Research Article

International Journal of Advanced Computer Research, Vol 9(40)
ISSN (Print): 2249-7277 ISSN (Online): 2277-7970
http://dx.doi.org/10.19101/IJACR.SRS16001

An empirical analysis on medical information sharing model based on blockchain

Sung-Hwa Han[1*], Ju-Hyung Kim[2], Won-Seok Song[3] and Gwang-Yong Gim[3]
Research Scholar, IT Policy Management, Soongsil University, Korea[1]
Representative Director, Korea Library Information Center Co. Ltd., Korea[2]
Professor, Department of Business Administration, Soongsil University, Korea[3]

Received: 24-June-2018; Revised: 30-August-2018; Accepted: 15-November-2018

Abstract
As the use of medical information improves, medical research is stepping up and legal disputes are rapidly increasing due to the broadening medical accidents. At the same time, there are security threats against the distribution of medical information by non - medical personnel, the forgery, and the difficulty of tracking. Blockchain based medical information sharing model is proposed to cope with such security threats. In this paper, the medical information sharing model based on blockchain is verified its effectiveness by actual implementation for it can or can't satisfy the security requirements for medical information. As a result, it has been confirmed that the blockchain based medical information sharing model can provide the reliability and traceability of medical information, and provide a data recovery function for the prevention of forgery and alteration of medical information.

Keywords
Medical information, Forgery prevention, Integrity, Information sharing service model, Blockchain.

1.Introduction
Healthcare is not only a requirement for the extension of life, but also an integral part of personal happiness. Currently, medical services are rapidly expanding with the increase of medical personnel and the development of medical technology, which are the result of the development of medical technology. The development of medical devices, and the improvement of medical services. The development of medical service gives positive effect, but it provides negative effect too. Although administrative, technical, policy, and financial problems are being reinforced, it is pointed out that medical disputes caused by medical accidents are consistently increasing, and loss of medical research due to data error results in loss. In order to solve this problem, it is indispensable to satisfy the reliability, integrity and traceability of medical information used in medical research and medical disputes, and a method of applying blockchain technology to medical information service is proposed as a technical alternative.

In this paper, to prove effectiveness proposed blockchain based medical information sharing model to meet the security requirements of medical information, we build real service and analyze that it is able to meet or not security requirement.

Section 2 explains the concept of medical information, health information service status, security threats to medical information, and security requirements for medical information. Section 3 specifies the blockchain based medical care Information sharing model and service structure are described. In section 4, we implement real service, according to block chain based medical information sharing model and verify the security requirements of the proposed model. Section 5 epitomizes the application of the proposed medical information sharing model and future research directions.

2.Related researches
2.1Concept of medical information
Medical information is defined as medical record about a patient, or information for medical service itself. Current medical information includes basic information, including the occupation, residence, sex,

*Author for correspondence

and age of the patient, insurance and welfare information, medical background information, medical administration information on the patient, and death information. Therefore, medical information is treated as personal information by law [1]. Now, the electronic medical record (EMR) using a patient's medical record as the form of electronic text has been advanced to the electronic health record (EHR) showing the information about an individual's health status, and in the later days, as the increased wearable devices, Internet of Things (IoT) and smart devices, the medical information range is expanded up to the personal health record (PHR) including a patient's all physiological information [2].

2.2Status quo of medical information service

Currently, medical information is used in various fields. Nowadays, standardization and exchange activities such as medical research, invention of medicines, development of preventive or cure technologies for diseases are continuously increasing for public benefit like discovery and improvement of medical services [3].

These improvements of medical service are based on highest quality of medical information. There were a lot of tries to create medical information standard and to apply many organizations. As a result, medical information standards like digital imaging and communications in medicine (DICOM) or health level 7 (HL7) is created and applied to many medical information systems [4, 5]. Now, new researches are created and continued for analyzing genes and predicting diseases as well as improving the quality of medical life based on the patient's daily life data and their medical information by connecting with the machine learning technology, beyond the level simply utilizing accumulated, stored medical data [6].

2.3Security threat against medical information

The increase usage of medical information does not represent only a positive aspect. With the development of medical services, the negative aspects are emerging, and the frequency is also increasing.

Various internal and external security incidents are continuing, such as the medical information system itself being infected with malicious code and failing to function properly anymore. Instead of simply ending with leakage of personal medical information, misuse of personal information contained in medical information leads to incidents such as various insurance premium fraud charges, personal identity fraud, and excessive medical charges [7].

