Regular paper

Journal of the KIECS. pp. 369-376, vol. 14, no. 2, Apr. 30. 2019, t. 94, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2019.14.2.369

제4차 산업혁명과 전자정부 보안연구
-지능형 정부의 빅데이터 사이버보안기술 측면에서-

이상윤* · 윤홍주**

A Study on the 4th Industrial Revolution and E-Government Security Strategy
-In Terms of the Cyber Security Technology of Intelligent Government-

Sang-Yun Lee* · Hong-Joo Yoon**

요 약

본고에서는 제4차 산업혁명시대의 새로운 사이버보안 인텔리전스 서비스에 대응하는 지능형 정부 연구측면에서 바람직한 미래형 전자정부의 새로운 모습을 찾았다. 특히 제4차 산업혁명시대의 주요 특징인 중앙화 및 지능화의 측면에서 빅데이터 사이버보안기술에 주목하여 미래형 전자정부의 전략방안에 대해 고찰하였다. 연구결과 빅데이터를 활용한 보안분석기술이 적용되는 보다 고도화된 상관관계 분석을 통한 기존의 한계를 뛰어넘는 시스템 마련을 제시하였다. 제4차 산업혁명시대에 적합한 보안 정보 및 이벤트 관리 시스템 구축 측면에서 IT 시스템에서 발생하는 로그정보를 빅데이터 분석 기술을 적용해 보안 위협 여부를 선제적으로 탐지하는 인공지능과 같은 지능형의 고도화된 SIEM(Security Information & Event Management) 시스템 마련을 제안하였다. 제안된 시스템이 구현되면 제4차 산업혁명시대의 전자정부 보안에 있어 중앙화 및 집중화된 빅데이터 대상 확대, 증가된 데이터에 따른 처리속도 및 탐지 후의 대응까지 보다 지능화된 차원에서 선제적으로 기능할 수 있다.

ABSTRACT

This paper studies desirable form of future e-government in terms of intelligent government research in response to new intelligent cyber security services in the fourth industrial revolution. Also, the strategic planning of the future e-government has been contemplated in terms of the centralization and intellectualization which are significant characteristics of the fourth industrial revolution. The new system construction which is applied with security analysis technology using big data through advanced relationship analysis is suggested in the paper. The establishment of the system, such as SIEM(Security Information & Event Management), which anticipatively detects security threat by using log information through big data analysis is suggested in the paper. Once the suggested system is materialized, it will be possible to expand big data object, allow centralization in terms of e-government security in the fourth industrial revolution, boost data process, speed and follow-up response, which allows the system to function anticipatively.

키워드

The 4th Industrial Revolution, Cyber Security Technology, Block Chain Technology, E-Government
제4차 산업 혁명, 사이버 보안 기술, 블록 체인 기술, 전자 정부

* 부경대학교 공간정보시스템공학과(sylee@pknu.ac.kr)
** 교신저자 : 부경대학교 공간정보시스템공학과
· 접 수 일 : 2018. 12. 04
· 수정완료일 : 2019. 02. 08
· 게재확정일 : 2019. 04. 15
· Received : Dec. 04, 2018, Revised : Feb. 08, 2019, Accepted : Apr. 15, 2019
· Corresponding Author : Hong-Joo Yoon
Dept. of Spatial Information Engineering, Pukyoung National University
Email : yoonhj@pknu.ac.kr

Ⅰ. Introduction

The establishment of the future e-government in the fourth industrial revolution has been commonly discussed in terms of materialization of the e-government. The key components of the fourth industrial revolution are centralization and intellectualization. The major four core technologies to centralization and intellectualization are the internet of things, cloud, big data, and mobile. The kernel of intelligent government is to anticipate the services needed and provide them. It is no exaggeration to say that intelligent government is a government that anticipatively searches the services and provide them in advance with intelligent technologies such as artificial intelligence with big data or centralized information such as cloud. Therefore, the desirable future of the current e-government will be materialization of the new e-government that is suitable to the fourth industrial revolution. Meanwhile, cyber security field of e-government in the fourth industrial revolution which is characterized by centralization and intellectualization is now facing a turning point. New cyber security technologies using or in response to new technologies are merging to materialize e-government progressing with its core technologies such as big data and cloud computing. Also, the development and progress of intelligent cyber security has greater significance today. In other words, it is critical to develop cyber security technology which is centralized and intellectualized to enable anticipatory response to cyber security threats. Thus, developing new intelligent cyber security services is important in the field of the e-government security in the imminent fourth industrial revolution. To be more specific, attaining intelligent cyber security which can detect the threats in advance and anticipate future threats is necessary. This paper contemplates strategic planning to find the desirable form of future e-government, especially focusing on big data cyber security technology, in terms of researches of intelligent government to respond to new intelligent cyber security services in the fourth industrial revolution.

