Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 9932091, 9 pages
https://doi.org/10.1155/2021/9932091

Research Article

A Study on Smart Healthcare Monitoring Using IoT Based on Blockchain

SoonHyeong Jeong,[1] Jun-Hong Shen,[2,3] and Byeongtae Ahn[4]

[1]*Onther Inc., 527, Gangnam-daero, Seocho-gu, Seoul, Republic of Korea*
[2]*Department of Information Communication, Asia University, Taichung 41354, Taiwan*
[3]*Department of Medical Research, China Medical University Hospital, China Medical University, Taichung 40447, Taiwan*
[4]*Liberal & Arts College, Anyang University, 22, 37-Beongil, Samdeok-ro, Manan-gu, Anyang 14028, Republic of Korea*

Correspondence should be addressed to Byeongtae Ahn; ahnbt@anyang.ac.kr

Received 12 March 2021; Accepted 3 May 2021; Published 15 May 2021

Academic Editor: Arun K. Sangaiah

Copyright © 2021 Soon Hyeong Jeong et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Background/Motivation. Recently, a lot of interest in health is increasing due to the technology of the 4th industrial revolution. In particular, personal medical information through intelligent self-diagnosis is emerging as very important. However, such personal medical information causes many problems in security and reliability. *Problem/Issues*. Personal medical information accidents may occur on the server, but most of all, they occur more often in information sharing and data transmission. Therefore, in this paper, blockchain technology is applied to improve the reliability of such personal information management. *Research Objective/Methodology*. For intelligent healthcare incorporating blockchain technology, this study utilized the blockchain-based Internet of Things. In addition, information was accumulated using a number of measurement sensors to analyze individual ECG information. The measured biosignals were monitored for personalized diagnosis by analyzing the fused threshold. *Result*. In this paper, we implemented a monitoring system using measurement sensors to analyze individual biometric information. The implemented system information has improved reliability and security by incorporating blockchain technology.

1. Introduction

Advances in information and communication technology led to Internet-connected devices such as smartphones, home appliances, wearable devices, and the IoT (Internet of Things) [1]. It is a network environment for analyzing data collected by these devices on a platform, processing them into meaningful data, and creating various services. The IoT consists of four layers: application service, platform, network, and device [2]. In particular, the IoT platform serves as a formalizing interface for processing data generated and collected from devices and providing it to application services. However, in this structure, IoT application services have no choice but to rely on the availability of the IoT platform. In other words, the IoT platform is a factor that causes a single point of failure [3]. Therefore, to solve the issues of such a centralized platform, a lot of research has been conducted on the structure of the distributed IoT. The devices also collect sensitive data associated with the users. Therefore, the privacy issue arises in the IoT, and research is being conducted to solve it. In this paper, we consider how to apply blockchain to IoT to solve the two problems mentioned above [4]. To this end, it derives requirements for constructing a distributed IoT and suggests a direction to be studied in the future to build a blockchain-based IoT platform that satisfies the derived requirements. Based on smart health, we plan to implement a monitoring system that predicts users' current state by detecting movements such as falls by acceleration sensors and measuring health conditions with an individual's vital signs such as blood pressure, heart rate, and body temperature [5]. The goal is to measure biosignals through sensor units, transmit them to the control unit via Bluetooth, store them in the database, analyze the stored biosignals, and derive the user's current state. Therefore, personal medical information is top secret. However, the existing system has poor reliability and security. The method