For protecting medical information, the ISO/TS 27799 was set as the standards, and the cyber security framework in medical service field (ISO/ICE013636) and the health device management & certification technology (HDM) were set and have been gradually expanded [8].

As medical information services are developed, there were security threats. As the concept of PHR has been expanded, there has been created and distributed medical information by non-medical service person. Such kind of information does not have any significant meaning to an individual, but they are raw-status information not being created and not verified by medical service professionals. Hence, in case of applying such raw-status information to a medical research, there may be drawn wrong research results. As medical research activities, by themselves have considerable high opportunity cost, so wrong results from a research may incur significant time and monetary losses to medical institutes or medical device developing companies [9].

Besides, the medical information is utilized to medical disputes, so its authenticity is emphasized. The medical information is basically encrypted and stored, but in special cases, the information storing techniques like the digital signature or the digital right management (DRM) are applied.

However, the encryption storage method which is currently used can modify the information as long as the administrator right of storage system is obtained. As the digital signature (electronic signature) uses a medical service personnel's authentication and applies a private authentication based on its nature, so if a patient's medical record in the system which stores medical records are modified and a medical service personnel's signature is regenerated, then the existing medical record can be replaced with the modified one. And for the DRM system can't be modified arbitrarily by the authority of medical service personnel, but if receiving its developing company's technical support, the past medical record can be modified [10].

2.4Security requirements about medical information

Medical information is always belonging to individual. According to the privacy information security laws, all information that identifies a

particular individual should be given a duty to be safeguarded. The category of medical information also includes information that can identify a particular individual, so it must be protected according to law [11].

Before using EMR, a medical service personnel manually wrote medical records in the form of hard copy, so as long as that the created medical records could meet the requirement of physical stability, then they could enough meet the security level having been generally required by society. However, due to the expansive spread of the internet, now, there are increased security threats by the increased malicious codes like various PC viral and worms, the distribution of unreliable medical information, and the environment in which large information can be easily taken out. That is, compared to the past state, it can be said that the current security level is enhanced in absolute term, but their security effects are relatively insufficient [12].

Medical information being used in medical institutes should basically secure the integrity, the usability as well as the confidentiality, and additionally, should require the security characteristics like access control and audit. Also, it emphasizes that the medical information, it should secure its reliability for reducing the loss of social welfare [13].

3.Blockchain based medical information sharing service architecture

3.1Blockchain platform

As a kind of distributed database, the blockchain technology is the ledger sharing technology that recorded changes in a certain information like addition, modification or deletion in the block unit and mutually shared/managed them. Here, the ledger means a list of transactions, but if it can be interpreted as the sharing information, the blockchain technology can be applied to the all data [14]. The information sharing based on the blockchain technology is achieved by verification and agreement between the information generator and its sharer. In the past, after saving certain information to certain storage, and then the user contacted the storage and accessed the shared information. But, in the blockchain based information sharing architecture, after coping an information to share, its generator distributes it to a sharer and then the sharer verifies the received information and saves it internally in a chain way. Like this way, the information is shared [15].

The reason that the blockchain is recently highlighted because of the blockchain's security features. On the blockchain network, chain information being stored in a certain node is possible to be forged by an unauthorized attack. However, as the principles of Proof of Stake (PoS) and Proof of Work (PoWax) are applied to the blockchain network, so any forged block being occurred in a node is rejected. In order to apply the forgery of certain information to the entire blockchain network, the chain information in the entire node should be forged at the same time, but that is practically impossible. Due to such mechanism, the blockchain technology is evaluated as a technology to satisfy the integrity requirement for sharing information. The way modifying and processing information on the blockchain is the way continually adding blocks without deleting or modifying any existing block. Thanks to this feature, it is possible to trace information-specified life-cycle only with the chain management technology without the need to implement a separate version management.

Due to these advantages, the blockchain is applied and expanded to an information service requiring the certificate/verification of sharing information, and now, the blockchain is being developed and advanced through many open projects like IBM's HyperLedger or Ethereum, Chain Core or Openchain [16].

3.2Structure of blockchain based medical information sharing service

A number of trails are carried out for meeting the requirements of medical information which are above described, and in recent, the movement applying the blockchain technology to the medical information service is often appeared. Especially, it is analyzed that the application of blockchain technology to the medical information service has high potential to contribute to the expansion of the mutual operation resulting from the medical information shared and the advancement of medical technology field [17].

