Journal of Korea Multimedia Society Vol. 25, No. 2, February 2022(pp. 197-205)
https://doi.org/10.9717/kmms.2022.25.2.197

Production Equipment Monitoring System Based on Cloud Computing for Machine Manufacturing Tools

Sungun Kim†, Heung-Sik Yu††

ABSTRACT

The Cyber Physical System(CPS) is an important concept in achieving SMSs(Smart Manufacturing Systems). Generally, CPS consists of physical and virtual elements. The former involves manufacturing devices in the field space, whereas the latter includes the technologies such as network, data collection and analysis, security, and monitoring and control technologies in the cyber space. Currently, all these elements are being integrated for achieving SMSs in which we can control and analyze various kinds of producing and diagnostic issues in the cyber space without the need for human intervention. In this study, we focus on implementing a production equipment monitoring system related to building a SMS. First, we describe the development of a fog-based gateway system that links physical manufacturing devices with virtual elements. This system also interacts with the cloud server in a multimedia network environment. Second, we explain the proposed network infrastructure to implement a monitoring system operating on a cloud server. Then, we discuss our monitoring applications, and explain the experience of how to apply the ML(Machine Learning) method for predictive diagnostics.

Key words: Multimedia Networking, Smart Monitoring, ML-based Data Analysis, Fog and Cloud Computing

1. INTRODUCTION

SMSs(Smart Manufacturing Systems) as an application field of Industry 4.0, are evolving in line with trends such as reduction of labor force, hyper-connectivity between manufacturing devices, expansion of digital manufacturing methods, and the advent of the era of intelligent manufacturing robots [1-2]. Industry 4.0 means that large - scale M2M(Machine-to-Machine) communication and IIoT(Industrial Internet of Things) technologies are well integrated to build efficient SMSs by monitoring, analyzing and diagnosing various issues without human intervention. The smart factory market based on various SMS systems is expected to reach USD 427.37 billion by 2025, at a compound annual growth rate(CAGR) of 9.22% during the forecast period(2020-2025) [3].

As a core field of Industry 4.0, a smart manufacturing is being applied to a wide variety of ways in many industries. However, it is not easy to develop such a CPS(Cyber Physical System) in which physical and virtual elements are closely integrated to provide appropriate M2M services suitable for the required SMS. In general, CPS consists of physical and virtual elements. The former involves manufacturing devices in the field space, whereas the latter includes the technologies such as network, data collection and analysis, security, and monitoring and control technologies in the cyber space.

In this paper, by combining physical elements,

※ Corresponding Author : Sungun Kim, Address: (608-737) 45 Yongso-ro, Nam-gu, Busan, Korea, TEL : +82-51-629-6235, FAX : +82-51-629-6235, E-mail : kimsu@pknu.ac.kr
Receipt date : Feb. 13, 2022, Approval date : Feb. 23, 2022

† Dept. of Information and Communications Eng., Pukyong National University
†† Smart Manufacturing Solution, UNOMIC Ltd.
(E-mail : paul.yu@unomic.com)
※ This work was supported by Pukyong National University Research Fund in 2020.

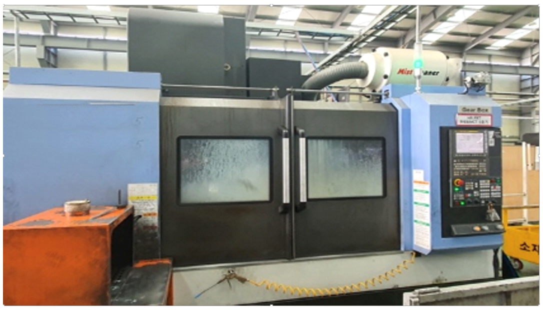


Fig. 1. An Example of CNC Manufacturing Machine Center.

i.e., system-based production equipment consisting of sensors and manufacturing facilities, with virtual elements in the cyber space, we focus on implementing a production equipment monitoring system related to building a SMS. In the proposed monitoring system, physical elements, exemplified by CNC(Computer Numerical Control, Fig. 1) manufacturing machine center that consists of tools including sensors and other manufacturing devices, interact with our fog-based gateway system. This gateway system captures and collects the data on operating status of the tools in real time and sends them to the cloud system after applying a filtering function. After analyzing the data received from the gateway system, the cloud system displays meaningful information on the dashboard. For this, as a crucial function, the monitoring system needs to meet the demand of predicting malfunction based on the operating state data of the machine tools.