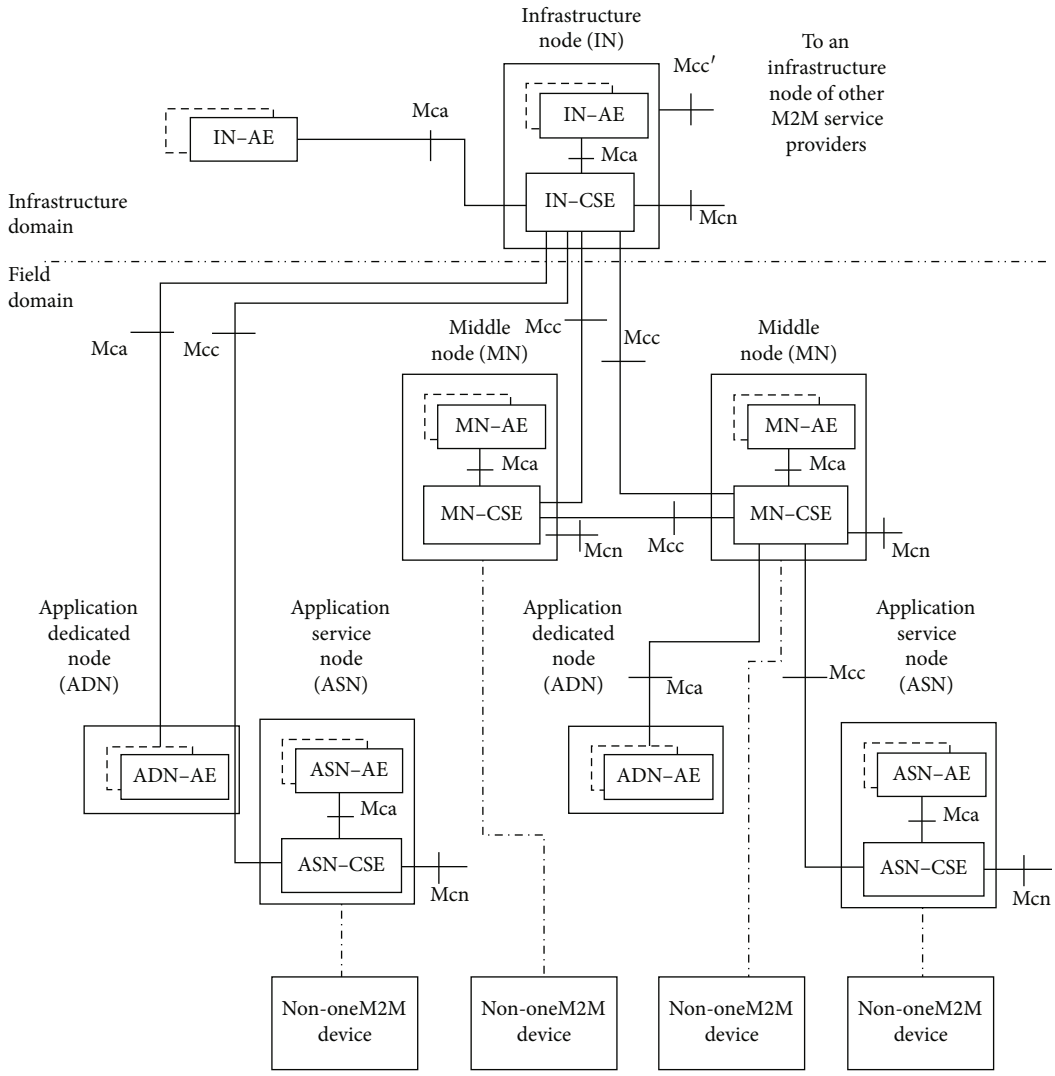


Figure 1: Overall structure diagram of oneM2M (source: ntt-review.jp).

proposed in this paper reinforces reliability and security by incorporating blockchain technology. The structure of this paper is as follows. We discuss the blockchain-based related research and configuration in Section 2 and the implementation of a smart healthcare monitoring system using biosignals utilizing blockchain-based technology in Section 3. We discuss the performance evaluation in Section 4 and present the conclusion and future research tasks in Section 5.

2. Related Work

In the past decade, the IIoT has attracted enormous research attention from both academia and industries and is becoming one of the key technologies to enhance manufacturing and industrial processes. The IIoT presents great promises in accurate and consistent real-time data processing, sustainable and green practices, predictive maintenance (PdM), etc. The IIoT will add £10.69bn to the global economy by 2030. In this section, we explore the structure of oneM2M (Machine to Machine), IoTivity, AllJoyn, and LWM2M (Lightweight Machine to Machine) as platforms that are mainly used in the IoT and study what role blockchain could play in the IoT field.

2.1. oneM2M. In this section, we explore the entire architecture of oneM2M. oneM2M defines a common platform on the IoT that can satisfy the requirements of various services and standardized interworking with other platforms [6]. By defining interfaces for compatibility between various applications, horizontal platforms can be constructed away from the traditional vertical forms of the IoT platforms to prevent fragmentation, reduction development, and operational costs [7]. The requirements are derived by reflecting the use cases of 7 industries such as smart home, smart car, energy, healthcare, enterprise, and public service, and core functions (data collection and reporting function, the remote control of devices, the maintenance of connectivity, security and privacy functions, etc.) and interface were defined [8]. The entity of oneM2M consists of the user/end-user, application service provider, M2M service provider, and network operator. The user/end-

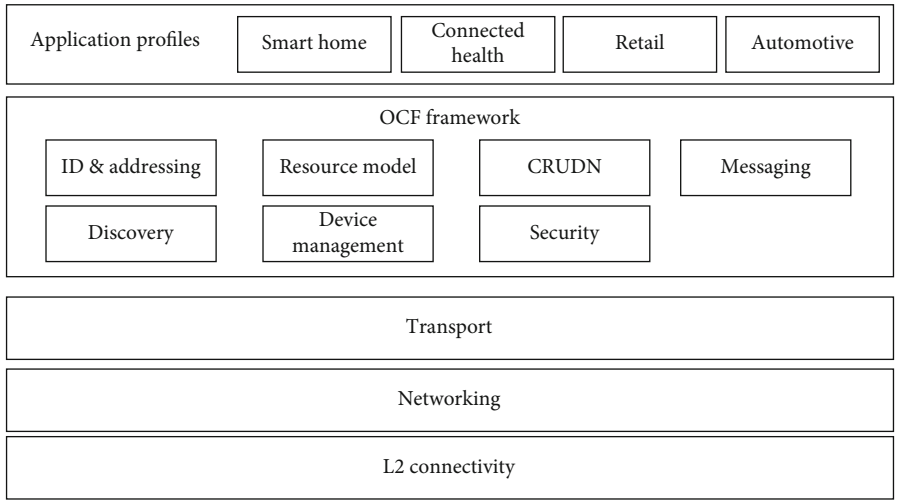


Figure 2: Overall structure diagram of IoTivity.

