ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20201209230220
Original scientific paper

The Detection Data Processing Mechanism for Vehicular Cyber Physical System in IoT Environment

Hyun-Jong CHA, Ho-Kyung YANG, You-Jin SONG*

Abstract: With the development of the Internet of Things and big data technology, it was easy to collect personal situation information. The information collected in this way requires the user to support customized services via big data technology. However, traditional situational awareness systems request action through user cognition or provide consistent services for the specific purposes of multiple users. Therefore, this paper proposes a mechanism of Vehicular CPS with situational cognitive function that minimizes direct user intervention for user customization services. In this paper, we designed the system configuration and detailed process based on the scenario of the situation where the user is driving a car. A vector is used to provide a method for determining a dangerous water level by analyzing an abnormal state of a reception threshold with a sensor. The proposed system was analyzed by simulation. By using the authorization step that operates based on the sensor data, we were able to know that the reliability of the user is improved and that the reliable processing of the IoT service is possible. In the future, research for personal authentication and encryption is needed for more secure information processing.

Keywords: fog computing; Internet of Things; multimedia big data; vehicular CPS

1 INTRODUCTION

The emergence of IoT (Internet of Things) is attributed to the strides made in sensor networks and ubiquitous computing and it refers to the intelligent technologies and the service environment that enable autonomous communications between not only people and things but between things and things by connecting all things wirelessly. In other words, IoT has to function on its own without the user working on the computer. Accordingly, for products and services of various areas linked under IoT, there must be minimal human intervention, and there must be autonomous awareness and judgement in providing services with multiple sensing techniques.

At the 2016 Davos Forum (World Economic Forum) the theme was "Understanding the 4th Industrial Revolution" and it was responding mainly to science and technology in the global crisis. The fourth industrial revolution refers to the age of technological convergence in which the boundaries between physical space, digital space and bio-engineering space become blurred by the digital revolution (the third industrial revolution) in IT and electronics technology. It is said that with the recent advancements and spread of such technologies as big data, cloud computing, and IoT, the boundaries between data of the cyber space and the physical world are breaking down to the extent that there are no distinctions between the two. With IoT, digitalization of things is spreading, and with artificial intelligence, data are being processed and moved not by people but by autonomous agents. Based on cloud computing technologies, even huge amounts of data generated by things can now be efficiently processed without restrictions of space and time. Further-more, cyber physical systems are becoming a reality, in which results of data processing from the cyber world can control the movements in the physical world [1-3].

CPS (Cyber Physical System) is an autonomous system based on IoT. With autonomous operation and connectivity, it can sense the surrounding environment and autonomously diagnose the need for maintenance and repair, and issue commands to objects in the physical world to carry out tasks such as repairs.

Gartner proposed the six-stage "Gartner roadmap for digital business" which describes the evolution of the business age driven by technological advancements. Digital business is the fifth stage and this is where a new kind of digital assets is expected to be a key component [4-6].

This paper proposes a processing mechanism for the Vehicular CPS service among the CPS services considering the steps 5 and 6 of the Fourth Industrial Revolution and Gartner's digital business roadmap. The vehicular CPS has minimal user intervention, and can be used in many different types of system domains. To achieve this, a sensor was used, which allows user authentication with heart rates. Because users do not have to have certain awareness or take a certain action in order to identify themselves, it is consistent with the goal of IoT, which aims to minimize user intervention and increase autonomy. Furthermore, with identification of different users, personalized services can be provided [7, 8].

Personalization service is a mechanism provided by each vehicle individually. The encrypted data is stored in the final cloud, and the edge computing is used in consideration of the speed of the service.

With the vehicular CPS system designed in this paper, all events that may occur in various driving scenarios of different users are processed by the actuator. The same services have been provided to all users thus far, but with this approach the n-dimensional vector processing mechanism of sensor data for vehicular CPS with context awareness for multiple users was proposed. Also, user reliability was improved with reliable real-time sensor data and with a privilege grant stage for actuating based on the appropriate sensor data. Recent situation-based systems that are being researched make situation decisions based on standardized criteria. In this paper, we made it possible to overcome these limitations and provide personalized services. In addition, security has been improved. With the findings of this study, reliable processing of IoT services suitable to the context can be performed in a 5G environment to make a commercial debut in the future.

This paper is organized as follows. Chapter 1 is the introduction where the background of the paper and its

purpose are described. Chapter 2 describes the concepts of CPS and fog computing. Chapter 3 describes the structure of the proposed system. Chapter 4 compares the findings of this study with findings of previous studies. Finally, Chapter 5 gives the conclusions and describes future work.

2 RELATED WORKS

2.1 Cyber-Physical System

Recently, various studies are being conducted on IoT technologies which allow things with sensors and actuators to be mutually operated. CPS seeks a convergence between the physical world, composed of physical entities, the cyber world, composed of system entities like sensors, actuators, and embedded systems. In other words, sensor data generated in the physical world are processed in the cyber world, and the physical world is controlled with actuators based on those processed data [9-11].

CPS is a concept derived from the IoT system, and it allows system autonomy. Going further than the existing context-aware systems, it senses the physical world by itself and controls the physical world autonomously based on that sensor data [12].

The products with embedded IoT technologies have progressed in capabilities in four stages: monitoring - control-optimization-autonomy. In particular there are various studies being conducted on minimizing user intervention in the autonomy stage. In IoT, autonomy means that in a IoT product the three functions come together — monitoring, control, and optimization — enabling automatic operation and linkage, and as a result it becomes aware of the surrounding environment, and it self-diagnoses the need for maintenance/repairs, and performs them as necessary [13].

Figure 1 Concept Map of Cyber-Physical System

A CPS can be viewed as a technology in which a computer in a virtual space controls an actual physical system via a network in an environment constructed by the IoT. As shown in Fig. 1, you can see the concept map of the CPS [9].

Vehicular CPS was studied, and as shown in Fig. 2, a dynamic parking service example that recognized the situation supported by the cloud was presented [14].

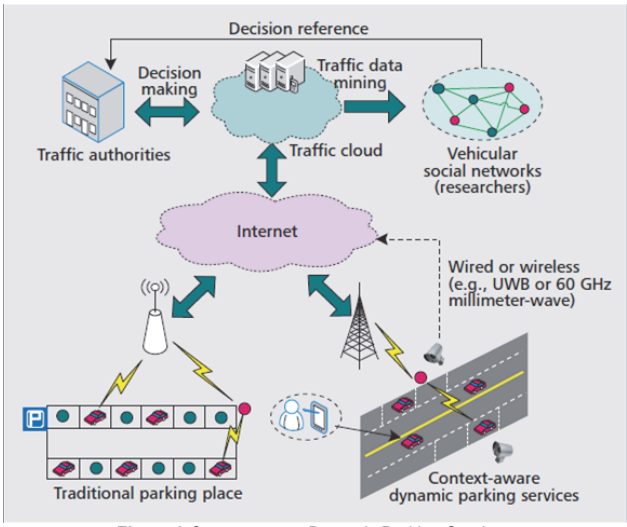

Figure 2 Context-aware Dynamic Parking Services

With the increase in the number of cars on the road, available parking spaces in large cities are becoming scarce, and this problem is only getting more aggravated. Besides multi-level parking lots, they cited a context-aware dynamic parking service, powered by latest technologies like wireless sensor networks and cloud computing, providing context data such as the condition of the road and the status of parking spaces. Two different types of scenarios are discussed with this cloud-based parking service: a traditional parking lot and a dynamic parking service on the road. With the traditional parking lot, parking reservation services are supported with real-time situation information and monitoring of the parking lot. With the dynamic parking service on the road, an efficient parking service is provided using real-time context data [15].