In this work, we describe a fog-based gateway system interacting with the cloud system in the proposed network infrastructure. Then, we discuss our monitoring applications and ML(Machine Learning)-based analysis of the data captured during the operation of machining manufacturing tools as physical elements.

This paper is configured as follows; we explain related works and our approach in Section 2. In Section 3, we describe the proposed machining tool monitoring system based on a fog-based gateway and cloud systems and then we describe how to display meaningful information on the dashboard. In Section 4, in order to do predictive diagnostics, we discuss ML-based analysis of the data captured during the operation of machining tools. The summary of the research works and future works are presented in Section 5.

2. RELATED WORKS AND RESEARCH APPROACH

2.1 Related Works

The smart manufacturing requires several key technologies, which include application, platform, device, and security [4]. The application consists of systems that can directly participate in manufacturing execution based on ICT(Information and Communications Technology) platforms such as MES(Manufacturing Execution System), ERP(Enterprise Resource Planning), PLM(product lifecycle management), and SCM(Supply Chain Management), or to visualize and analyze the data collected from field devices. SAP(Systems, Applications, and Products in Data Processing) of Germany provides MES and integrated ERP that can interface with PLC(Programmable logic Controller) on the existing vertical architecture in real time, providing a solution that can flexibly respond to dynamic changes in the production environment [5].

The platform such as IoT(Internet of Things), big data analysis, and cloud computing technologies connects devices to applications, and provides data channels and analysis tools between devices and applications. For example, TIA(Totally Integrated Automation) of Siemens provides a technology that can be extended to a wide-area factory by supporting standard IoT-based interworking with various manufacturing devices and connectivity of multiple single factories [6].

The device is physical elements of the smart factory which includes various components such as robots, sensors, and controllers, transmits data to the applications, receives calculation and analysis results from them, and gives feedback to the field. Germany's FESTO(A. FEer and G. STOll) developed various functions such as controllers and wireless communication devices in an integrated manner, enabling real-time status monitoring, data communication control of relevant parts, and real-time communication between equipment parts [7].

From a security point of view, IoT end-devices constantly generate the data that are used for communicating with the edge device or the cloud server for monitoring and controlling. The data contains important information which should be protected from various threats in networks. Encryption technology could be used in response to the content leakage, on the other hand, a security tag, as a message authentication, is useful to face tampering or forgery. Esfahani et al. proposed a lightweight authentication mechanism using hash and XOR operations for M2M communications in IIoT environments [8]. And more G. Koh et al. suggested a method of creating and maintaining both secret key and security tag used for message authentication between end devices and edge device [9]. Even though, for edge computing in a short-range network environment, a security tag is sufficient to just cope with tampering and forgery, but, in cloud computing, we need both technologies, i.e., encryption technology and message authentication tag, due to open network environments [10].

In the smart manufacturing environment, each IoT device can be actively utilized and easily connected to internal devices or external environments. Um et al. proposed an industrial device monitoring and control system with stable and flexible functions based on oneM2M [11]. They also proposed a virtualization concept which can build independent and common environments and functions to be easy to adapt with external elements [12]. The proposed system was built with an open source IoT platform and hardware. Their system was restricted in edge computing architectures.

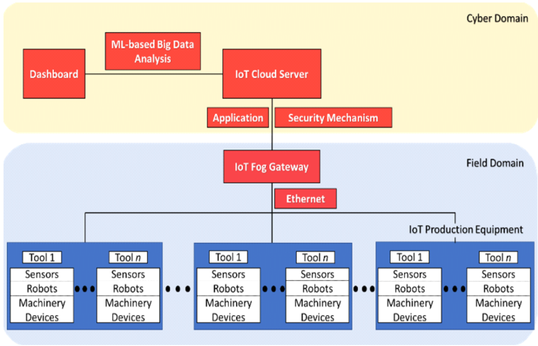


Fig. 2. Infrastructure of the Proposed Production Equipment Monitoring System.

2.2 Proposed Approach

Fig. 2 describes the structure of the proposed monitoring system based on an M2M framework structure composed of two domains: the field domain and the cyber domain.

In the field domain, the proposed IoT production equipment is composed of several tools in charge of machining, where each tool indicates a system-based precision machining end-device built with sensors and machinery devices. As a unit of end devices, the tools generate status-related data such as sensing values and motion angles (the feed speed, spindle speed, and axis info(A, B, X, Y, Z) of the production equipment) during operation in real time. The data generation is due to the smart capabilities of the end device tools.