user refers to individuals or companies using M2M solutions, and the application service provider refers to providers that provide M2M services [9]. The M2M service provider is the principal provider of M2M common services to the application service provider. The network operator is the main provider of the network to the M2M service provider. oneM2M is connected by multiple nodes to form an infrastructure, with one node consisting of AE (Application Entity), CSE (Common Service Entity), and NSE (Network Service Entity) [10]. AE is responsible for application function logic for providing M2M service, and CSE provides 12 common service functions for AE from a functional perspective. NSE provides CSE with network device management and services, and each entity interacts through a reference point. The reference point refers to the connections between CSE, AE, and NSE, which are mapped to the binding protocol for real-world communication. Figure 1 shows the overall structure of oneM2M [11].

In Figure 1, Mca represents communication between CSE and AE, Mcc represents communication between CSE and CSE, Mcn represents communication between CSE and NSE, and Mcc represents communication with other infrastructure domain CSE [12]. CSE provides various common service functions, including Lookup/Discovery/Resolution and CRUDN (Create, Retrieve, Update, Delete, Notify) operations to 12 common service functions based on ROA (Resource-Oriented Architecture).

2.2. IoTivity. Figure 2 shows the overall structure of IoTivity.

IoTivity is composed of the application profiles, OCF framework, transport, networking, and L2 connectivity layers. The application profiles layer executes various application applications such as smart home, connected health, retail, and automotive [13]. As a layer for providing the functions required by an application executed in the application profiles layer, the OCF framework provides ID and addressing, resource model, CRUDN, messaging, discovery, device management, and security functions. The transport layer provides an end-to-end transmission function with specific QoS (Quality of Service) constraints. The networking layer provides the function of exchanging data between devices on a network such as the Internet, and the L2 connectivity layer provides a connection between the physical layer and the data link layer [14].

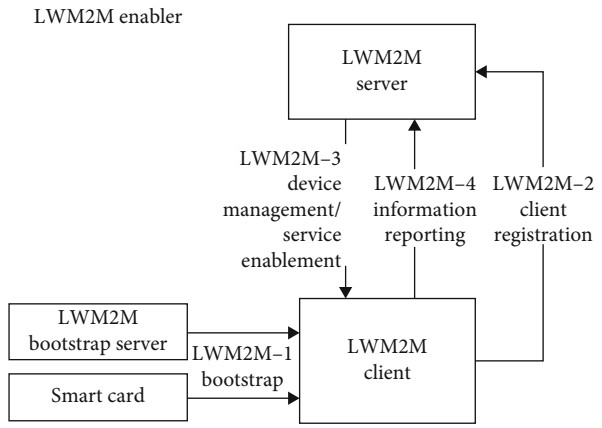


Figure 3: Overall structure diagram of LWM2M (source: http://researchgate.net/).

2.3. LWM2M. Figure 3 shows the overall structure diagram of the LWM2M.

The LWM2M consists of an LWM2M bootstrap server, a smart card, and an LWM2M server/client. The LWM2M enabler describes the LWM2M server and LWM2M client elements. To use the LWM2M, the bootstrap step can be initially optionally performed [15]. The bootstrap phase of LWM2M is the process of predescribing parameters to LWM2M clients to simplify some information or mutual authentication of the LWM2M server. The LWM2M bootstrap server and the smart card are used to perform the LWM2M bootstrap [16]. The LWM2M client performs client registration on the LWM2M server, which provides device management and service enablement functions to manage the LWM2M client. The LWM2M client provides an information reporting function to help

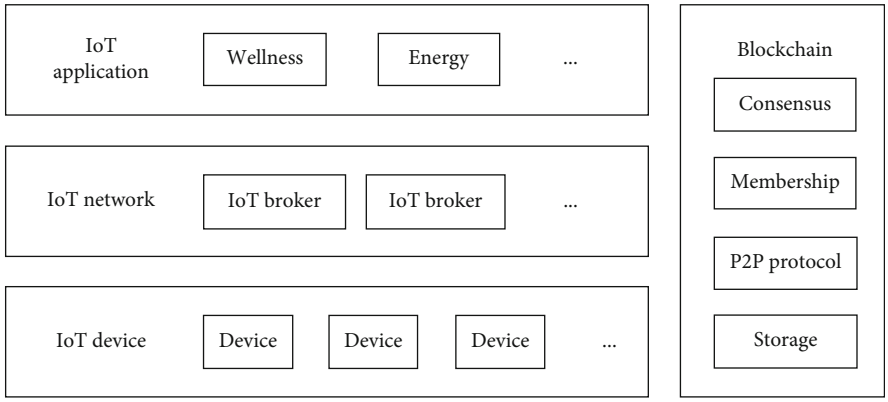


Figure 4: IoT structure diagram based on blockchain.