Medical-related CPS research was also promoted. CPS is applied in an environment where all medical practices such as medical care, prescription, surgery, and treatment in the U-health industry are computerized in a cloud virtual space. With U-health, real-time biometrics of users is informatized in a virtual space using their wearable devices, which allows remote real-time monitoring from the hospital. Also, because the medical actions regarding the users are stored in a virtual space on the cloud, they can immediately get medical care from a different hospital than the one they usually get it from [16].

In this context, intelligent remote ECG monitoring was performed in the U-Health industrial environment. In this system, people suspected of arrhythmia wear a small sensor that can take ECG readings, and the collected data are sent to the arrhythmia detection system over a wireless network, where the data are analyzed and the results are sent to a monitoring agency, and a medical specialist care is requested or an ambulance is dispatched as necessary. The physical entity here is individuals either with or suspected of arrhythmia, and the arrhythmia detection system is a cyber system, and these two interact closely via telecommunications, computing, and control (see Fig. 3) [16, 17].

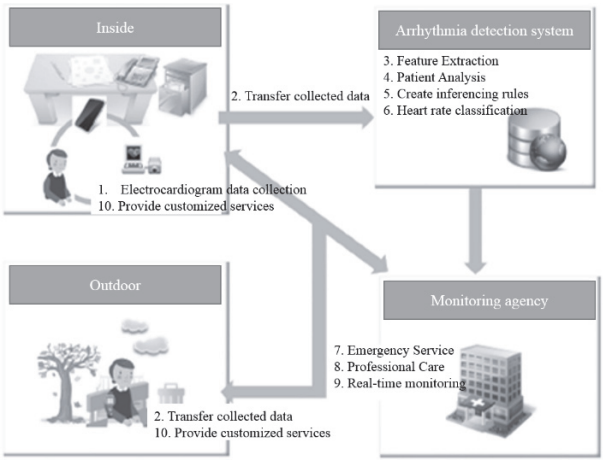

Figure 3 Flow chart of remote electrocardiogram monitoring system

In this paper, a system that is aware of each of the multiple users based on U-health data on the cloud is designed, which provides them with customized control services in real-time.

Previously related research proposed an access control system to protect sensitive data obtained by sensors in IoT environment by situational awareness. It focuses on the management of access privileges which allow or deny access depending on user context, with access control policies that deny access to the data stored in the network for unauthorized users. To that end they analyzed a previously-studied context data access control scheme based on CP-ABE, included dynamic situations within the scope of context data and proposed an extended access control policy that reflects extended multi-dimensional context attributes [18-21].

In the security field, cyber-physical security (CYPSec) was studied in consideration of the interaction between components and the physical environment, as well as the characteristics of the components involved in designing CPS security solutions. CYPSec is a security solution integrated with the environment where the conventional basic security components are used together with the environmental knowledge and information. This means that as a security aim, the complicated and dynamic characteristics of the physical environment can be utilized [22].

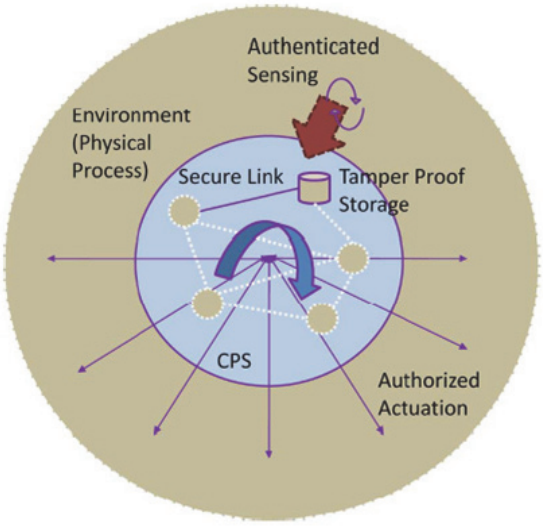

Figure 4 CPS Security Requirements

When it comes to the security requirements of this kind of CPS, there are five aspects: sensing security, storage security, communication security, operation control security, and feedback security. Sensing security deals with the validity and accuracy of the sensing process; storage security prevents cyber and physical breaches of all data stored in CPS; communication security secures internal communications between CPSs from interference and eavesdropping; operation control security ensures that operations do not take place without proper authorization; lastly, feedback security ensures that the control system of CPS is protected, which provides the needed feedback when an operation is being performed (see Fig. 4), [23].

In this paper, a system is designed in which each of the multiple users is recognized by matching data of user with the cloud and which provides real-time control services based on threshold values of different users.

2.2 Fog Computing

To improve the extent of use of things in IoT, things equipped with various sensors and actuators have come on the market, which increased the complexity of the configuration of things and it was expanded to a multi-service IoT system supporting various types of services. As that happened, real-time interactions became impossible with the existing cloud server centric structure. To resolve this, various fog computing models are being studied which disperses roles to fog servers located in a local network [24-27].

That is, fog computing is a concept in which services that were once provided by cloud computing are expanded. It was introduced in order to accommodate the skyrocketing amount of traffic with increasing number of IoT devices and to increase the network capacity. With fog computing, the fog server or node is located near the mobile device, and with the placement of the fog server which enables direct communication with the mobile device, mobile devices can be directly supported. In addition, bottleneck problems with the central processing of cloud computing can be resolved [28-29].

Among the various methods of using fog computing, research on fog computing-based vehicle communication networks and fog networks has been promoted. With regard to the fog computing-based vehicular communication network, with the support for V3V communication needed for vehicle-to-vehicle communication and with the skyrocketing amount of data used by moving vehicles, the fog server is installed on the bus in order to improve the quality of service to users and to reduce the over-all burden on the network. For vehicles like the bus, the latency between terminals can be reduced with the users inside the vehicles and bus users and with the support for V3V communication. Besides on the vehicle, the fog server can be placed in a place with a lot of data traffic like a traffic signal or a bus stop in supporting the vehicular communication network (see Fig. 5).

A fog network supports itself with local proximity and data cache capability. Data are analyzed at the fog server and portions of the data used frequently are stored with the fog server. Then, the data in the cache are sent to the user when requested, reducing network latency and congestion. In this paper, a system that includes fog computing is

designed to reduce the communication latency between the cloud and the device and acquire fast actuating golden time.

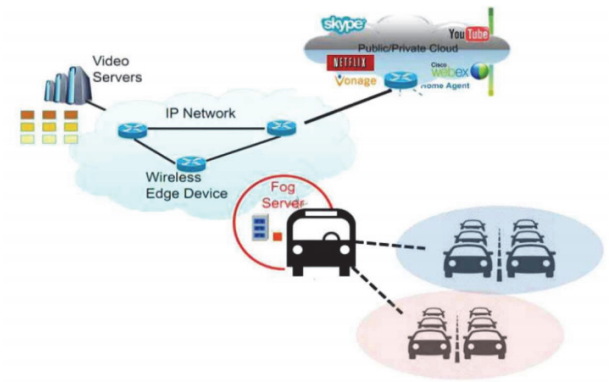

Figure 5 Operation of a fog computing-based vehicular communication network

2.3 Trust Support for SDN Controllers and Virtualized Network Applications

The paradigm of SDN (Software-Defined Networking) allows dynamic reconfiguration of the network using a network application program. SDN is particularly important for NFV (Network Functions Virtualization). While network programming features provided by SDN have various merits, they also cause various threats from potential attacks on the network (see Fig. 6).