First, the proposed approach requires a fog-based gateway system in order to implement the production equipment monitoring system in the cyber domain. The gateway system collects the data generated, in real time, by each tool through Ethernet and filters it. Then, the filtered data should be transmitted to the cloud server in the cyber domain through the Internet. Second, the monitoring system needs a secure data transmission method between the fog gateway system and the cloud server. Especially, the security mechanism applied here should be both practical and powerful, and it should not incur a high computational cost. By modifying the method of creating and maintaining both secret key and security tag used for message authentication between end devices and edge devices [9], we applied both technologies, i.e., encryption technology and message authentication tag, due to open network environments. Relevant details are beyond the scope of this paper.

Third, the cloud server in the cyber domain needs a function to manipulate the dashboard. The red shaded box in Fig. 2 corresponds to the task that need to be implemented as mentioned above.

3. PROPOSED MONITORING SYSTEM BASED ON FOG GATEWAY AND CLOUD SYSTEM

3.1 Network Platform of Production Equipment Monitoring System

Fig. 3 shows the suggested network platform for our monitoring system. In the field domain, the production equipment composed of production machining tools with collaborative robot systems, is connected to the fog gateway system via an Ethernet interface. The cloud system in the cyber domain interacts with the fog gateway system through the Internet, and also plays a role of displaying custom and monitoring reports on the dashboard related to the operating status of the production equipment.

The data communication between the production equipment and the fog gateway system is based on the ISO standard OPC(Open Platform Communications) UA(Unified Architecture) method and the North American Manufacturing Industry Association standard MTConnect [13]. The tool control application connected to TCP(Transmission Control Protocol) as a socket program was implemented in the environment of the ROS(Robot Operating System) standard that supports data transmission and reception for collaborative tools and the fog gateway system in manufacturing environments.

The fog gateway system composed of 8 cores based on ARM's Cortex-A53, e.g., 1.4 GHz CPU, 1 gigabyte DDR 800 MHz memory, and 4 gigabyte FLASH memory, supports TEE(Trust Environment Execution) technique that enables to use a specific memory space designated for security, and accommodates wireless communications including IEEE 802.11a/b/g/n/ac standard, Bluetooth 4.1 Low Energy(LE), and ZigBee 802.15.4. The major hardware configurations such as memory, control and communication are located in the center and two RJ-45 based Ethernet ports are attached at the bottom edge for the communication interface. We developed such a H/W product, as shown in Fig. 4, with a product dimension 100 × 100 × 30 mm, so that it can be easily attached even in a narrow production facility space.

The fog gateway system is connected to the cloud system through the Internet. Both systems send and receive the target data via a TCP-oriented

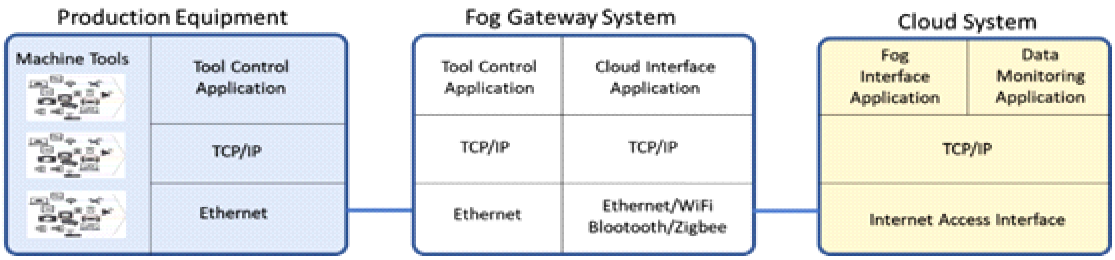


Fig. 3. Network Platform of Monitoring System.