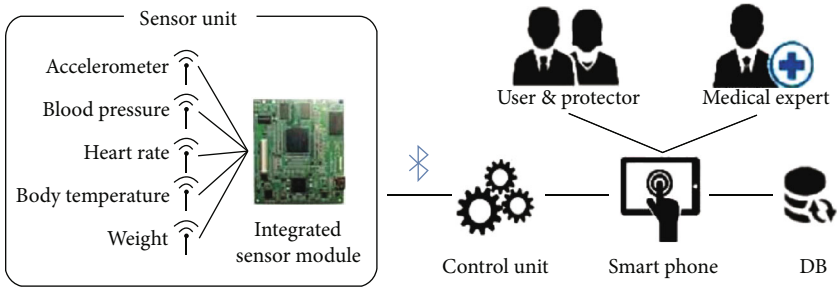


Figure 5: Structure diagram of the system.

resource management of the LWM2M server. In the LWM2M, the M2M user receives services from the M2M service provider, and the M2M service provider provides the LWM2M server and the M2M application service [17]. The LWM2M server can access the LWM2M clients through the network. The LWM2M server is operated by a network service provider, not the M2M service provider, provides the LWM2M server interface to the M2M application service, and performs LWM2M server/client communication.

2.4. Blockchain-Based IoT Utilization. The IoT has received a lot of attention as a technology that will change the future due to the development of small hardware and wireless network technology, but its lack of scalability and security vulnerability due to limited platforms have been pointed out as disadvantages so far [18]. However, it is not an exaggeration to say that the IoT is still the foundation of the 4th industrial revolution, and the IoT is located at the center of the convergence of various ICTs. Blockchain is pointed out as a technology that can highlight the IoT's importance and compensate for its shortcomings. When blockchain is applied to the IoT, various changes occur as, first of all, the centralized structure becomes a distributed structure. First, the IoT devices' connection becomes a P2P structure, making all members of equal status and easing the hierarchy. This will reduce the cost of system construction and maintenance. In addition, new IoT devices will be able to participate in the system without additional equipment such as gateways [19]. Individual IoT devices are vulnerable to security, and there have been attacks on the devices and even the system. In 2016 DEFCON, the demonstration of ransomware demanding bitcoin by hacking Nest's thermostat is a famous example. However, it is meaningless to attack only one IoT device in an environment with the requirements of distributed data blockchain-based decentralized IoT due to blockchain. In other words, even if some of the systems have problems, the entire system is generally safe without being seriously impacted. Therefore, there are various attempts to apply the IoT by converging blockchain [20]. Horizon is an open-source project that attempts to collect and analyze all data by connecting the IoT with blockchain. The nodes participating in Horizon discover each other using Horizon, share their transaction information according to smart contracts, and record them in the ledger. Therefore, all Horizon participants can know one another's transaction details, and the content updated through consensus cannot be forged. Horizon participants are basically divided into producers and consumers, in which the consumers receive the producer's data. For example, if a consumer wants a certain type of data and posts the information on Horizon, it matches with the producer and their transactions are registered in the blockchain to complete the contract. Currently, eight functions are provided, including radio content analysis, aircraft location tracking, and current GPS location tracking by devices. IOTA is a type of cryptocurrency that supports the sharing of resources on the IoT. IOTA implements

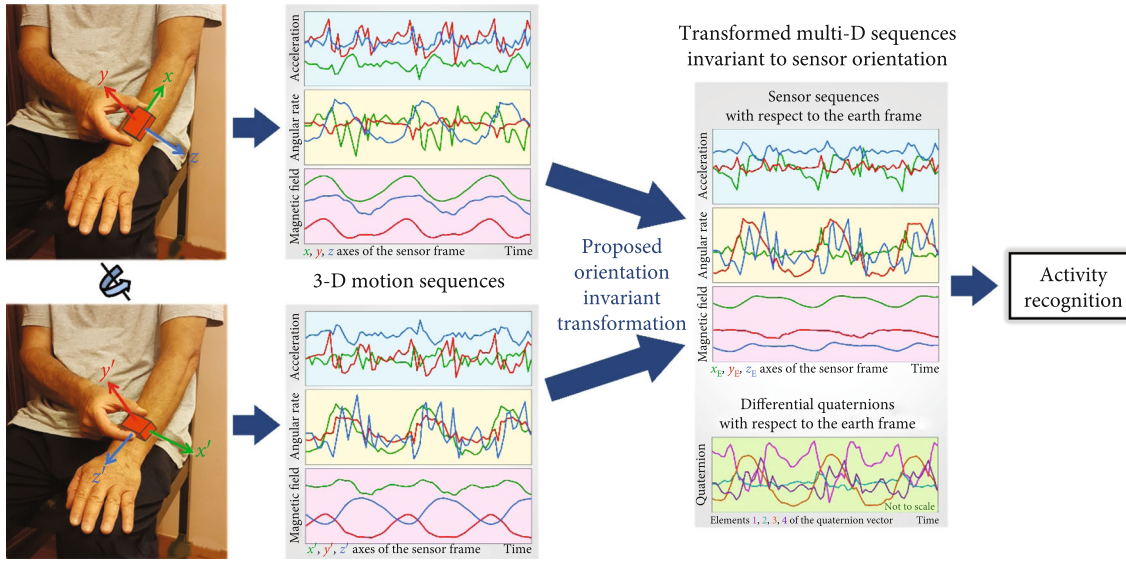


Figure 6: Sensor unit.