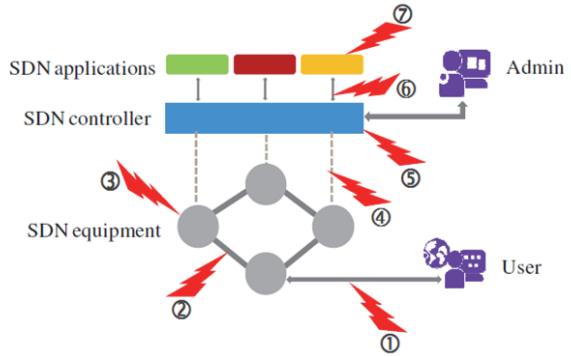

Figure 6 Structure of SDN and security threats

To improve the threat of SDN, a systematic study was undertaken to address the possibility of lack of trust in SDN controllers and applications that use multiple "redundant" controllers that can run in multiple execution environments, rather than a single controller. In this scheme, a network configuration request received by a specific controller is compared with those of the rest of the controllers and the request is actually passed to the network only if it is deemed trustworthy (see Fig. 7), [12].

The Trusted Oriented Controller Proxy (ToCP) is responsible for comparing flow rules from different controllers and installing the most trusted one on the data plane devices. The use of several redundant controllers is connected to the ToCP, and the ToCP gathers and analyses network configuration requests from different controllers. And if ToCP trusts the request it will then enforce it on the respective data plane devices.

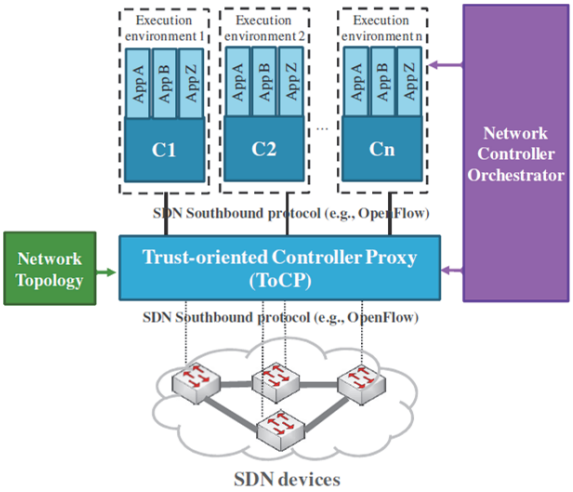

Figure 7 Multi-controller structure

This approach is more of controller to data plane security rather than trust between controller and network application. Nevertheless the ToCP monitors and analyses request coming from network applications emanating from different controllers. One of the limitations of ToCP is the added complexity in accepting requests from multiple controllers. This brings Fig. 5. Application to Control layer threat latency issues in the mechanism which makes it not to scale and suffer from performance issues as traffic increases in the network. Distributed controller implementation brings issues of timing, synchronisation, consistency and coordination. ToCP lacks mechanism that checks the trustworthiness of the network application itself, not the configuration sent by the network application.

2.4 Biometric Sensor Based Authentication

Recently, smartphones using biometric information have been combined with fingerprint sensor-based screen lock apps and various financial services, and non-face-to-face financial services based on biometric information have been started, and authentication systems using biometric information have been developed. It is being actively promoted. Biometric authentication methods based on physical information use fingerprints, irises, retinas, hand shapes, G vein shapes, DNA, brain waves, and the like. This method is relatively stable and utilizes parts with little change in the body of an individual (fingerprint, iris, retina, hand shape, finger vein shape, DNA, brain wave, etc.).

Since generating the user's context information through the user's biometric information is based on accurate information, it is expected to increase the utilization in the field requiring sensitive and accurate context information such as user authentication. However, there is a problem that the recognition of biometric information has a low recognition rate, and in particular, the user's involvement cannot be minimized in the IoT environment because fingerprints, irises, etc. must be directly recognized by user's actions.

The ECG (Electro Cardio Gram) sensor can be used to identify a user by combining the intervals and amplitudes between the points on the ECG waveform, and to identify the user in the shape of the ECG waveform. (See Fig. 8.).

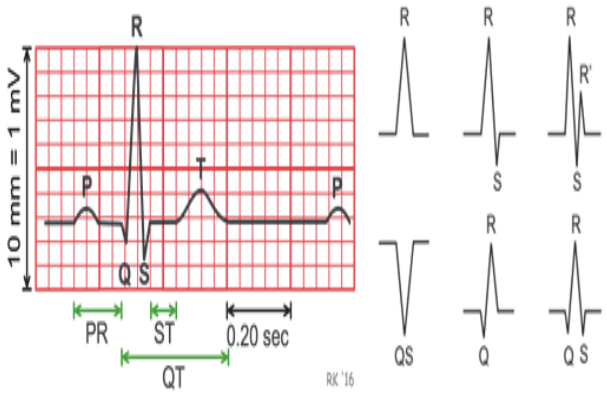

Figure 8 ECG waveform

In this paper, the designed system authenticates the user using biometric information such as the user's electrocardiogram. The average recognition rate of personal identification using electrocardiogram is 92% to 99%, [30].

2.5 Potential Security Threats to the 5G Network

With the growing interest in 5G, the next-generation mobile network, the IoT paradigm is making our daily lives more convenient in all respects, while new security challenges are becoming more serious.

The 5G network has the characteristics of high-speed video transfer due to the formatting of content such as ultra-HD video and the popularization of cloud services. It is said. The basic concept of 5G network is to cope with the development of wireless communication. In other words, it is necessary to comply with requirements such as large traffic capacity and high data transfer rate, increase in the number of users, low delay, low cost and low power consumption. In particular, physical layer security is expected to solve many security problems of 5G networks.

In this paper, we intend to provide security for services provided by Vehicular CPS in 5G environment. In particular, it aims to enhance safety by providing modules to satisfy Authenticated Sensing and Authorized Actuating within the system.

3 STRUCTURE OF BIOMETRIC SENSOR-BASED CPS

3.1 Service Scenarios

In this paper, some assumptions are made about the situations of the user driving a vehicle to come up with the scenarios. Personalization service is a mechanism provided by each vehicle individually. The encrypted data is stored in the final cloud, and the edge computing is used in consideration of the speed of the service.

- The user stores biometric log data on the cloud using a wearable device that they wear as they go about their daily lives.
- When the users get into a rented vehicle or their own vehicle, their wearable device connects to the vehicle via Bluetooth.
- The vehicle, connected to the wearable device of the user, recognizes the user getting onto the vehicle based on their biometric data, and while the user is driving prepares customized control services for them based on their medical conditions.
- During their drive, the user constantly provides their biometric data to the sensor.
- If the vehicle detects biometric data indicating that the user is not fit to drive, such as if the user suddenly drops in their blood-sugar level or heart rate, control services will be provided.

3.2 Design of the System Structure

The system designed in this paper has three different stages to the system domain in representing the data flow (see Fig. 9).