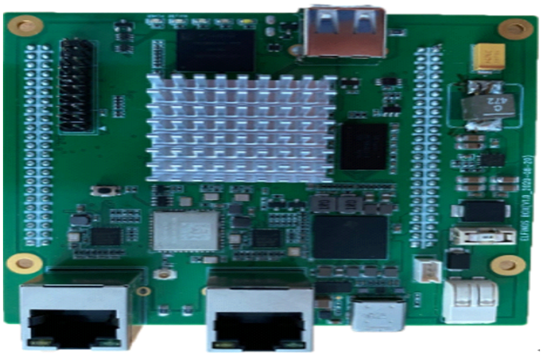


Fig. 4. Fog Gateway System.

protocol, and this data should be used in the cyber space. Both fog and cloud interface applications use Kafka, which provides a distributed message streaming function. Kafka, developed for the large-capacity real-time message transmission, is currently used in various server cluster communication methods [14-15]. As a distributed system consisting of servers and clients that communicate via a TCP-oriented protocol, Kafka can be deployed on cloud environments. This system expands cloud regions employing the server as a cluster of one or more servers. And clients allow the system to implement distributed applications that read, write, and process streams of events in parallel even in the case of network or system problems. As given in Fig. 3, we implemented the data monitoring application of the cloud system by interacting with three major elements of Kafka, such as producer, broker, and consumer. For example, the three applications, i.e., cloud interface application(producer), fog interface application (broker), and data monitoring application(consumer) are collaborating with each other as corresponding elements for the monitoring of machining tools' status.

3.2 Dashboard Monitoring System

The data monitoring application of the cloud system has the functions that analyze and display the data collected through TCP-oriented communication with Kafka. The dashboard provided by the proposed monitoring system is composed of three functions. The first function depicted in Fig. 5(a) shows the processing status for the production equipment. In other words, it indicates the working properly, alarm, and off states. The second function exemplified by Fig. 5(b) represents the data processing performance on each equipment such as a function to display and report analysis information about statistics generated by the production equipment. The third one described in Fig. 5(c) derives KPI(Key Performance Index) from the data generated from production environments such as workers and machining tools, and evaluates the achievement rates. Fig. 5 shows the corresponding screen-shots for monitoring the previously mentioned contents.

4. DATA ANALYSIS EXPERIENCE USING MACHINE LEARNING IN CLOUD

To apply machine learning methods for predictive diagnostics in cloud systems, we use the data generated from our production equipment testbed. Each set of data is generated from 5 days of operation. We tested several ML regression models to predict the spindle load on each time-stamp, using the feed speed, spindle speed, spindle load, axis load info(A, B, X, Y, Z) of the production equipment testbed. Here, the details of each data are not described as they are beyond the scope of the study of this paper and we note that these values depend on the test environment. For each equipment, we trained a separate model using 4 days of data as a training data, and the remaining one day for the evaluation.

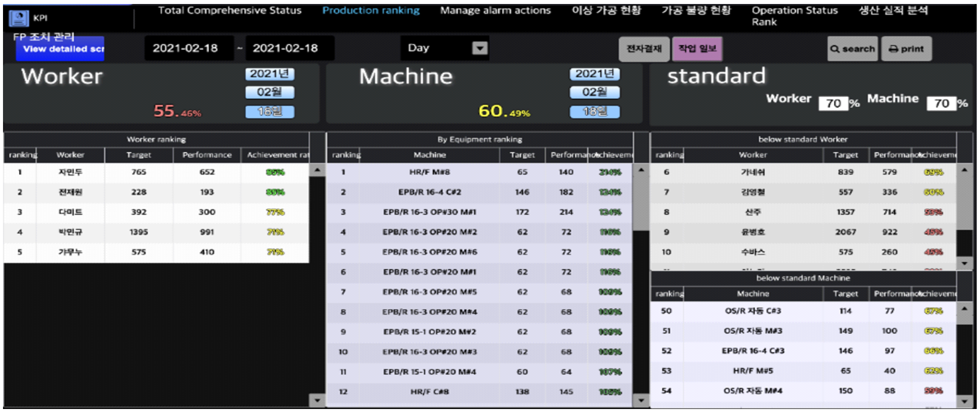
4.1 Regression Modeling

We use Root Mean Square Error(RMSE=γ) and its standard deviation as our evaluation metric, where RMSE(γ) can be calculated as below:

$$\gamma = \sqrt{\frac{\sum_{t=1}^{n}(a_t - p_t)^2}{n}} \quad (1)$$

(a)

(b)



(c)

Fig. 5. Screen-shots of Manufacturing Monitoring Tools. (a) Processing Status for the Production Equipment, (b) Data Processing Performance on Each Equipment, and (c) Key Performance Index for the Production Equipment.

Table 1. Regression Evaluation on Data from Equipment Simulator (RMSE within 1 Standard Range).