The blockchain technology can be applied to the EMR, a representative medical information service. Blockchain based medical record sharing service can be become a patient node generating or using medical records to share with the blockchain network which is composed of blockchain services.

The medical record sharing has gone through the following process. First, the medical information being recorded by a medical institute is generated as a block, and then is transmitted to the blockchain

network and is shared there. The medical information is divided into the metadata and the general data again, and the both kinds of data are stored in the provider node's repository, respectively. In case of utilizing and verifying the medical information, a patient node accesses to the provided node and inquires or requests to verify his/her wanting medical information. On being requested, the provider node transmits or verifies the corresponding medical information according to the patient node's request [18].

4.Verification of the effectiveness of blockchain based medical information sharing architecture

In order to verify the effectiveness of blockchain based medical information sharing model, we first confirm the vulnerability through verification of the electronic signature forgery attack to existing medical information sharing method. For each of the blockchain based healthcare information sharing schemes, we try to share medical information by unauthorized persons, forgery of medical information, and trace the history of medical information.

4.1Forgery attacks against digital signature

As the above mentioned, the medical information can be generally stored in the database after being encrypted or can be applied to the digital signature or the DRM technology. Representatively the digital signature way is known about the safest way. In relation to that, this paper checked out whether a digital signature could be forged.

Figure 1 is a case showing that already generated medical information is enabled to be forged. Though the forged medical service provider's ID and the medical information ID and its generation date and time are the same with the original medical information, but the both digital signatures are different. Even though the digital signature way is applied, when a hacker has modified the already generated medical information and generates a new digital signature using the medical service provider's certificate, then the original medical information can be forged.

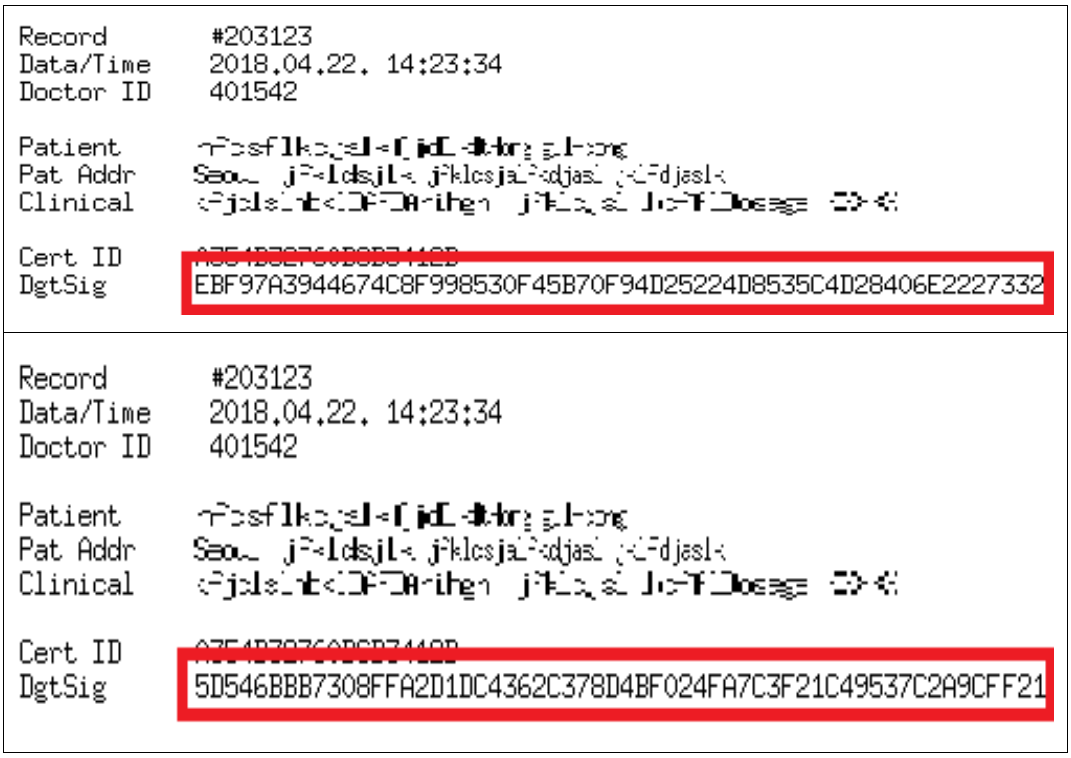

Figure 1 A forgery attack against the medical information applying the digital signature way

4.2Verification environment and verification scenario for blockchain based medical information sharing architecture model

In order to verify whether the proposed blockchain based medical information sharing architecture model meet the security requirements of reliability, integrity and traceability, this paper consisted a provider node as seen in the *Figure 2*.