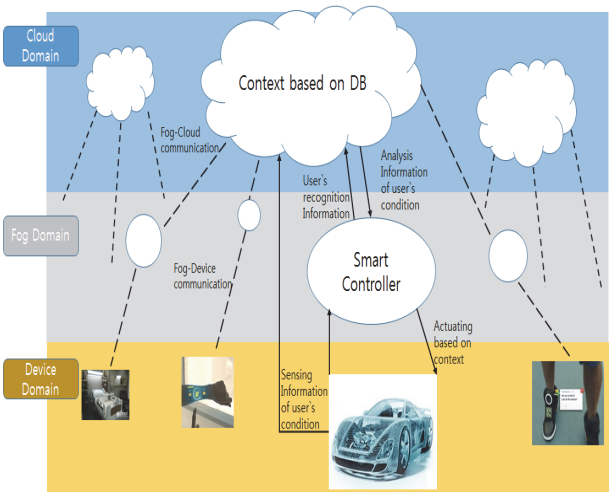

Figure 9 Overall system flow

A cloud domain is where the server is situated, and it has various databases. A fog domain either sends data received from the device domain via the smart controller to the cloud domain or controls the device domain based on the data received from the cloud domain. The device domain sends the sensor data received from the user to the fog domain, which controls the data to control the user.

Fig. 9 shows the overall system flow and Fig. 10 shows the basic structure reflecting that.

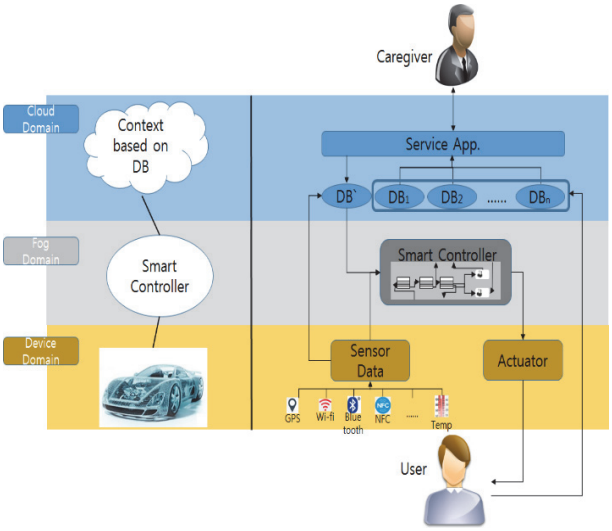

Figure 10 Basic system structure

The cloud domain's DB_1, DB_2, ..., DB_n are sensor log data obtained from the daily life of the user. The caregiver (doctor, nurse, biometric index of inability to drive, etc.)

stores the threshold values of the user's inability to drive in the database using the service app based on the biometric log data and the user's medical data. With the concept of sharing economy, the user of the vehicle can always be changed. Hence, the user is recognized by the vehicle or recognized based on the user's biometric data the vehicle received from their wearable device. Then, the smart controller requests the threshold value from the database. The smart controller of the fog domain sends the control data, determined based on the threshold value, to the actuator to control the user.

The threshold setting can vary depending on the application. For example, the driving environment can be adjusted according to the health condition of the driver of the vehicle. If the driver's blood pressure becomes abnormal, it is *n*-dimensional context information (data that includes information such as temperature and humidity in addition to the driver's blood pressure information) that senses the driver's state information from the car. In this paper, it may be 3D context information. These pieces of information are set in advance so as to satisfy normal operation conditions. In the case of blood pressure, the threshold can be different for each driver. Usually, in the case of high blood pressure patients and low blood pressure patients, adjustment is possible according to the doctor's measures.

3.3 System Module and Detailed Process

Fig. 11 shows the detailed module and process of the designed system.

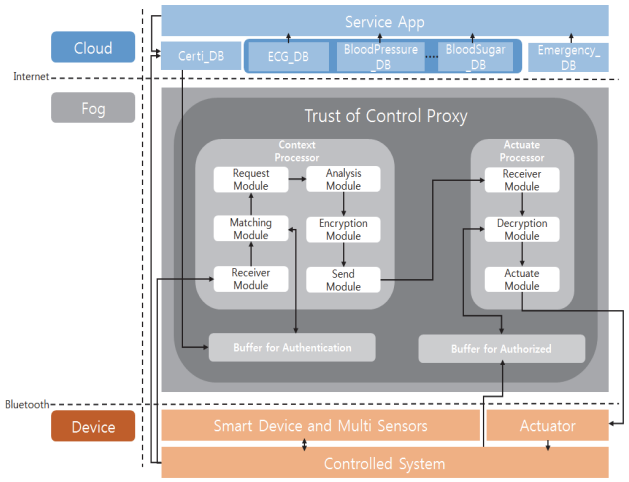

Figure 11 Detailed system module and process structure

The smart device and multiple sensors of the controlled system send the authentication data detected to Certi_DB to request the personal threshold value. The personal threshold value and the user's personal authentication data are sent to the buffer for authentication and stored. The smart device and multiple sensors send to the receiver module of the context processor the personal authentication data and real-time sensor data. The matching module matches the user's personal authentication data stored in the buffer for authentication and mounts the threshold value stored in the buffer for authentication using the request module. Afterward, the analysis module analyzes the risk based on the threshold value and real-time sensor data and if deemed enough of a risk, determines the actuating required. The encryption module encrypts the actuating so determined using the context data for approving the actuating, which is sent to the actuate processor via the send module. The buffer for authorized initializes the context data of the control target in real-time, and stores them. At the decryption module, an actuate approval process is performed in which the encrypted actuating data encrypted using the buffer for authorized are decrypted. Then, the actuating data are sent to the actuator via the actuate module to control the target.

Fig. 12 shows the analysis of whether actuating is needed performed by the analysis module of the context processor using an example in three dimensions.

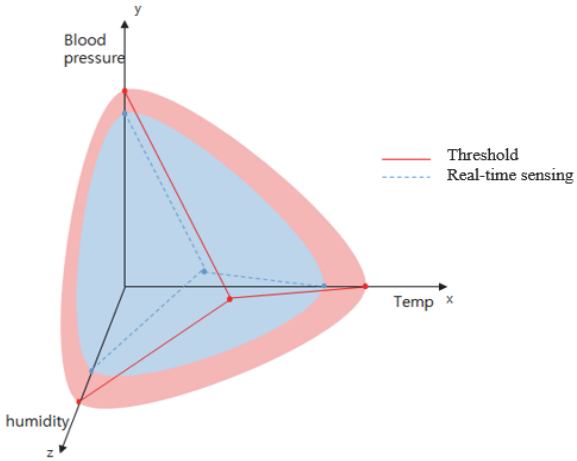

Figure 12 Threshold value and the user's sensor data

The limits of risk with the threshold values associated with the user are set. Whether or not the real-time sensor data exceed the risk threshold is constantly checked. Not all threshold values have to be exceeded for it to be deemed enough of a risk, because the level of risk differs for the multi-dimensional threshold values. While the user may experience a shock after the early signs of a shock manifested in different stages, a shock may also come even without the early warning signs. For example, when the user perspires a lot, their temperature would increase, and with that their blood pressure may also rise; however, even before they have perspired a lot, their blood pressure may rise with a rapid change in their body temperature. In that situation, the judgement that there is no overall risk just because the humidity has not exceeded its risk threshold value is a wrong one. Accordingly, the weights of different threshold values are all different. The context processor determines the required actuating based on the threshold values that exceed the limits and the weights of those threshold values. The determined actuating then gets encrypted and sent to the actuate processor.