Table 1: Benchmark measurement.

Blood pressure measurement	30~280 mmHg, error range ± 3 mmHg
Heartbeat measurement	70 cycles per minute
Body temperature measurement	10~40°C, measurement unit 1.0°C, measurement error ± 0.2°C based on the outside temperature

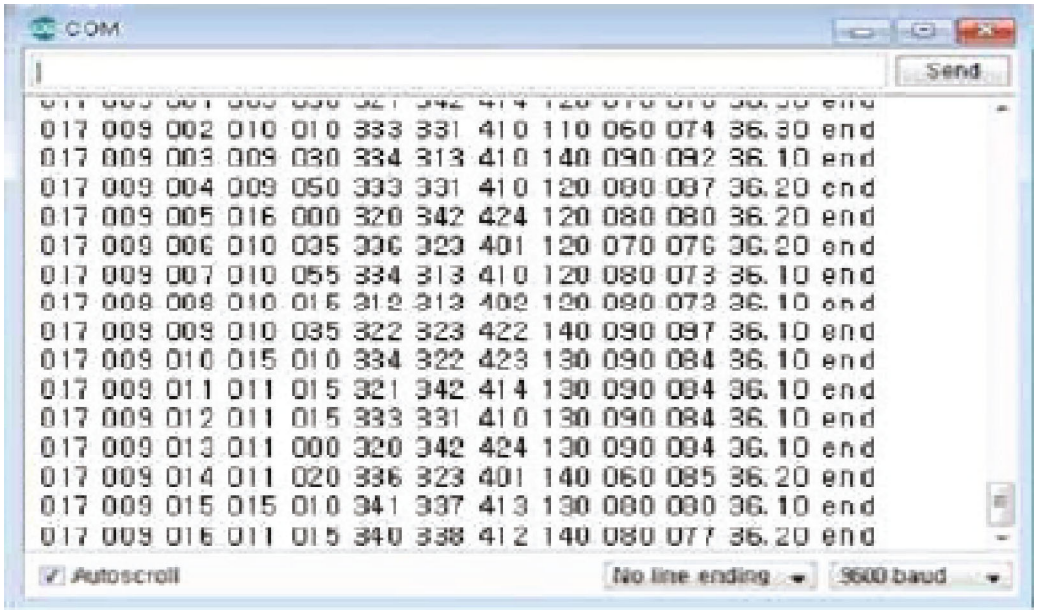


Figure 7: Monitoring control unit.

Table 2: The status of each user's biosignals.

Physical condition		Blood pressure (mmHg)		Heart rate (times)	Body temperature (°C)
		Systolic	Diastolic		
Step1	Good	100-130	60-80	60-90	35.8-38.0
Step2	Unsound	131-149	80-90	91-140	38.1-39.0
	Serious	150-180	90-100	141-180	39.1-39.9
	Emergency	Over 200	Over 100	Over 180	Over 40

blockchain without blocks but is aimed at exchanging resources with one another only through a distributed and shared ledger called Tangle [21].

2.5. Blockchain-Based IoT Platform. This section presents a plan to solve the existing IoT environment, which cannot solve the single point of failure problem in the IoT, through blockchain technology. The IoT environment is divided into four layers: application service, platform, network, and device. IoT big data collected from devices is delivered to the IoT platform through an IoT gateway or broker in this typical IoT platform. The IoT platform mainly plays the role of formalizing data after analyzing and processing it for application services. However, the IoT-based application service receives data from one platform. In other words, all application services are bound to depend on the availability of one platform, which can provide a single point of failure. The IoT platform fundamentally provides a data hub's role, and this paper presents a blockchain-based data hub IoT platform to solve the abovementioned problems [22]. The blockchain-based data hub constructs a blockchain that turns data into blocks by becoming the main body of IoT brokers and application services. While the existing IoT environment had a vertical four-layer structure, the blockchain-based IoT environment horizontally constructs a blockchain layer that can replace the IoT platform. In the blockchain-based IoT architecture, such as Figure 4, data collected from IoT devices is added to the blockchain network either directly or through the IoT network layer [23].

In the IoT application service, data can be imported from blockchain networks instead of the IoT platform. In this structure, the problem with single points of failure disappears, and blockchain technology can be used to ensure reliability and consistency of data.

3. System Configuration and Implementation

The smart healthcare monitoring system we want to implement in this paper consists of a sensor unit that can sense the user's condition, a control unit that can control it, and a monitoring system that can be checked on smartphones. Figure 5 shows the proposed system scheme [24].

In Figure 5, the integrated sensor module collects sensor chip information and stores it in the database through the control device. The stored data provides information to the user in real time through the smartphone.