Method	Tool 1	Tool 2	Tool 3	Tool 4	Tool 5	All
Linear	11.06±0.21	4.26±0.22	2.59±0.04	2.29±0.27	1.51±0.32	4.34±3.55
SVR	10.16±0.20	4.34±0.22	2.59±0.04	1.39±0.36	2.19±0.28	4.13±3.23
RF	7.37±0.35	2.52±0.41	2.43±0.08	1.38±0.38	1.70±0.33	3.08±2.26
GBT	7.05±0.29	2.09±0.37	2.38±0.05	1.34±0.35	1.47±0.29	2.91±2.28

where t is each time-stamp of the data, a_t is the actual spindle load at time-stamp t, p_t is the predicted spindle load value at time-stamp t.

In this experiment, we tested a simple linear regression[16], SVR(Support Vector Regression)[17], and two ensemble regression methods, i.e., RF (Random Forest) and GBT(Gradient Boosted Trees), to predict the spindle load. RF is an ensemble learning method by constructing a set of decision trees and aggregating the prediction of each individual tree on inferencing by using mean prediction value of the trees to minimize the variance [18]. On the other hand, GBT builds subsequent weak regression trees to be added to correct the residual(reduce bias) during inferencing [19-20]. Those ensemble methods are known to be more robust with less overfitting problem. For both RF and GBT, we trained 100 trees, using mean square error as an estimator criterion to make branches on each tree.

Table 1 shows the validation evaluation results on the production facility testbed, where the last column all is the average of all data. The result shows in general we get lower RMSE on ensemble methods, especially GBT outperforms other methods on all data.

4.2 Predictive Diagnostics

In this section, we show the possibility of using the regression model trained on Section 4.1 to predict the equipment malfunction. Assuming that the root square error of prediction of regression model follows the normal distributions, 68%, 95%, and 99.7% of all root square difference of the predicted spindle load value and the actual value lies within 1, 2, and 3 standard deviation(σ) range respectively [21]. Values outside those ranges could be an indication of equipment malfunction, so we use this fact to set the threshold to warn the facility workers to check whether the equipment is operating properly or not. We evaluate how frequent the predictor will warn the facility workers if the root square difference of predicted value and the actual spindle load differs more than RMSE+1σ, 2σ, and 3σ. Evaluation is done with 5-fold cross validation, calculating the average frequency and ratio of 5 different runs.

Table 2 shows the frequency of possible warning alarms using with the best regression model(GBT) on Table 1. Each column shows the average raw frequency of warning alarms, where the percentage in the parenthesis is the frequency ratio.

Table 2. Regression Evaluation on Data from Equipment Simulator (RMSE within 1 Standard Range).

Threshold Value	Tool 4	Tool 5
RMSE+1σ	910.2(5.90%)	150.8(1.01%)
RMSE+2σ	463(2.94%)	114.6(0.77%)
RMSE+3σ	221.6(1.35%)	85.4(0.58%)

5. CONCLUSION

Implementing a complete SMS is very difficult. Furthermore, it is not easy to develop a CPS in which physical and virtual elements are closely integrated to provide appropriate M2M services suitable for the required SMS.

Monitoring in the cyber space is an important issue in manufacturing environments where products are manufactured by intelligent system-based production equipments. In order to realize this kind of monitoring system, it is necessary to expand the M2M processing area of edge computing into the cloud computing area. As a key element for this, the fog-based gateway system is of great importance.

In this paper, developed using open sources, we dealt with a fog-based gateway system that interacts with production equipment tools. In addition, we used a secure transmission method that guarantees security in delivering the data generated by end devices to the cloud. As one of the cloud system functions, the remote monitoring function on dashboard and real-time data processing function using Kafka were implemented. Lastly, we showed that ML-based regression models trained on the data could predict the possibility of malfunction of production equipment during the operation of machining tools.

In conclusion, as the smart systemization in manufacturing industries drastically expands, building a flexible smart monitoring system is also strongly required to meet the demand of predicting malfunctions based on the status of machining tools' operation. In order to satisfy such need, without the need for human intervention, it is required to control end devices directly in the cyber space. As a future work, we need to make an effort to apply our experience in ML-based data analysis to actual machine manufacturing monitoring.

REFERENCE

[1] 10 Trends That Will Change the Manufacturing Industry, https://www.daytranslations.com/blog/trends-manufacturing-industry/ (accessed January 20, 2022).