3.4 Vector Element for Detection

There is a lot of information that is sensed by individuals. Among them, information used in the medical field to determine the driver's condition includes blood pressure, blood sugar, blood alcohol level, heart rate per minute, respiratory rate per minute, and brain waves. This information can be easily obtained with a compact meter. In the case of blood pressure, more than 140/90 mmHg is defined as hypertension. In addition, when systolic blood

pressure is 100 mmHg or less, it is determined as hypotension. Abnormal blood pressure causes acute heart failure, cerebral hemorrhage, and diseases such as myocardial infarction. For blood glucose, 126 mg/dL of fasting glucose levels and 200 mg/dL of 2 hours after meals are considered diabetes. If you have low blood sugar while driving, you may lose consciousness without any precursors. Blood alcohol concentration refers to the percentage of alcohol in the blood. In general, blood alcohol concentration is used as a legal or medical measure of alcoholism and as a legal measure in drunk driving. Blood alcohol concentration is in mg/100 ml units. For example, if there is 80 mg of alcohol in 100 ml of blood, the alcohol concentration is 80 mg/100 ml. When measuring the alcohol concentration in the blood, the commonly used unit % is applied, 80 mg/100 ml (alcohol content of 0.8 is applied) corresponds to the blood alcohol concentration of 0.1%. Drunk driving reduces the ability to drive and affects the body physically, limiting your visibility and increasing your ability to judge.

If the driver's heart rate and breathing rate increase, it can be assumed that the driver's psychological state is unstable and the mental workload is high. Biosignals for evaluating workload include heart rate per minute (HR), respiration rate per minute (RR), electroencephalogram (EGE), skin conductance level (SCL), skin temperature and the like can be used. The analysis was performed based on pre-measured driving bio-signal and driving performance data for 20 s and 60 s men and women in a simulated driving experiment using STISIM DriveTM (Systems Technology Inc., USA). The ECG signal itself is the relative magnitude of the electrical signal that appears during the heartbeat. By processing the measured data, it is easy to interpret such as heart rate per minute (HR, beat/min), heart rate variable (HRV), and standard deviation of normal to normal (SDNN). Convert it to an evaluation index and use it. It is also used to assess the degree of mental workload through the change in breathing rate (breath/min) per minute. RR is used to assess the degree of mental workload through the change in respiratory rate (breath/min) per minute. In general, it is known that the RR increases as the load becomes higher than during a break. SCL can be used to assess mental workload through measurement magnitude and visual analysis. SCL is an expression that sweat is secreted into the body when the workload increases, and by measuring the electrical conductivity of the skin, the SCL value is instantaneously high when the workload occurs. It is measured and restored to its original level over time.

Therefore, important vector components in this paper are blood pressure, blood sugar, blood alcohol level, HR, RR, SCL. In addition, the degree increases according to the additional medical information.

3.5 Find the Necessary Vector Elements

For the vector element, normalization is required for the values of the three elements as in the following equation.

$$m_p = \frac{\sum(blood\_pressure / unit\_time)}{Number\_of\_unit\_time} \tag{1}$$

$$m_s = \frac{\sum(blood\_sugar / unit\_time)}{Number\_of\_unit\_time} \tag{2}$$

$$m_a = \frac{\sum(blood\_alcohol / unit\_time)}{Number\_of\_unit\_time} \tag{3}$$

$$\sigma_p^2 = \frac{\sum(X_i - m_p)^2}{Number\_of\_unit\_time} \tag{4}$$

The meaning of each term is as follows.

- Number of unit time: Average amount of data per unit time.
- Blood pressure/unit time: Average value of data per unit time.
- $X_i - m_p$: Deviation

Eq. (4) is a value for HR, and RR and SCL, blood pressure, blood sugar, and blood alcohol concentration can be obtained by the same equation. The average data values obtained from the above equations all follow a normal distribution as the amount of data increases. This distribution becomes a standard normal distribution with a mean of 0 standard deviations by standardization. Fig. 13 summarizes the cumulative distribution function of the standard normal distribution in a table.

	0.00	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09
0.0	0.5000	0.5040	0.5080	0.5120	0.5160	0.5199	0.5239	0.5279	0.5319	0.5359
0.1	0.5398	0.5438	0.5478	0.5517	0.5557	0.5596	0.5636	0.5675	0.5714	0.5753
0.2	0.5793	0.5832	0.5871	0.5910	0.5948	0.5987	0.6026	0.6064	0.6103	0.6141
0.3	0.6179	0.6217	0.6255	0.6293	0.6331	0.6368	0.6406	0.6443	0.6480	0.6517
0.4	0.6554	0.6591	0.6628	0.6664	0.6700	0.6736	0.6772	0.6808	0.6844	0.6879
0.5	0.6915	0.6950	0.6985	0.7019	0.7054	0.7088	0.7123	0.7157	0.7190	0.7224
0.6	0.7257	0.7291	0.7324	0.7357	0.7389	0.7422	0.7454	0.7486	0.7517	0.7549
0.7	0.7580	0.7611	0.7642	0.7673	0.7704	0.7734	0.7764	0.7794	0.7823	0.7852
0.8	0.7881	0.7910	0.7939	0.7967	0.7995	0.8023	0.8051	0.8078	0.8106	0.8133
0.9	0.8159	0.8186	0.8212	0.8238	0.8264	0.8289	0.8315	0.8340	0.8365	0.8389
1.0	0.8413	0.8438	0.8461	0.8485	0.8508	0.8531	0.8554	0.8577	0.8599	0.8621
1.1	0.8643	0.8665	0.8686	0.8708	0.8729	0.8749	0.8770	0.8790	0.8810	0.8830
1.2	0.8849	0.8869	0.8888	0.8907	0.8925	0.8944	0.8962	0.8980	0.8997	0.9015
1.3	0.9032	0.9049	0.9066	0.9082	0.9099	0.9115	0.9131	0.9147	0.9162	0.9177

Figure 13 Standard normal table

The probability of this standard normal distribution can be used to convert the values of the vector elements into values between 0 and 1. The elements of a vector can extend to n-dimensional vector elements as the elements increase.

We can standardize the elements by following the steps below.

First, select an element to analyze per unit time.

$$\vec{R} = (P, S, A, ...) \tag{5}$$

Second, standardization of each element

$$z_p = \frac{p - m_p}{\sigma_p} \tag{6}$$

Applying Eq. (6) to all elements yields the value of $z_{(p|s|a|...)}$. All elements of the vector are normalized to values between 0 and 1.

Third, converting values into probability values.

$$P\left(Z \le z_{(p|s|a|...)}\right) \tag{7}$$

$$\vec{r} = \left(p_p, p_s, p_a, \ldots\right) \tag{8}$$

The value of Eq. (7) represents the dark part in Fig. 14.

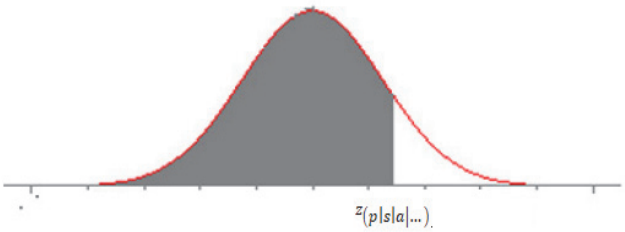

Figure 14 Standard Normal Distribution Curve

When a vector is created with standardized vector elements, the generated values are represented in n-dimensional vector space by the vector elements. When the values expressed in the vector space are orthogonal to each axis, only the value of the vector element remains, and all other elements become 0. For example, orthogonal projection to the HR axis results in $\vec{r} = \left(p_p, 0, 0, \ldots\right)$.