3.1. Sensor Unit. For the smart healthcare monitoring system, we built and used a sensor module that incorporates each measurement sensor to acquire stream data (systolic blood pressure, diastolic blood pressure, heart rate, and body temperature) [25]. Figure 6 shows the sensor unit.

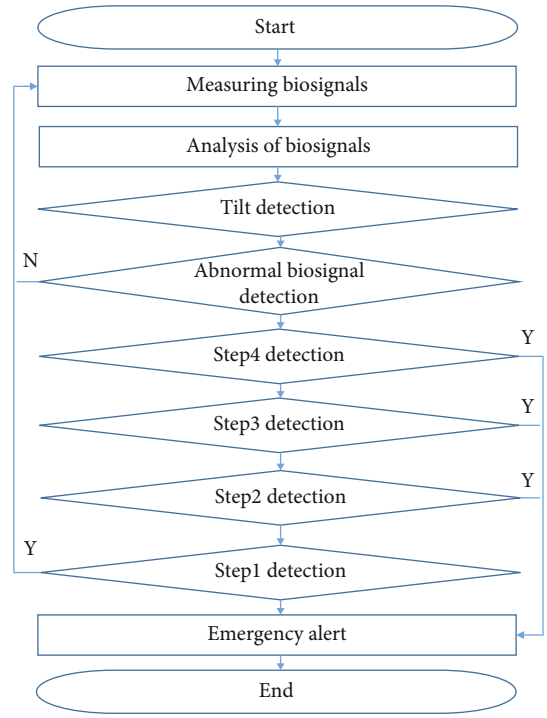


Figure 8: Flow chart of the monitoring system.

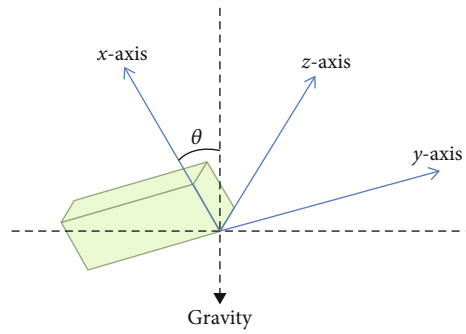
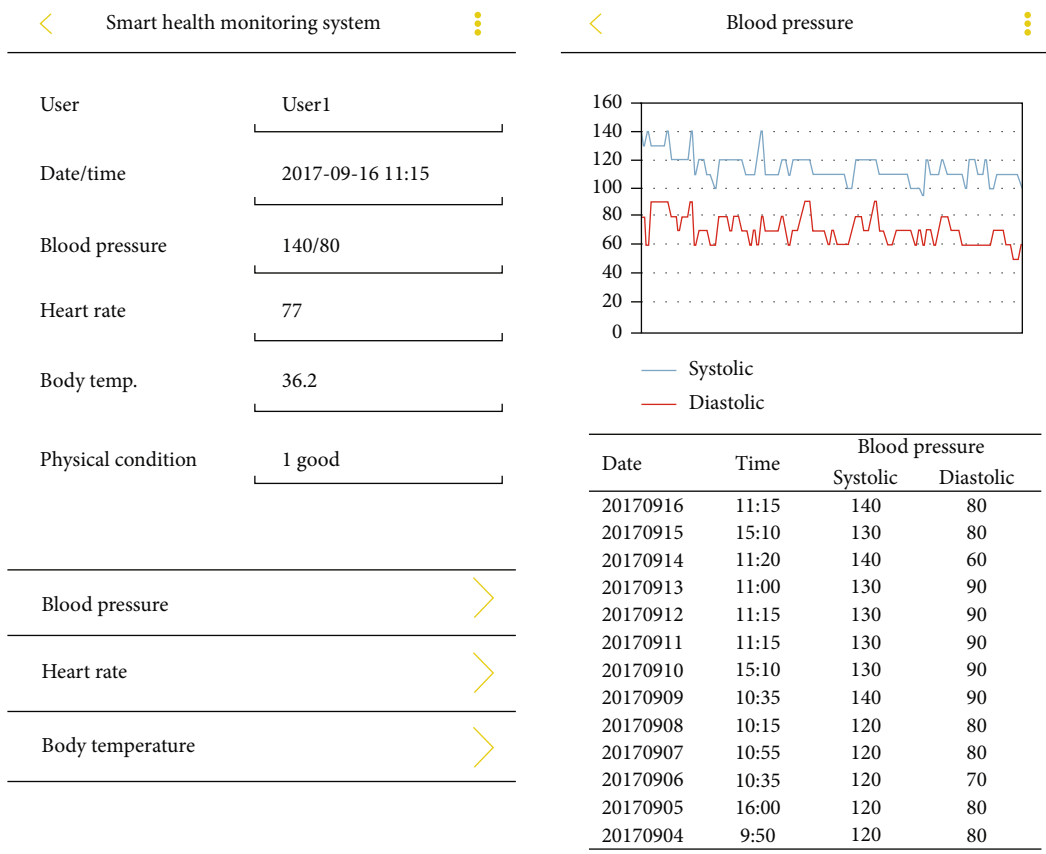


Figure 9: Angle between gravity and the x-axis.

