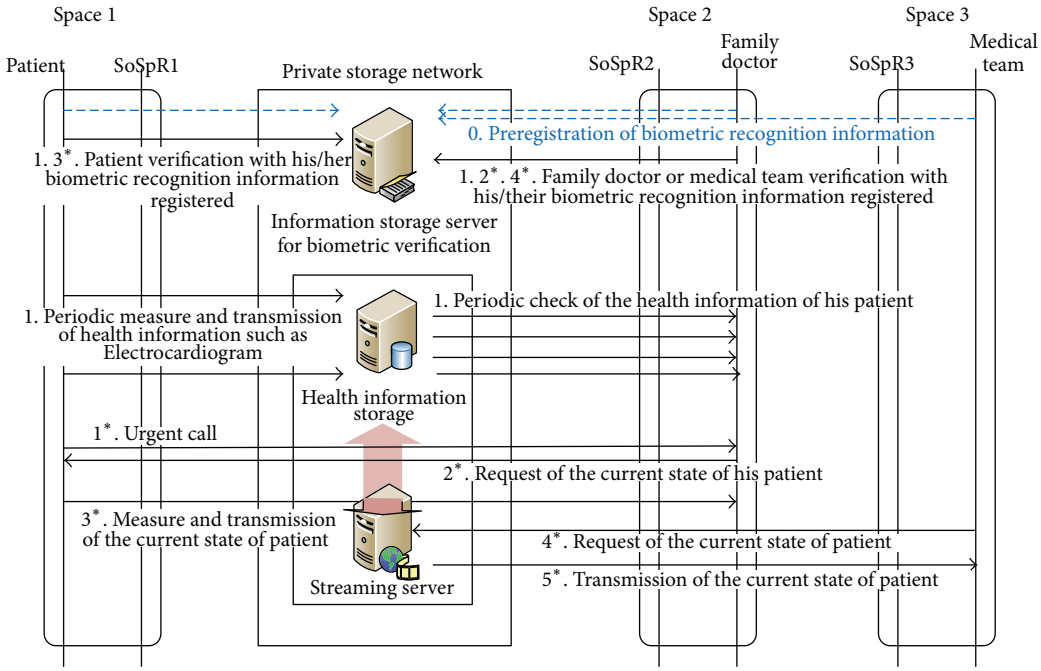


Figure 5: Secure health information management on SoSp.

patient's privacy is protected. The issuing time, $T$, prohibits a relay attack.

*4.3. Authentication and Authorization.* Figure 5 shows a sequence diagram of health information management on the SoSp.

Verification information on the biometric recognition for the patient, family doctor, and medical team should be registered in advance. Verification of the family doctor or medical team is done every time they are requested to access the patient's health information. They should be verified periodically while accessing and monitoring the biosignal of the patient because of the limited effective verification time. The verification of the patient is done each time their biosignal is measured, and the information is kept in private storage.

During an emergency, the patient can call his/her family doctor by pushing the emergency button on his/her PAAR watch. The family doctor requests the biosignal of his/her patient in real-time, who is verified simultaneously. The biosignal is measured and transmitted to both the family doctor and the private storage. When the family doctor requests cooperation of the medical team, the medical team can obtain the patient's state from the streaming server through the verification procedure.

The strong points of the proposed security framework for health information management on the SoSp are its exact verification capability using biometric recognition, secure protection of data and its simple and convenient user interface.

## 5. Evaluation

*5.1. Framework Analysis.* This section analyzes whether the proposed framework satisfies the requirements of health information handling on the SoSp.

*5.1.1. Lack of Central Administration.* All nodes on the SoSp should route and search for services for users without a central administration through a central server. However, it overcomes a single point of failure of the central server, the centralized burden of processing, and the nonscalability. The performance of the SoSp with mobile nodes is better than a centralized environment [32]. The proposed framework manages important data such as the biometric authentication and the biosignal of the patients or elderly users for periodic check-ups on the private storage network. This framework provides a safe deposit of private information.

*5.1.2. Routing Mechanisms.* In the framework, fixed SoSpRs are connected through a wired network. Mobile nodes have a one-hop connection to fixed SoSpRs. This simple scheme lessens the side effects of routing on the SoSp.

*5.1.3. Cooperation.* Cooperation among the nodes on the SoSp is under implementation. There are many nodes providing the same services in the SoSp network. The SoSp network will be implemented in such a way that the service group is reorganized by isolating any selfish nodes [33–36].