In this way, if the orthogonal vector is obtained for each element and the angle formed by r and the orthogonal vector for each axis is $\theta_{(p|s|a|\ldots)}$, the size of the vector is obtained by the values of $\|\vec{r}\|$ and $\left\|\vec{r}_{(p|s|a|\ldots)}\right\|$.

$$\cos\theta_{(p|s|a|\ldots)} = \frac{\left\|\vec{r}_{(p|s|a|\ldots)}\right\|}{\|\vec{r}\|} \tag{9}$$

$$\|\vec{r}\| = \sqrt{\frac{2\left(p_p^2 + p_s^2 + p_a^2 + \ldots\right)}{n}} \tag{10}$$

Eq. (9) allows us to observe the variation of a particular element with respect to the whole element. Eq. (10) shows the converted value of the vector size so that in the case of n dimension, Fig. 15 below can be applied.

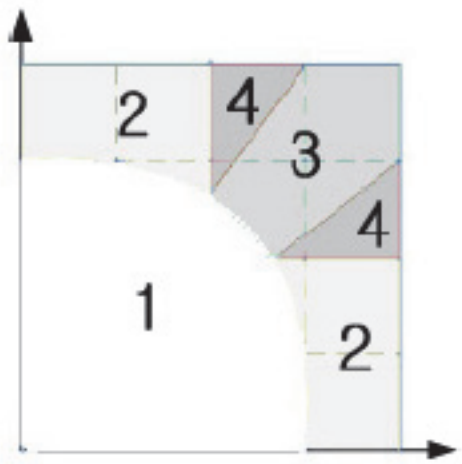

Figure 15 Two-dimensional division of warning areas

The $\|\vec{r}\|$ and $\cos\theta_{(p|s|a|\ldots)}$ values determine the driver's probability of problem. The warning of abnormality determines the path level as follows.

- Level 1 $\left(\|\vec{r}\| \le 0.7\right)$: Indicates the area of 1 and has no effect.
- Level 2 $\left(\|\vec{r}\| > 0.7 \text{ and } p_p \text{ or } p_s \le 0.5\right)$: An area of 2 and rarely occurs.
- Level 3 $\left(\|\vec{r}\| > 0.7,\ 0.6 \le \cos\theta_{(p|s|a|\ldots)} \le 0.8\right)$: This is an area of 3 and the blood pressure and blood sugar values are all slightly increased, so it can be judged as a normal increase, but it may need to be adjusted because it can go into danger stage.
- Level 4 $\left(\|\vec{r}\| > 0.7 \text{ and } p_p \text{ and } p_s \le 0.5 \text{ and } \cos\theta_{(p|s|a|\ldots)} < 0.6 \text{ or } \cos\theta_{(p|s|a|\ldots)} > 0.8\right)$ is due to an abnormal signal

4 EXPERIMENT AND ANALYSIS

4.1 2D Vector Analysis of Driver BioSignal

Assume an abnormal increase in respiratory rate per minute.

In Fig. 16 $\vec{p} = (0.764, 0.812)$, $\vec{p}_p = (0, 0.812)$, $\|\vec{p}\| \approx 1.115$ and $\cos\theta_p \approx 0.684$.

Because it is $\|\vec{p}\| > 0.7$, the heart rate increased per minute, but because it is $0.6 \le \cos\theta_p \le 0.8$, the respiration rate also increased per minute, so it is considered a normal situation and a "Level 3" warning is issued.

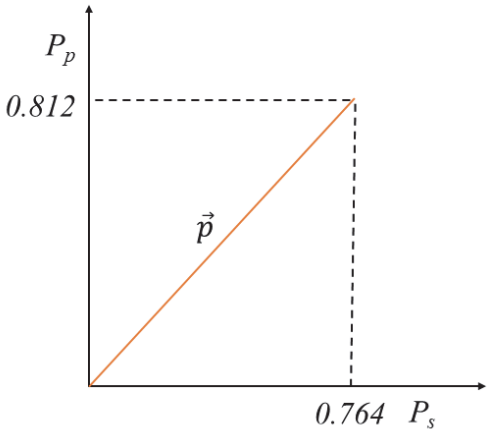

Figure 16 Normal 2d vector

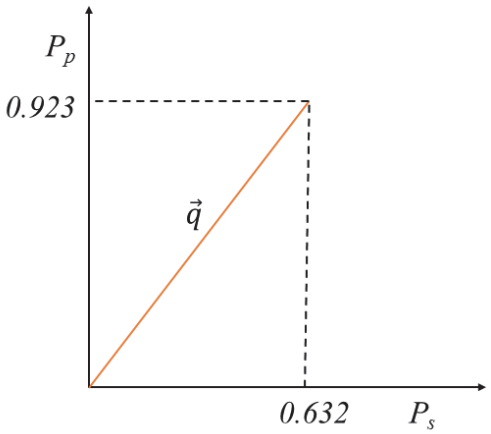

Figure 17 Unusual two-dimensional vector

The case in Fig. 17 is a vector of abnormal situations. $\vec{q} = (0.632, 0.923)$, $\vec{q}_p = (0, 0.923)$, $\|\vec{q}\| \approx 1.118$ and $\cos\theta_p \approx 0.826$. Heart rate per minute increased with $\|\vec{q}\| > 0.7$ and abnormal state with $\cos\theta_p > 0.8$. Thus a Level 4 warning is issued.

4.2 3D Vector Analysis of Driver BioSignal

Assume an abnormal increase in the level of skin conduction. Fig. 18 is a vector of normal situations.

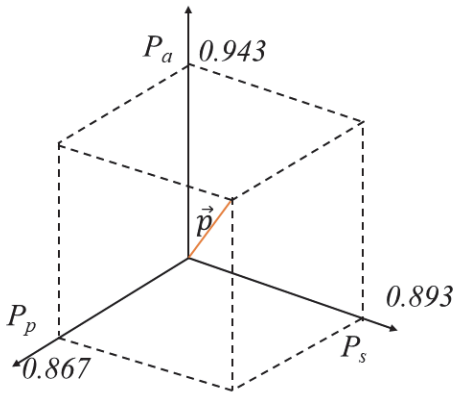

Figure 18 Experiment result

$\vec{p} = (0.867, 0.893, 0.943)$, $\vec{p}_a = (0, 0, 0.943)$, $\|\vec{p}\| = 1.275$ and $\cos\theta_a \approx 0.740$. By $\|\vec{p}\| \approx 0.7$ it can be seen that the heart rate per minute increases. And, it can be seen that the skin electrical conduction level also increased by $0.6 \le \cos\theta_a \le 0.8$. It is assumed to be normal and a Level 3 warning is given.