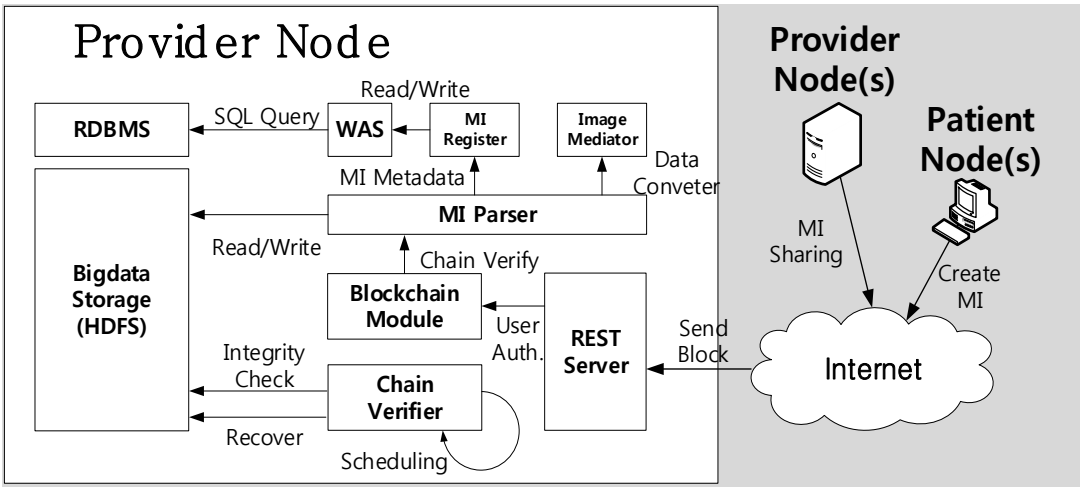

Figure 2 Verification environment for blockchain based medical information sharing model

A repository stores a medical information chain and its metadata respectively by applying the big data platform and the relational database management system (RDBMS). A blockchain module is implemented as a server daemon receiving and verifying the medical information block being transmitted by a patient node or server in remote places. The chain verifier is a daemon in scheduling way, and periodically verifies the integrity of the medical information chain in the Bigdata Platform. *Table 1* is a scenario verifying whether the security requirements are met, and the tests in the table were carried out according to the verification order on the basis of presumptions for 3 scenarios' respective security threats and their verifications by scenario.

Table 1 Verification scenario

Verification scenario	**Medical information spread by non-medical service person**	**Forgery attack against medical information, its detection and recovery**	**Identification of medical information history**
Security threat	Non-authorized person can generate and spread non-reliable medical information	Medical information can be non-authorized, forged by a malicious attacker	The authenticity of newly generated medical information is doubted
Assumption	Non-authorized person possesses a separate certificate and also has the information about the provider node	Malicious attacker can arbitrarily access to the repository that the medical information is stored and can modify the information	Accesses to the medical information and separately store the information's processing history
Verification order	1) Non-authorized person generates a block about medical information in utilizing a X.509 - based certificate. 2)Transmit the newly generated block to the known blockchain node	1)Malicious attacker accesses the repository of provider node 2) Forge the signature values of some nodes in the stored chain. 3)Inquires the results of periodical integrity test about the blockchain	1) Inquires the processing, integration & modification history of a certain medical information

4.3Verification results of proposed model

The proposed model satisfies the security requirements for medical information in response to the security threat described above.