Ⅱ. The 4th Industrial Revolution and Intelligent Government

2.1 Related Research

Researches regarding the security of e-government in terms of cyber security technology with big data in the fourth industrial revolution on which this paper mainly focuses have not been yet adequately found. Nevertheless, the researches about e-government system and the anticipation to the fourth industrial revolution can be found as of the followings. The research of S. Lee and M. Chung(2016a)[1] focused on providing customized public service in terms of administrative process and information system. In addition, S. Lee and M. Chung(2014)[2] performed researches on the materialization of platform e-government focusing on settling the information gap. Furthermore, S. Lee(2017)[3] performed exploratory studies on national informatization and e-government of Korea in terms of data governance. Especially, S. Lee and H. Yoon(2016b)[4] suggested the big data administrative space information system for system materialization in relation to artificial intelligence or the internet of things prior to such researches. In addition, S. Lee and H. Yoon(2016c)[5] focused on application of the administrative space information as metadata. Also, S. Lee and H. Yoon(2016d)[6] put emphasis on the significance of establishing big data for administrative space information system. Especially S. Lee and H. Yoon(2012a)[7] focused on cloud computing technology development which are one of the core information communication technologies in the fourth industrial revolution.

Moreover, S. Lee and H. Yoon(2012b)[8] performed researches on big data e-government in terms of national informatization strategic plans using public data. Also, S. Lee and H. Yoon(2015)[9] performed researches on the governance risk management. Furthermore, S. Lee(2012c)[10] demonstrated a study of electronic voting system. Finally, S. Lee(2013)[11] performed researches on informatization of policy using space information technology.

2.2 The Fourth Industrial Revolution

Although the discussion regarding the future of e-government is still an ongoing process, in terms of cyber security, the significance of intelligent cyber security is beyond dispute. As the fourth industrial revolution matures, it is likely that the information flow will be centralized in cloud and the big data analysis is important to come up with more profound solutions for cyber security issues. As aforementioned preceding researches describe, the establishment of system to provide administrative system has gained attention which relies on metadata analysis. Such data is collected to the central such as big data and the data of future of e-government is collected by cloud computing, big data, and public data. Therefore, e-government security is indispensable to such field and it is necessary to consider intelligent services using artificial intelligence and intelligent service provision. Also, it is important to prepare policies and technologies regarding cyber security in advance with big data which enables intelligent service characterized by centralization and intellectualization. As there is a surge in the number of malicious software and applications, threats on activation of exploit kits, compromised security such as Mirai and DDos in the internet of things devices, information attacks due to target attacks such as shadow brokers, and damages from ransom ware attack, not only enhancement in cyber security but also intellectualization of cyber security should be considered. Also, in the fourth industrial revolution of which information is further centralized, it is expected to have more variants of ransom ware and it is obvious that the number of threats to the next-generation information technologies such as the internet of things. Cyber security now is expected to detect multiform malicious codes as well as be prepared for cyber attacks and malicious codes on major facility by using big data analysis. Moreover, it is necessary to be prepared to being attacked by cyber attacks against the new intelligent services. Also, in terms of e-government that highlights openness and sharing characteristics as data governance, establishing anticipative plans is also critical to enable communications among different participants in platform e-government in the course of evolution to mature stage that intensifies openness of information.

Table 1. Big Data, cloud computing and national informatization

Classification	Assignment
Big Data	Fusion with the data from private sectors and enhancing cyber security with linkage with public data in a government-scale.
Cloud Computing	Establishment of governance based on advanced Information Technology for public services compatible with National Informatization in the Smart Era.

Table 1 describes the evolution of e-government where public data are actively linked, the data from government are open to public in harmony with the data from private sectors. In addition, policy making has aimed enhancement in security and it is necessary to prepare strategic plans for policy

making of cyber security as the governance of information technology compatible with advanced services nationwide in the smart era and national informatization. Therefore, it is necessary to anticipatively build strategic plans according to the policies. Namely, in terms of security and cyber threats cyber security technology with security intelligence level is necessary for those data centralized in the cloud mentioned above. Intelligent cyber security has gained attention as one of the intelligent security that respond to unknown cyber threats and enhances security intelligence by analyzing correlation between the data and cyber attacks in networks, systems, and application services of the information technology structures. As e-government security technology in the fourth industrial revolution, this technology, in terms of performing intelligent response, is critical. In other words, in the fourth industrial revolution the information technology environment changes at an alarming rate, which requires technology to detect and respond to cyber security threats by utilizing intelligent security such as big data correlation unlike existing threats which are simple and expectable.