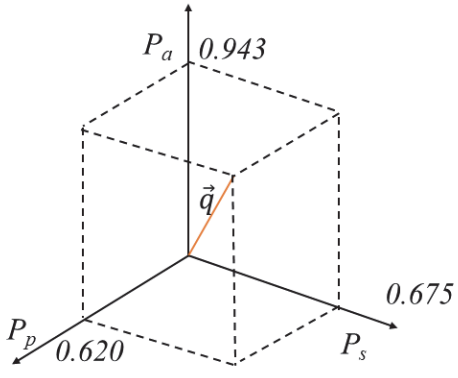

Figure 19 3d abnormal vector

Fig. 19 shows a vector of abnormal situations. $\vec{q} = (0.620, 0.675, 0.943)$, $\vec{q}_a = (0, 0, 0.943)$, $\|\vec{q}\| \approx 1.153$ and $\cos\theta_a \approx 0.817$. It is possible to confirm that the heart rate increases every minute by $\|\vec{q}\| > 0.7$, and is convinced that the situation is abnormal, and warns Level 4.

4.3 Data Transmission Experiment

In this paper, we have experimented with a simulator called Mininet. Mininet is an emulator that allows you to build and test an SDN environment.

We have three SDN controllers in the experiment. The reliability was set to 50, 30, and 30, respectively. The confidence threshold is 70%. Experiments were carried out mainly on the following three points.

The confidence threshold is an average value that allows normal driving depending on the situation. In normal driving to a reliable threshold, blood pressure that can fall into a state where you can't drive may be the limit. Moreover, the combination of these information can correspond to the range of security.

First, the controller sends the same network configuration request without corruption. The confidence level is 100%. Since the trust level is better than 70%, the network is configured with this route. The second one requests that one controller be manipulated to configure a different path from two different controllers. The confidence level is about 72%. Since the trust level is better than 70%, the network is configured with this route. Third, two controllers are manipulated to request that they be configured in different paths. The confidence level is 45%. The network path is not configured be-cause the trust level is lower than 70%.

We measured throughputs obtained by transferring 32 MB and 2.4 MB files, respectively. Measurements were made 100 times each.

Fig. 20 shows a graph of the experimental results.

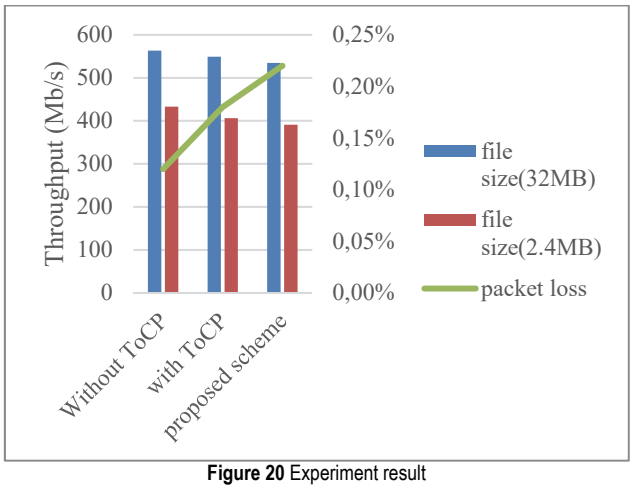

Figure 20 Experiment result

In the experimental results, the difference between "with ToCP" and the proposed scheme is not significant. This is because security techniques are applied additionally. Similar, but the proposed technique may require some additional computation, so there may be some performance degradation. However, it has higher reliability in terms of security.

As security improves, it leads to service degradation. However, it is judged that the deterioration of the service does not hinder the availability.

4.4 Comparative Analysis

Previous work has explored approaches to addressing the potential for lack of trust in SDN controllers or their applications. In this scheme, a single controller is not used. Instead, it uses multiple controllers provided by multiple suppliers which can be run under many different environments. The network configuration requests coming

in from the heterogeneous controllers are analyzed, and if the requests are deemed to be consistent enough and trustworthy enough, the request is passed to the actual network equipment. To allow this kind of analysis and decision-making, a middle layer based on the network hyper visor was introduced, known as Trust oriented Controller Proxy (ToCP). To implement this layer, the feasibility of implementing this scheme was demonstrated, and a preliminary assessment of the costs involved was provided (see Fig. 21), [12].

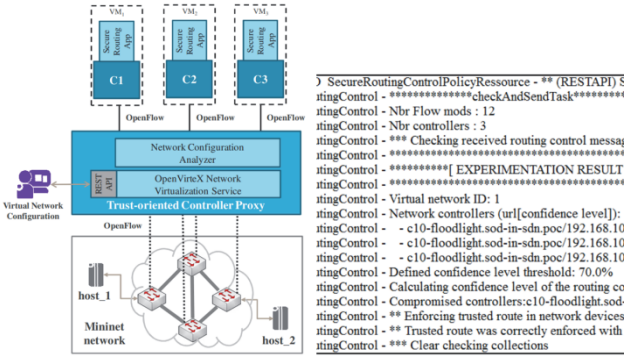

Figure 21 Trust-oriented Controller Proxy Prototype and Experiment

The CPS S3 Solution's official foundation CPS research provides a theoretical framework for cyber-physical interaction that supports the ability to systematically design solutions to ensure safety, security, or sustainability Established. With this framework, CPS researchers can systematically design solutions ensuring safety, security, and substantiality. The general applicability of this framework is substantiated by various example solutions for S3 under the CPS domain. It also provides the insight with regard to the public research problems for ensuring S3 in CPS [22].

With the vehicular CPS system designed in this paper, events that may occur in various driving scenarios with various users are handled by the actuator. With this approach, different users are no longer provided with the same service but there is a sensor data processing mechanism for vehicular CPS with context awareness for multiple users.

5 CONCLUSIONS

This paper proposed a sensor data processing mechanism for vehicular CPS with context awareness for multiple users. Furthermore, user reliability was increased with a privilege grant stage for the actuating determined based on reliable real-time sensor data. The findings of this study may allow reliable processing of IoT services suitable to the context in a 5G environment to make a commercial debut in the future.

For future work, we are going to study access policy algorithms for the sensor data of authenticated sensing and authorized actuating modules for strong security in a future 5G environment. Furthermore, we are going to review the application feasibility of attribute-based encryption for packets of ICN (Information Centric Network)/CCN (Content Centric Network) which are associated with 5G.

Acknowledgements

This research was supported by the Basic Science Research Program through the National Re-search Foundation of Korea (NRF) funded by the Ministry of Education (2019R1F1A1056507). This work was also supported by the Dongguk University Research Fund of 2020.

6 REFERENCES

[1] Oh, J. T. & Kim, K. Y. (2016). Trends of Digital Security Technology. *Electronics and Telecommunications Trends, 31*(5), 110-119.

[2] Cha, H. J., Yang, H. K., & Song, Y. J. (2018). Secure Data Sharing using Proxy Re-Encryption for Intelligent Customized Services. *International Journal of Grid and Distributed Computing, 11*(10), 29-39. https://doi.org/10.14257/ijgdc.2018.11.10.03

[3] Chinthakunta, S. & Chigarepalli, S. B. (2018). Certificateless Dynamic Data Integrity Verification using Lattices in Cloud Storage. *International Journal of Grid and Distributed Computing, 11*(10), 65-74. https://doi.org/10.14257/ijgdc.2018.11.10.06

[4] Yu, L., Chen, B., Huang, B., & Wang, N. (2013). Context-aware access control for resources in the ubiquitous learning system using ciphertext-policy attribute-based encryption. *Context, 6*, 18.