4.3.1Spread of medical information by non-medical personal

If a user wants to generate a chain about certain medical information and wants to store the chain in the blockchain repository, the blockchain module should receive and verify the chain first of all. As medical information being generated by a non-registered medical service provider can't be received, so the blockchain module should abolish the corresponding chain on receiving it as seen in the *Figure 3.*

```
=== Recv Chain Start ===
Recv ChainID    34A1258DA4F900E1D325768DFA998123
Data/Time       2018.04.23. 13:42:21

=== Digital Signature ===
Cert ID         F7815B993316500B7
Valid Check     Invalid
Result          Drop Block - 34A1258DA4F900E1D325768DFA998123
```

Figure 3 Detecting and blocking any generation and registration trial of non-authorized medical information

4.3.2Non-authorized medical information's forgery attack, and attack detection and recovery

Some chains of medical information being stored in the blockchain repository may be modified by a malicious attacker. In order to counter such a security threat, the chain verifier periodically verifies the integrity of all chains in the blockchain repository. In case of detecting a forgery trial in a certain chain as seen in *Figure 4*, the chain verifier deletes the all chain data being stored after the corresponding chain, and request to provide the all data after the corresponding chain to the blockchain node.

```
=== Integrity Check ===
Time    2018.04.25 10:43:45

Check Chain ..............................................

Violation Detected
Chain ID : C8EDCEB2778BCED84A31DCFED83773852BE14CE4F7

Erase ..............
Erase Completed.

Request Block to other.
Req Chain ID : C8EDCEB2778BCED84A31DCFED83773852BE14CE4F7 .... Confirmed.
Req Chain ID : 9020C540817BB59D8B13374E9CEBCE50D5228D6E24 .... Confirmed.
Req Chain ID : 68CE8B90A7FE4FACA1653B5E215239BD4B9571EAB3 .... Confirmed.
```

Figure 4 Verification and recovery of integrity of shared chain

4.3.3Identification of medical information history

At requiring the authenticity of newly generated medical information, the corresponding medical history information can be verified through the entire inquiry by inquiring the medical information index link of chains being stored in the blockchain repository. *Figure 5* shows the modification history of newly generated medical information.

In the medical information index link, it can be inquired what process current medical information goes through from the first generated medical information. Additionally, the newly generated medical information's integrity and traceability can be secured because other medical information being applied to the processing process of medical information can be inquired together.

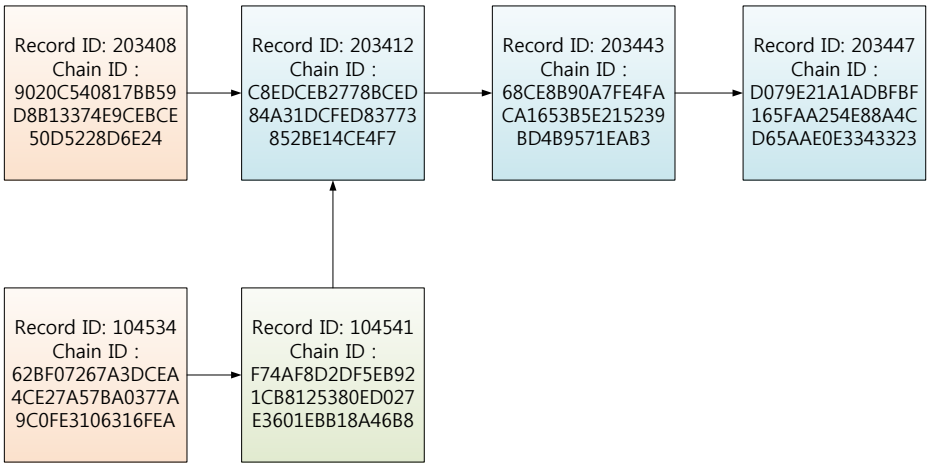

Figure 5 Modification tree of new medical information history

5.Conclusion

When blockchain technology is applied to the medical information sharing service, it is possible to transmit / store the medical information for each existing medical institution in the existing center, and to have the effect of the distributed database that can detect and restore the integrity violation. It is confirmed that the reliability of medical information distributed can be secured through subject verification. In addition, since the entire history of accessing, processing, and disposing of medical information is managed by the chain, it is possible to simultaneously provide the medical information audit function, thereby satisfying the security requirements described above.

However, since the block chain technology does not provide confidentiality function itself, it is necessary to apply encryption storage and network.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Sweeney L. K-anonymity: a model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems. 2002; 10(5):557-70.

[2] Heart T, Ben-Assuli O, Shabtai I. A review of PHR, EMR and EHR integration: a more personalized healthcare and public health policy. Health Policy and Technology. 2017; 6(1):20-5.