The sensor unit was attached to the wrist to measure the biosignals, and the biosignals were measured with reference to the measurement information in Table 1.

The data used for analysis were data in the same environment, so they were grouped and transmitted in one packet. It



Date	Time	Blood pressure	
		Systolic	Diastolic
20170916	11:15	140	80
20170915	15:10	130	80
20170914	11:20	140	60
20170913	11:00	130	90
20170912	11:15	130	90
20170911	11:15	130	90
20170910	15:10	130	90
20170909	10:35	140	90
20170908	10:15	120	80
20170907	10:55	120	80
20170906	10:35	120	70
20170905	16:00	120	80
20170904	9:50	120	80

Figure 10: Result interface of system implementation based on a smartphone.

Table 3: Data reduction results.

Window size	Reduction ratio	Accuracy
1000	16.4%	0.932
3000	18.9%	0.941
5000	19.2%	0.972
Average	18.2%	0.948

is configured to be processed as a single packet and transmitted in a single packet. Figure 7 shows the sensor value received by the sensor unit [26].

3.2. Monitoring Control Unit. We constructed and used a measurement module that can analyze biosignals received via a Bluetooth module from a sensor unit and output them to a smartphone. We classified biosignals received from sensor units by the biosignal-specific condition of users in Table 2 to determine the degree of risk. We made it determine the degree of risk if two or more biosignals were included in the range [27].

3.3. Algorithm. The algorithm of smart healthcare monitoring systems implemented in this paper is shown in Figure 8.

The proposed algorithm detects abnormal movements such as falls with the sensor values received from the acceleration sensor and analyzes the biosignals after abnormal movements are detected to determine the user's current state according to the user's biological condition as in Table 2. If a three-stage or higher serious condition is detected, an alarm is sent to the user, requesting a response, and alarms and the current condition are also sent to the guardian and medical staff. The value of the three axes measured by the sensor unit's acceleration sensor is converted to an angle to determine the target's posture. The angle measurement using acceleration uses the angle between gravity and the x-axis. The angle between gravity and the axis is shown in Figure 9.

When the user is lying down, the angle between gravity and the x-axis approaches 90°. Therefore, when an abnormal movement occurs, a movement such as a fall of the user can be detected through the angle of the target.

3.4. Monitoring System. In this paper, a monitoring system that allows users, guardians, and experts to check the user's measured biometric information anytime and anywhere using a smartphone was implemented using a JAVA-based Android service environment. Figure 10 shows the implemented monitoring system [28].

In the interface, the current condition of users can be identified by classification of the result of the data, items for monitoring numerical data by an hour and date, and biological signal conditions. In addition, a graph item to view the change of each biosignal was added.

4. Performance Evaluation

To evaluate the system's performance in this paper, we utilized four biometric signals (20,000 systolic blood pressure, diastolic blood pressure, heart rate, and body temperature

datasets) of each of the 50 individuals when an abnormal movement from the sensor unit was detected. In addition, each data was classified into the four conditions of good, abnormal, severe, and emergency, according to an expert's diagnosis. Since the biosignal data used in the experiment used irregular data rather than a linear relationship, the error rate had to be measured. In this experiment, the error rate according to the size change of the sliding window was measured.

Table 3 uses 20,000 datasets and divides the window size from 1000 to 2000 according to the number of tuples and reduces data through SVM algorithm classification. As a result of the experiment, when the size of the window was divided by 5000, the maximum storage space could be reduced by 19.2%, which was more efficient than the size of other windows. The classification accuracy was the highest at 97.2% when the window size was divided by 5000.

5. Conclusion

As the recent population is expected to experience an extremely aging society, the demand for smart medical devices and telemedicine services for constant disease management is increasing, and the importance and necessity of the smart healthcare industry is inevitable to form an active welfare society. Interest in mobile health is also growing in Korea. In this paper, we proposed a smart health-based monitoring system that detects abnormal movements such as falls with sensor values received from acceleration sensors and analyzes basic biosignals of an individual's blood pressure, heart rate, and body temperature after detecting abnormal movements. A monitoring system was implemented using a JAVA-based Android service environment so that users, guardians, and experts can check the user's measured biometric information anytime and anywhere using a smartphone, and the performance evaluation was conducted with biological signals such as 500 systolic blood pressure, diastolic blood pressure, heart rate, and body temperature datasets of 50 individuals. As a result of the experiment, the SVM algorithm for analyzing biosignals showed an average error rate of 2%. When the window size was divided by 5000, it was shown to be effective by reducing the maximum by 19.2% of the storage space. The classification accuracy was the highest at 97.2% when the window size was divided by 5000. Of the total 5000 evaluation data, 84 results came out differently, but there were no significant problems; i.e., the results from the system were lower than the expert's judgment with approximately 98% accuracy. In the future, we believe that a more improved system will be achieved with the addition of ultrasmall biometric sensors and patient positioning functions, the implementation of a home network system using wireless sensors, and a study on the development of an algorithm that can predict fall accidents before they happen. This paper has applied blockchain technology to improve reliability and maintain confidentiality to protect personal medical information. The accumulation of personal medical information is stored in data and monitored in real time using a sensor chip, an Internet of Things technology. Personal medical information is provided through a smartphone in real time.