[5] Kim, J. M., Moon, J. K., & Song, Y. J. (2016). A Secure Content Delivery Service in CPS Environments. *International Journal of Security and Its Applications, 10*(9), 257-264. https://doi.org/10.14257/ijsia.2016.10.9.24

[6] Ram, A. & Mishra, M. K. (2017). Position Based Density Conscious Routing Protocol in Vehicular Ad Hoc Networks. *International Journal of Future Generation Communication and Networking, 10*(9), 57-74. https://doi.org/10.14257/ijfgcn.2017.10.9.06

[7] Weber, S. G. (2012). A hybrid attribute-based encryption technique supporting expressive policies and dynamic attributes. *Information Security Journal: A Global Perspective, 21*(6), 297-305. https://doi.org/10.1080/19393555.2012.738374

[8] Minopoulos, G., Kokkonis, G., Psannis, K., & Ishibashi, Y. (2019). A Survey on Haptic Data Over 5G Networks. https://doi.org/10.33832/ijfgcn.2019.12.2.04

[9] Ulz, T., Haas, S., & Steger, C. (2018). Cyber-Physical System and Internet of Things Security: An Overview. *Solutions for Cyber-Physical Systems Ubiquity*, 248-277. https://doi.org/10.4018/978-1-5225-2845-6.ch010

[10] Lu, T., Xu, B., Guo, X., Zhao, L., & Xie, F. (2013). A new multilevel framework for cyber-physical system security. *First international Workshop on the Swarm at the Edge of the Cloud.*

[11] Tan, Y., Goddard, S., & Pérez, L. C. (2008). A prototype architecture for cyber-physical systems. *ACM Sigbed Review, 5*(1), 1-2. https://doi.org/10.1145/1366283.1366309

[12] Betgé-Brezetz, S., Kamga, G. B., & Tazi, M. (2015). Trust support for SDN controllers and virtualized network applications. *Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft)*, 1-5. https://doi.org/10.1109/NETSOFT.2015.7116153

[13] Porter, M. & Heppelmann, J. (2014). Capabilities of smart, connected products. *HBR, 70.*

[14] Wan, J., Zhang, D., Zhao, S., Yang, L. T., & Lloret, J. (2014). Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges, and solutions. *IEEE Communications Magazine, 52*(8), 106-113. https://doi.org/10.1109/MCOM.2014.6871677

[15] Lee, I., Sokolsky, O., Chen, S., Hatcliff, J., Jee, E., Kim, B., & Venkatasubramanian, K. K. (2011). Challenges and research directions in medical cyber-physical systems. *Proceedings of the IEEE, 100*(1), 75-90. https://doi.org/10.1109/JPROC.2011.2165270

[16] Stojanović, R., Škraba, A., Koložvari, A., Kofjač, D., Stanovov, V., & Semenkin, E. Cyber Physical System for Stress Monitoring in Individuals and Groups.

[17] Yu, J., Kuang, Z., Zhang, B., Zhang, W., Lin, D., & Fan, J. (2018). Leveraging content sensitiveness and user trustworthiness to recommend fine-grained privacy settings for social image sharing. *IEEE transactions on information forensics and security, 13*(5), 1317-1332. https://doi.org/10.1109/TIFS.2017.2787986

[18] Song, Y. J., Seo, A., Lee, J., & Kim, Y. C. (2015). Access Control Policy of Data Considering Varying Context in Sensor Fusion Environment of Internet of Things. *KIPS Transactions on Software and Data Engineering, 4*(9), 409-418. https://doi.org/10.3745/KTSDE.2015.4.9.409

[19] Yu, J., Tao, D., Li, J., & Cheng, J. (2014). Semantic preserving distance metric learning and applications. *Information Sciences, 281*, 674-686. https://doi.org/10.1016/j.ins.2014.01.025

[20] Sun, Y. E., Huang, H., Chen, S., Zhou, Y., Han, K., & Yang, W. (2019). Privacy-Preserving Estimation of $ k $-Persistent Traffic in Vehicular Cyber-Physical Systems. *IEEE Internet of Things Journal, 6*(5), 8296-8309. https://doi.org/10.1109/JIOT.2019.2916349

[21] Hussain, M. M. & Beg, M. S. (2019). Using Vehicles as Fog Infrastructures for Transportation Cyber-Physical Systems (T-CPS): Fog Computing for Vehicular Networks. *International Journal of Software Science and Computational Intelligence (IJSSCI), 11*(1), 47-69. https://doi.org/10.4018/IJSSCI.2019010104

[22] Banerjee, A., Venkatasubramanian, K. K., Mukherjee, T., & Gupta, S. K. S. (2011). Ensuring safety, security, and sustainability of mission-critical cyber-physical systems. *Proceedings of the IEEE, 100*(1), 283-299. https://doi.org/10.1109/JPROC.2011.2165689

[23] Eun, Y., Park, K. J., Won, M., Park, T., & Son, S. H. (2013). Recent trends in cyber-physical systems research. *Communications of the Korean Institute of Information Scientists and Engineers, 31*(12), 8-15.

[24] Hong, K., Lillethun, D., Ramachandran, U., Ottenwälder, B., & Koldehofe, B. (2013, August). Mobile fog: A programming model for large-scale applications on the internet of things. *Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing*, 15-20. https://doi.org/10.1145/2491266.2491270

[25] Yi, S., Li, C., & Li, Q. (2015, June). A survey of fog computing: concepts, applications and issues. *Proceedings of the 2015 workshop on mobile big data*, 37-42. https://doi.org/10.1145/2757384.2757397

[26] Bonomi, F., Milito, R., Natarajan, P., & Zhu, J. (2014). Fog computing: A platform for internet of things and analytics. *Big data and internet of things: A roadmap for smart environments*, 169-186. Springer, Cham. https://doi.org/10.1007/978-3-319-05029-4_7

[27] Yin, Y., Zhang, W., Xu, Y., Zhang, H., Mai, Z., & Yu, L. (2019). QoS prediction for mobile edge service recommendation with auto-encoder. *IEEE Access, 7*, 62312-62324. https://doi.org/10.1109/ACCESS.2019.2914737

[28] Kibria, M. G., Fattah, S. M. M., Jeong, K., Chong, I., & Jeong, Y. K. (2015). A user-centric knowledge creation model in a web of object-enabled internet of things environment. *Sensors, 15*(9), 24054-24086. https://doi.org/10.3390/s150924054

[29] Song, Y. J. & Kim, J. M. (2019). Characterization of privacy based on context sensitivity and user preference for multimedia context-aware on IoT. *Multimedia Tools and Applications, 78*(5), 5355-5366. https://doi.org/10.1007/s11042-018-6103-5

[30] Barros, A., Resque, P., Almeida, J., Mota, R., Oliveira, H., Rosário, D., & Cerqueira, E. (2020). Data Improvement Model Based on ECG Biometric for User Authentication and Identification. *Sensors, 20*(10), 2920. https://doi.org/10.3390/s20102920

Contact information:

Hyun-Jong CHA
Department of Multimedia Science,
Chungwoon University,
Michuhol-gu, Incheon-si, 22100, KOREA
E-mail: chj826@kw.ac.kr

Ho-Kyung YANG
Division of Information Technology Education,
Sunmoon University,
Asan-si, Chungcheongnam-do, 31460, KOREA
E-mail: porori2000@nate.com

You-Jin SONG
(Corresponding author)
Department of Information Management,
Dongguk University,
Gyeongju-si, Gyeongsangbuk-do, 38066, KOREA
E-mail: song@dongguk.ac.kr