[2] 11 Trends That Will Dominate Manufacturing in 2021, https://global.hitachi-solutions.com/blog/top-manufacturing-trends (accessed January 20, 2022).

[3] Smart Factory Market-growth, Trends, COVID-19, Impact, and Forecast (2020-2025), https://www.mordorintelligence.com/industry-reports/smart-factory-market (accessed Jan- uary 20, 2022).

[4] L.M. Gladence, A.V.E. Jayakiran, A. Indraneel, and V.M. Anu, "An Integrated and Cohesive Methodology - Smart Manufacturing Service," *International Conference on System, Computation, Automation and Networking(ICSCAN)*, pp. 1-6, 2020.

[5] SAP Full Form & Definition of SAP ERP Software, https://www.stechies.com/u-mean-sap/ (accessed January 20, 2022).

[6] Totally Integrated Automation³, https://new.siemens.com/global/en/products/automation/topic-areas/tia.html (accessed January 20, 2022).

[7] FESTO, Industrial Automation, https://www.festo.com/us/en/c/automation/industrial-automation-id_pim2/ (accessed January 20, 2022).

[8] A. Esfahani, G. Mantas, R. Matischek, F.B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M.G. Tauber, C. Schmittner, and J. Bastos, "A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment," *IEEE Internet of Things Journal*, Vol. 6, No. 1, pp. 288-296, 2019.

[9] G. Koh, H. Yu, and S. Kim, "Secret Key and Tag Generation for IIoT Systems Based on Edge Computing," *Journal of Multimedia Information System*, Vol. 8, No. 1, pp. 57-60, 2021.

[10] M. Shin and S. Kim, "A Study on the Security Framework for IoT Services based on Cloud and Fog Computing," *Journal of Korea Multimedia Society*, Vol. 20, No. 12, pp. 3-27, 2017.

[11] C. Um, J. Lee, and J. Jeong, "Industrial Device Monitoring and Control System based on oneM2M for Edge Computing," *IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 1528-1533, 2018.

[12] C. Um, J. Lee, and J. Jeong, "Virtualized oneM2M System Architecture in Smart Factory Envir-

onments," *28th International Telecommunication Networks and Applica- tions Conference (ITNAC)*, pp. 1-6, 2018.

[13] MTConnect, https://www.mtconnect.org/ (accessed January 20, 2022).

[14] F. Bosi et al., "Cloud-enabled Smart Data Collection in Shop Floor Environments for Industry 4.0," *15th IEEE International Workshop on Factory Communication Systems (WFCS)*, pp. 1-8, 2019.

[15] P. Bellavista, R.D. Penna, L. Foschini, and D. Scotece, "Machine Learning for Predictive Diagnostics at the Edge: an IIoT Practical Example," *IEEE International Conference on Communications(ICC)*, pp. 1- 7, 2020.

[16] D.A. Freedman, *Statistical Models: Theory and Practice*, Cambridge University Press, 2009.

[17] H. Drucker, C.J. Burges, L. Kaufman, A. Smola, and V. Vapnik, "Support Vector Regression Machines," *Advances in Neural Information Processing Systems 9*, pp. 155-161, 1996.

[18] L. Breiman, "Random Forests," *Machine Learning*, Vol. 45, pp. 5-32, 2001.

[19] J.H. Friedman, "Stochastic Gradient Boosting," *Computational Statistics & Data Analysis*, Vol. 38, No. 4, pp. 367-378, 2002.

[20] T. Chen and C. Guestrin, "Xgboost: A Scalable Tree Boosting System," *Proceeding of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 785-794, 2016.

[21] F. Pukelsheim, "The Three Sigma Rule," *The American Statistician*, Vol. 48, No. 2, pp. 88-91, 1994.

Sungun Kim

received the M.S. and Ph.D. degrees in department of Information and Communication Engineering from University Paris Diderot in 1990 and 1993 respectively. Currently, he is a Professor in the Department of Information and Communication Engineering at Pukyong National University. His research interests include Wireless Network Security Technology, Sensor Network, Transmission Network and Access Network Technology, IoT, Fog Computing and Cloud Computing.

Heungsik Yu

received his BS and MS degree form Kyungsung University, Korea, in 1997 and 1999. He received his Ph.d degree in the Department of Information and Communication Engineering from the University of Pukyong National University, Korea, in 2014. He has been a member of IEEE since 2000. His research interests in cloud protocol engineering, big data analytics with machine learning, and Industrial IoT.