Study on the sensor database for realizing Healing Communication System

Tatsuro NAKAMURA, Keita GOTO, Takamasa SHIMADA, Noriko KONNO, Noriharu MIYAGO
Tokyo Denki University, Graduate school of Information Environment

1. Introduction

Recently, the healing effect of light or aroma has got a lot of attentions. For instance, it is proposed that a network service which can control the aroma generator device that is remotely located by delivering the healing recipe via network [1], and the healthcare will be realized for pain clinic by using light and aroma.

In previous work we have already studied that healing communication system as a network service which can be used for the telemedicine service to improve the user’s QoL by utilizing the sensor network technology with remotely controllable aroma generating device and lighting device, which are expected for increasing relaxation effect [2]-[5]. However in case that the network service for medical treatment is commercialized, advanced network security and information secrecy technologies for individuals will be required. For instance, the health care organizations such as hospitals have to prevent from personal information leakage. In this paper we propose an encryption method of the sensor data and an access method for the database, taking user’s personal information and the encryption method of the sensor data and an access method for the database into account when the system is being made use of. The evaluation result of the proposed real-time system performance is discussed in the section 3.

2. System Configuration

The healing communication system architecture is shown in Fig. 1.

![Figure 1. Healing Communication System architecture](image)

This system architecture is composed of the Monitoring Centre and the Remote Node. The former is equipped with various databases, the GPS and a Monitoring Centre. GPS technology with accuracy of several centimeters is now in practical use and can be easily used for the authentication. The latter is equipped with the GPS, the Intelligent Sensors including the GPS and the Pulse Wave Sensor which measures user’s biomedical data, and the Node Manager that controls actuators such as the aroma generating device and lighting device based on the received recipe after the mutual authentication process with the Monitoring Centre by making use of the GPS.

3. Evaluation of the Network Performance

For ascertaining the confidentiality of the user’s personal information such as measured sensor data and several private information, we investigated the secure access method for the Sensor Database. In addition taking the mutual authentication process into account, we investigated the quantitative evaluation for the real-time performance.

Proposed database system consists of the Sensor Database where the encrypted data are stored and the Monitoring Centre where the encryption keys are stored.

3.1 Database System Configuration

Proposed database system consists of the Sensor Database where the encrypted data are stored and the Monitoring Centre where the encryption keys are stored. The corresponding stream encryption method which requires low processing power is employed for data encryption as shown in Fig. 2.

![Figure 2. Proposed Encryption Method](image)

In the proposed encryption method, sensor data which correspond to a series of plain texts are divided into certain bits as a specified data piece. One data piece and the subsequence data pieces can be randomly calculated one after another, by using reversible operation, such as binary addition, subtraction or exclusive computation based on the indication of the encryption keys which are stored at the Remote Node Manager. Thereafter the calculated result is replaced to the original subsequence data piece.

Efficient encryption and decryption can be realizing by setting the appropriate size of a data piece. The calculations process history described above as binary digit sequence data of ‘1’ and ‘0’ (metadata) is under the management of the ‘Monitoring Centre. Since, usually the
decryption to the plain text method requires the power of 2 times number of data-piece combinations trials, it is quite difficult to decrypt by the malicious third party. In addition, the size of data piece is regularly changeable, it becomes more difficult to decrypt.

3. 2 Experimental Methodology

Performance evaluation of the proposed system was carried out by taking 2 parameters into account. One is the number of the simultaneously connected user. And the other is the Sensor Database’s Input and Output (DBIO) buffer memory amounts. The number of Dummy Remote Node is ranged from 100 to 300. It was assumed that 20MB DBIO buffer memory and more than 100 users can receive the service is assumed to be sufficient.

The detailed procedure of the evaluation is as follows.

After the mutual authentication, the remote node receives the recipe data. The Intelligent Sensor transmits the sensor data (1kB data, sampled by 1 kHz, 8 bit) to the Sensor Database for 5 minute at intervals of 1 second. As it was assumed 5 minutes as the sufficient amounts of sensor data acquisition interval for the healing recipe evaluation, the transmitting time from each dummy Intelligent Sensors was set. The sensor data transmitted by the intelligent sensor are immediately encrypted and stored at the sensor database. The number of dummy client terminals and dummy Intelligent Sensors are ranged from 100 to 300. To verify the real-time performance of the Sensor Database, we measured that the usage ratio of the storage of the total amount of Sensor Data transmitted by each Intelligent Sensor.

On this condition, one Intelligent Sensors transmits 300 data since each Intelligent Sensor sends the sensor data for 5 minute at intervals of 1 second. And the total amount of sensor data equals to 300 sensor message data multiplied by the simultaneously connected user number.

3. 3 Experimental Result.

Fig. 3 shows the evaluation result. The parameter ‘A’ used in the experimental conditions in the Fig. 3 corresponds to the connecting user numbers, while, ‘B’ corresponds to the amount of the DBIO buffer memory storage.

![Figure 3. Evaluation Result of the System Performance](image)

Experimental results are as follows.

1. Since almost 100% of the usage ratio of the storage of the Sensor Database means that every acquired data are collected, and these situations are just realized in the condition of 1 and 3, when 5 minutes elapse after the beginning of the experimental test. To provide with the network services in real-time, it becomes necessary to determine the appropriate size of the DBIO memory, according to the increase of number of connected users. In case of the conditions of 1 and 3, the appropriate amount of the memory is allocated and hence, realizes the effect for the real-time performance in the system.

2. By comparing the case of the condition 4 with that of the condition 5, we found that the larger size of the DBIO memory has the effect to improve the system performance. However, as shown in case of the condition 6, the system performance improvement by just increasing the amount of DBIO buffer memory is not sufficient enough. The total number of connected users affects the required conditions.

3. It is verified that according to the number of total connected users, the appropriate DBIO memory amount satisfies with the real-time performance requirement of the system and the surplus DBIO memory amount will become ineffective on the contrary.

4. Conclusion

We proposed the effective stream encryption and the access method for the sensor database of the healing communication system to assure the security of the user’s biomedical information. By evaluating the real-time performance of the proposed system, we clarified the requirement of DBIO memory. These experimental results can be applied for realizing the sensor network services with real-time processing which are required by the future telemedicine.

For the future subjects of investigation, we will proceed to collaborative researches with hospital organizations to confirm these proposed system requirements and architecture to achieve the practical cooperation.

References