*5.1.4. Performance Variation in Memory and Computation Resources.* Based on an XOR operation, the security framework does not cause a delay in real-time streaming. We limit the operations to an XOR because it is a lightweight operation [37]. Therefore, there is no problem stemming from performance variations in the node resources in the SoSp network.

*5.1.5. Energy-Constrained Operation.* Most types of wireless networks have limited computational power such that they

cannot perform operations over large finite fields [37]. An XOR operation has been evaluated as having good operations and can be used for wireless network coding.

### 5.2. Security Analysis

*5.2.1. Node Security.* SoSpRs do not maintain the health information of users. All of the data are processed at the RAM of the SoSpRs. It is infeasible to acquire data that passes the SoSpRs. In the proposed security framework, the node security is less focused. Instead, the security scheme covers the overall security for the health information handling on the SoSp.

*5.2.2. Secure Information Handling.* A health information handling service is only served to the clients who are authenticated. In addition, only the person who knows the ID of a patient can see his/her health data.

According to the streaming patterns in the SoSp network, health information is protected in the following manner.

(1) Push-pull transmission between the WBAN-Hub and a fixed SoSpR.
Because the fixed SoSpR receives $A_{\text{patient}} \oplus \text{ID}_{\text{source}} \oplus \text{ID}_{\text{patient}}$ and transmits it, the SoSpR cannot know $A_{\text{patient}}$.

(2) Push-pull transmission between fixed SoSpRs.
When there is no SoSpR that provides streaming service, the biosignal is relayed to the SoSpR, which can provide the service. In this case, the SoSpR that relays the signal cannot know $A_{\text{patient}}$ because it does not know $\text{ID}_{\text{source}} \oplus \text{ID}_{\text{patient}}$.

(3) Publish-subscribe transmission between a fixed SoSpR and various devices such as a tablet PC, desktop PC, or TV.

The proposed security framework only allows a one-hop connection between the fixed SoSpR and the end nodes. Of course, the end nodes should subscribe to the service. This lessens the security threat caused by a multihop connection.

*5.2.3. Easy HCI.* Identification by a password is not suitable because the process memorizing the password and its input is somewhat burden for a patient or elderly user, particularly during an emergency [38]. Because biometric authentication is easy, it is a good HCI instead of password identification.

*5.2.4. Efficient and Simple Security Mechanism.* An efficient and simple sequence is another important security mechanism for a patient or elderly user. The security mechanism should be fast and cooperate simply with the HCI. A self-organizing platform is characterized by no presettings or central management. The proposed security framework does not require any complex sequences that the users should follow or participate in.

*5.2.5. Exact Identification and Authentication.* Biometric authentication is secure because the biometric data are unique and are hard to copy or falsify. A password can be easily leaked or cracked [38].

*5.2.6. Authentication and Authorization.* The proposed framework provides a strict authorization for the health data. Only the doctors or medical team members who are authenticated and authorized can access the data of the patient or elderly user.

Today, many security incidents from loose authentication procedures have occurred [39]. In the proposed framework, all users are identified through their biometric authentication. Because biometric data are unique, they are difficult to copy or modify. The biometric method is also easy for patients and elderly users to use.

*5.3. Estimation of Performance and Overhead.* The performance of the proposed framework and the overhead imposed on the SoSp by the framework are estimated as follows.

(i) The performance of the biometric authentication added to the real-time streaming service of biosignals
One type of biometric authentication, fingerprint verification, is loaded onto smartphones. High-performance SW products for fingerprint verification of smartphone users have been developed [40]. Under the SoSpR prototype with Exynos5 Octa Cortex-A15 1.6 Ghz quad core and Cortex-A7 quad core CPU, 2 GB LPDDR3 RAM, the XOR overhead of 4 B and 8 B were negligible (~0 sec); the unit of data streaming is 3 B at current state.
It may therefore not be a problem to use such biometric verification on the SoSp in near future. In the proposed framework, a storage server is used to keep the biometric data for authentication safe and conduct a heavy authentication procedure. Therefore, biometric authentication does not cause a delay in real-time service.

(ii) The performance of the XOR operation when streaming data are created and streaming data are restored at the destination.
Because an XOR operation is sufficiently lightweight to be used as a wireless network packet [37], real-time streaming is not affected seriously by an XOR operation at the source or destination of the streaming data.
Because biometric authentication and XOR operations are extra modules for the SoSp, some overhead exists when adopting them. However, they overcome the overhead in the following way.

(iii) Biometric authentication is exact, not copy-prone, and unmodifiable. It is easy for a patient or elderly user to adopt, especially during an emergency.