Data Availability

The source data of this paper used to support the findings of this study have not been made available because a part of the developed source is confidential. No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the Institute for Information & Communication Technology Planning & Evaluation grant funded by the Korea Ministry of Science and ICT (No. 2020-0-00105).

References

[1] M. Kim, "IoT devices grow 2.5x in 2022, expecting half the world's networking devices," Science Times, 2019.

[2] L. Mearian, "IoT can be a blockchain killer app… Active PoC of large companies," IT World, 2018.

[3] B. L. Risteska Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: challenges and solutions," *Journal of Cleaner Production*, vol. 140, pp. 1454–1464, 2017.

[4] Y. Seo, J. Song, and Y. Kong, "Blockchain technology: prospect and implications in perspective of industry and society," SPRI Issue report, No. 2017-004, 2017.

[5] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: the case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 618–623, Kona, HI, USA, 2017.

[6] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, 2019.

[7] P. Manjunath, R. Soman, and D. P. Gajkumar Shah, "IoT and block chain driven intelligent transportation system," in *2018 Second International Conference on Green computing and Internet of Things (ICGCIoT)*, pp. 290–293, Bangalore, India, 2018.

[8] S. Kushch and F. Prieto-Castrillo, "Blockchain for dynamic nodes in a smart city," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 29–34, Limerick, Ireland, 2019.

[9] M. Kim and Y. Kim, "Development of IoT device management system using blockchain DPoS consensus algorithm," *Journal of IKEEE*, vol. 23, no. 2, pp. 508–516, 2019.

[10] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, 2020.

[11] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *Journal of Information Processing Systems*, vol. 14, no. 1, pp. 101–128, 2018.

[12] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2019, 2008, https://bitcoin.org/bitcoin.pdf.

[13] "Introduction to smart contracts — Solidity 0.5.8 documentation," 2019, https://solidity.readthedocs.io/en/v0.5.8/introduction-to-smart-contracts.html.

[14] J.-R. Kim, "Overview of smart healthcare technology," *The Magazine of the IEEE*, vol. 44, no. 2, pp. 18–23, 2017.

[15] K. Tuck, "Tilt sensing using linear accelerometers," Freescale Semiconductor AN3461, 2007.

[16] Y. Liu, R. Wang, H. Huang, Y. Zeng, and H. He, "Applying support vector machine to P2P traffic identification with smooth processing," in *2006 8th international Conference on Signal Processing*, vol. 3, pp. 16–20, Guilin, China, 2006.

[17] D. Zhuang, B. Zhang, Q. Yang, J. Yan, Z. Chen, and Y. Chen, "Efficient text classification by weighted proximal SVM," in *Proceedings of the Fifth IEEE International Conference on Data Mining*, pp. 538–545, Houston, TX, USA, 2005.

[18] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[19] D. Christin, A. Reinhardt, P. S. Mogre, and R. Steinmetz, "Wireless sensor networks and the Internet of Things: selected challenges," in *Proceedings of the 8th GI/ITG KuVS Fachgespräch Drahtlose sensornetze*, pp. 31–34, Harburg, Germany, 2009.

[20] M. J. Covington and R. Carskadden, "Threat implications of the Internet of Things," *Cyber Conflict (CyCon)*, pp. , 20131–12, 2013.

[21] A. Alcaide, P. Esther, M. José, and R. Arturo, "Anonymous authentication for privacy-preserving IoT target-driven applications," *Computers & Security*, vol. 37, pp. 111–123, 2013.

[22] X. Lin, S. Lin, and Q. Haipeng, "Insecurity of an anonymous authentication for privacy-preserving IoT target-driven applications," *Computers & Security*, vol. 48, pp. 142–149, 2015.

[23] J. B. Bernabe, L. H. Jose, V. M. Moreno, and A. F. S. Gomez, "Privacy-preserving security framework for a social-aware Internet of Things," in *International conference on ubiquitous computing and ambient intelligence*, pp. 408–415, Cham, 2014.

[24] A. Ukil, S. Bandyopadhyay, and A. Pal, "IoT privacy: to be private or not to be private," *Computer Communications Workshops (INFOCOM WKSHPS)*, pp. , 2014123-124, 2014.

[25] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[26] M. Singh and S. Kim, "Blockchain based intelligent vehicle data sharing framework," 2017, https://arxiv.org/abs/1708.09721.

[27] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. M. Goldrick, "Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels," 2017, https://arxiv.org/abs/1704.02553.

[28] R. W. van der Heijden, F. Engelmann, D. Mödinger, F. Schönig, and F. Kargl, "Blackchain: scalability for resource-constrained accountable vehicle-to-X communication," in *Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, pp. 1–5, Rennes, France, 2017.