[3] Walker J, Pan E, Johnston D, Adler-Milstein J, Bates DW, Middleton B. The value of health care information exchange and interoperability: there is a business case to be made for spending money on a fully standardized nationwide system. Health Affairs. 2005; 24(Suppl 1):10-8.

[4] Gibaud B. The DICOM standard: a brief overview. In molecular imaging: computer reconstruction and practice 2008 (pp. 229-38). Springer, Dordrecht.

[5] Dolin RH, Alschuler L, Beebe C, Biron PV, Boyer SL, Essin D, et al. The HL7 clinical document architecture. Journal of the American Medical Informatics Association. 2001; 8(6):552-69.

[6] Soni J, Ansari U, Sharma D, Soni S. Predictive data mining for medical diagnosis: an overview of heart disease prediction. International Journal of Computer Applications. 2011; 17(8):43-8.

[7] Appari A, Johnson ME. Information security and privacy in healthcare: current state of research. International Journal of Internet and Enterprise Management. 2010; 6(4):279-314.

[8] Greer BJ. Cybersecurity for healthcare medical devices. Doctoral Dissertation, Utica College. 2018.

[9] Palmer S, Raftery J. Economics notes: opportunity cost. BMJ: British Medical Journal. 1999; 318(7197):1551-2.

[10] Kim YY, Shin SS. A study on reliable electronic medical record systems. Journal of Digital Convergence. 2012; 10(2):193-200.

[11] Thompson LA, Black E, Duff WP, Black NP, Saliba H, Dawson K. Protected health information on social networking sites: ethical and legal considerations. Journal of Medical Internet research. 2011; 13(1):1-11.

[12] Anderson RJ. A security policy model for clinical information systems. IEEE; 1996.

[13] Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. Security requirements and solutions in electronic health records: lessons learned from a comparative study. Journal of Medical Systems. 2010; 34(4):629-42.

[14] Rowan S, Clear M, Gerla M, Huggard M, Goldrick CM. Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels. arXiv preprint arXiv:1704.02553. 2017.
[15] Preuveneers D, Joosen W, Ilie-Zudor E. Trustworthy data-driven networked production for customer-centric plants. Industrial Management & Data Systems. 2017; 117(10):2305-24.
[16] Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: trust-less medical data sharing among cloud service providers via blockchain. IEEE Access. 2017; 5:14757-67.
[17] Xia Q, Sifah EB, Smahi A, Amofa S, Zhang X. BBDS: blockchain-based data sharing for electronic medical records in cloud environments. Information. 2017; 8(2):1-16.
[18] Ekblaw A, Azaria A, Halamka JD, Lippman A. A case study for blockchain in healthcare:"MedRec" prototype for electronic health records and medical research data. In proceedings of open & big data conference 2016 (p.13). IEEE.

Sung-Hwa Han works as a Senior Manager at SGA Solutions, Co., Ltd and he is currently a Ph.D. student in IT policy management at Soongsil University. His major work part is QA and CC Certificate on System Security Solutions. His interests are in Information Security and Security Management, Conversions IT Security. He published a few papers in journals such as Information Security.
Email:taifanz@naver.com

Ju-Hyung Kim is currently serving as the Representative Director of Korea Library Information Center Co., Ltd. In doing business, he is building a library information system. Among them, we focus on security system construction and personal information protection system related business. In addition, he has been studying security at the Graduate School of Soongsil University. He has a career in LGCNS and has professional qualifications such as MCSE, CCNA, and Quality Management.
Email: bmckorea@empas.com

Won-Seok Song is a Professor at Soongsil University in the Department of Business Administration. He graduated from Ajou University in 2007 with a Master of Science in Information and Communication Engineering. He is currently a Ph.D. student in IT policy management at Soongsil university from 2016 to 2018. He is a working as a researcher from 2018 to present in Security Institute on Cryptographic Technology. His interest includes Security Policy, C4I, Electronic Warfare, Information Protection, PMP, etc.
Email: sws.itpm12@gmail.com

Gwang-Yong Gim is a Professor at Soongsil University in the Department of Business Administration. Dr. Gim has been interested in research, such as 4th Industry Revolution, ICT ODA, Intellectual Property Rights, Service Science, Big Data Analysis, Information Security, S/W industrial Policy, and Open Innovation. He published a lot of papers in journals such as Information Science, Fuzzy Sets and System, Journals of Society of Management Information Systems, and Journals of Management Science.
Email: gygim@ssu.ac.kr