(iv) An XOR operation is simple and lightweight. When such an operation is applied to health information, the information is hidden without the need for complex cryptography.

In addition, even though the streaming data are revealed, it is difficult to know whose data belongs to which $\text{ID}_{\text{patient}}$. Anonymity guarantee is another strong point of the proposed security framework.

## 6. Conclusion and Future Works

This paper proposed an essential security framework of the SoSp to maintain, access, and transmit health information such as a biosignal. As sensitive and private data, health information needs to be kept securely, and should be strictly accessible only by the authorized persons.

The proposed security framework requires mutual authentication between the patient or elderly user and the medical team through biometric authentication. In addition, it protects the privacy of the patient or elderly worker with a temporary anonymous ID issued by the family doctor or doctor in charge. Through a simple and lightweight operation, that is, an XOR, the biosignal is hidden. The signal can be recovered only by those persons who know the temporary ID, $ID_{patient}$, and the ID of the device measuring the biosignal, $ID_{source}$.

The proposed security framework is under implementation. After implementation, the framework will be tuned according to the upgraded SoSp to improve its performance and reduce the overhead. In addition, node security, particularly the SoSpR, will be intensively considered.

## Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

## Acknowledgment

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

## References

[1] F. Dressler, "A study of self-organization mechanisms in ad hoc and sensor networks," *Computer Communications*, vol. 31, no. 13, pp. 3018–3029, 2008.

[2] Center of Self-Organizing Software-Platform, http://www.csosp.org/.

[3] S. Oh, "Using an adaptive search tree to predict user location," *Journal of Information Processing Systems*, vol. 8, no. 3, pp. 437–444, 2012.

[4] H.-Y. Kang, S.-Y. Jeong, C.-S. Ahn, Y.-J. Park, and S.-J. Kang, "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* , vol. 38, no. 7, pp. 630–642, 2013.

[5] J. Ahn and R. Han, "An indoor augmented-reality evacuation system for the smartphone using personalized pedometry," *Human-Centric Computing and Information Sciences*, vol. 2, article 18, 2012.

[6] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

[7] S. Sonkamble, R. Thool, and B. Sonkamble, "Survey of biometric recognition systems and their applications," *Journal of Theoretical and Applied Information Technology*, vol. 11, no. 1, pp. 45–51, 2010.

[8] A. Chaudhary, K. Vatwani, T. Agrawal, and J. L. Raheja, "A vision-based method to find fingertips in a closed hand," *Journal of Information Processing Systems*, vol. 8, no. 3, pp. 399–408, 2012.

[9] D. Mishra, S. Mukhopadhyay, S. Kumari, M. K. Khan, and A. Chaturvedi, "Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce," *Journal of Medical Systems*, vol. 38, no. 5, article 41, 2014.

[10] C.-L. Tsai, C-J. Chen, and D.-J. Zhuang, "Trusted M-banking verification scheme based on a combination of OTP and biometrics," *Journal of Convergence*, vol. 3, no. 3, pp. 23–30, 2012.

[11] S. Marcel, C. Cool, C. Atanasoaei et al., "MOBIO: mobile biometric face and speaker authentication," in *Proceedings of the Conference on Computer Vision and Pattern Recognition (CVPR '10)*, 2010.

[12] J. Rokita, A. Krzyzak, and C. Y. Suen, "Cell phones personal authentication systems using multimodal biometrics," in *Proceedings of the International Conference on Image Analysis and Recognition (ICIAR '08)*, pp. 1013–1022, 2008.

[13] S. Basak, M. I. Islam, and M. R. Amin, "A new approach to fingerprint detection using a combination of minutiae points and invariant moments parameters," *Journal of Information Processing Systems*, vol. 8, no. 3, pp. 421–436, 2012.

[14] A. P. Pons and P. Polak, "Understanding user perspectives on biometric technology," *Communications of the ACM*, vol. 51, no. 9, pp. 115–118, 2008.

[15] A. Chandra and T. Calderon, "Challenges and constraints to the diffusion of biometrics in information systems," *Communications of the ACM*, vol. 48, no. 12, pp. 101–106, 2005.

[16] A. Sprokkereef and P. de Hert, "Ethical practice in the use of biometric indentifiers within the EU," *Law, Science & Policy*, vol. 3, no. 2, pp. 177–201, 2007.

[17] L. A. Jones, A. I. Antón, and J. B. Earp, "Towards understanding user perceptions of authentication technologies," in *Proceedings of the 6th ACM Workshop on Privacy in the Electronic Society (WPES '07)*, pp. 91–98, October 2007.

[18] S. Khan and P. Gurkas, "Identification using biometric technology: issues and attitudes," in *Proceedings of the IADIS International Conference ICT, Society and Human Beings*, 2010.

[19] K. Poulsen, "DEA Data Thief Sentenced to 27 Months, Security Focus," 2002, http://online.securityfocus.com/news/1847.

[20] E. Ball, D. W. Chadwick, and D. Mundy, "Patient privacy in electronic prescription transfer," *IEEE Security & Privacy*, vol. 1, no. 2, pp. 77–80, 2003.

[21] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: a systematic literature review," *Journal of Biomedical Informatics*, vol. 46, no. 3, pp. 541–562, 2013.

[22] R. Savola and I. Uusitalo, "Towards node-level security management in self-organizing mobile ad hoc networks," in *Proceedings of the Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT/ICIW '06)*, 2006.

[23] N. Oualha, M. Önen, and Y. Roudier, "A security protocol for self-organizing data storage," Research Report RR-08-208, Institut Eurecom, 2008.

[24] A. B. Can and B. Bhargava, "SORT: a self-organizing trust model for peer-to-peer systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 1, pp. 14–27, 2013.

[25] J. Couturier, D. Sola, G. Scarso Borioli, and C. Raiciu, "How can the internet of things help to overcome current healthcare challenges," *Digiworld Economic Journal*, vol. 87, pp. 67–81, 2012.

[26] D. K. Lee, T. H. Kim, S. Y. Jeong, and S. J. Kang, "A three-tier middleware architecture supporting bidirectional location tracking of numerous mobile nodes under legacy WSN environment," *Journal of Systems Architecture*, vol. 57, no. 8, pp. 735–748, 2011.

[27] A. Shikfa, "Security issues in opportunistic networks," in *Proceedings of the 2nd International Workshop on Mobile Opportunistic Networking (MobiOpp '10)*, pp. 215–216, Pisa, Italy, February 2010.

[28] J. Kee-Yin Ng, "Ubiquitous healthcare: healthcare systems and applications enabled by mobile and wireless technologies," *Journal of Convergence*, vol. 3, no. 2, 2012.

[29] M. Fouzia and J. Subrun, "Push pull services offering SMS based m-banking system in context of Bangladesh," *International Arab Journal of e-Technology*, vol. 1, no. 3, 2010.

[30] D. Lagutin, K. Visala, A. Zahemszky, T. Burbridge, and G. F. Marias, "Roles and security in a publish/subscribe network architecture," in *Proceedings of the 15th IEEE Symposium on Computers and Communications (ISCC '10)*, pp. 68–74, June 2010.

[31] T. S. Messerges, J. Cukier, T. A. M. Kevenaar, L. Puhl, R. Struik, and E. Callaway, "A security design for a general purpose, self-organizing, multihop ad hoc wireless network," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03)*, pp. 1–11, October 2003.

[32] S. Y. Jeong, H. G. Jo, and S. J. Kang, "Remote service discovery and binding architecture for soft real-time QoS in indoor location-based service," *Journal of Systems Architecture*, 2014.

[33] S. Silas, K. Ezra, and E. B. Rajsingh, "A novel fault tolerant service selection framework for pervasive computing," *Human-Centric Computing and Information Sciences*, vol. 2, p. 5, 2012.

[34] X. Zhou, Y. Ge, X. Chen, Y. Jing, and W. Sun, "A distributed cache based reliable service execution and recovery approach in MANETs," *Journal of Convergence*, vol. 3, no. 1, pp. 5–12, 2012.

[35] V. Viswanathan and I. Krishnamurthi, "Finding relevant semantic association paths through user-specific intermediate entities," *Human-Centric Computing and Information Sciences*, vol. 2, article 9, 2012.

[36] D. Werth, A. Emrich, and A. Chapko, "An ecosystem for user-generated mobile services," *Journal of Convergence*, vol. 3, no. 4, pp. 10–15, 2012.

[37] A. Khreishah, I. M. Khalil, P. Ostovari, and J. Wu, "Flow-based XOR network coding for lossy wireless networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 6, pp. 2321–2329, 2012.

[38] J. Catone, "Bad Form: 61% Use Same Password for Everything," January 2008.

[39] APWG, "Phishing Activity Trends Report," 2013.

[40] Precise BioMatch Mobile, http://www.precisebiometrics.com.