III. The 4th Industrial Revolution and E-Government

3.1 E-Government and Big Data Analysis Technology

The analysis technology that simply categorizes big data by data capacity is not sufficient for what future evolution of e-government requires. In other words, it is necessary to regard the data centralized in the cloud as a whole new set which is incomprehensible with existing data process method. The technology focuses on cyber security performance rather than just database, finds proper response to a wide variety of data, collects and analyzes the information by utilizing artificial intelligence so that it can anticipatively respond to attacks. Specifically, development of a proper big data analysis technology despite of increased diversity of data with careful observations on data entry and output speed is important while data volume increases. The followings are the core technologies to be mature or expected in the fourth industrial revolution. The first is data fusion and integration technology. The technology enables integrating data and analyzing from multiple sources, which allows improved accuracy in results and better efficiency for insight. The second is cluster analysis technology. For instance, this technology is used to categorize the clients with self-similarity. This is a statistics-related technology that is used to categorize the subjects of which similar characteristics are unidentified. The third is classification technology. This is one of the data mining technologies which enables distinguishing under which category belongs based on the data set. The fourth is data mining technology which combines database management, statistics and machine learning to extract particular patterns among massive data. The fifth is association rule learning technology which consists of a series of algorithm that produces and tests potential rules. The technology is to find relevant rules among massive data and variables. The sixth is ensemble learning technology. This technology is to learn new hypotheses to categorize machine learning, create classifier, and combine the expectations from them. The seventh is genetic algorithm. It is a calculation model based on evolution process of the nature to solve problems with optimal solutions. The eighth is visualization technology. This technology is to visualize the analysis results and assist comprehension of the data.

3.2 Security Analysis Technology for E-Government and Big Data Application

Aforementioned big data security analytics technology which responds to core technology to analyze big data of the fourth industrial revolution which can be expected or intensified enables threat analysis on cyber attacks which have not yet been solved or not been responded on time. With centralization and concentration, cyber attacks are expected to be more advanced.

Thus, to take actions proactively, it is critical to respond according to the security correlation analysis through intelligent security system in terms of application of big data in security analysis technology. Existing responses in the centralized and concentrated big data system are not sufficient. In other words, it is important to improve responses with more creativity, which make it important to establish intelligent security system based on big data analysis. For example, improvement in security of e-government is necessary through intelligent security response which were not found in the past. The cyber attacks prior to the fourth industrial revolution were defendable by materializing the advanced pattern-matching algorithm and securing signature database of the attacks, however, this old response will no longer work in the future. In other words, it is important to define specific factors occurring in the internal network based on comprehensive data processing technology, analyze correlations, and respond with cyber security against the cyber attacks on centralized and concentrated big data. Therefore, the cyber analysis technology utilizing big data which enables correlation analysis is critical and the related core technologies are as followings. The first is threat intelligence technology. It is a brand-new information system that recognizes irregularity more accurately in response to security threats and attacks. For instance, the technology recognizes threats when small amount of outbound traffic to external IP is disguised as normal traffic and is overlooked. The second technology is analytics technology which is an essential security analysis technology. This technology analyzes the characteristics of source information by using traditional big data analysis method such as network mining, data mining, and machine learning. The third is behavior profiling. This technology is anomaly detection and analysis based on profiling due to difficulty for rule based methods to detect all of the abnormal activities. This technology enables defining related rules to search a series of certain conditions when the conditions of major technologies anomaly are well defined. The fourth is real-time monitoring technology which collects and manages the data from different sources. The technology monitors user activities in the application program and tracks attacks and threats in system components. The fifth is data & user monitoring technology. The technology is basically required to monitor sensitive data access and privileged users. Monitoring user activity that contains data context is essential to detect infiltration and abuse. The sixth, application monitoring technology. This technology is essential for the vulnerable points of abnormal application program monitoring technology, which can be a target of the attacks.

Ⅳ. Discussion

In terms of e-government security during the maturity of the fourth industrial revolution, establishment of proper security technology according to changing information technology environment cannot be overvalued. In other words, it is important to recognize cyber threats and establishing intelligent security is essential to reduce threats to centralized big data. For instance,

it is important for technologies to proactively respond to the threats by analyzing correlations such as internal information and attack log of big data. Namely, establishing cyber security with intelligent security concept to protect e-government and the centralized cloud is critical.

Therefore, it is important to establish the system which surpasses limitations of existing ones.

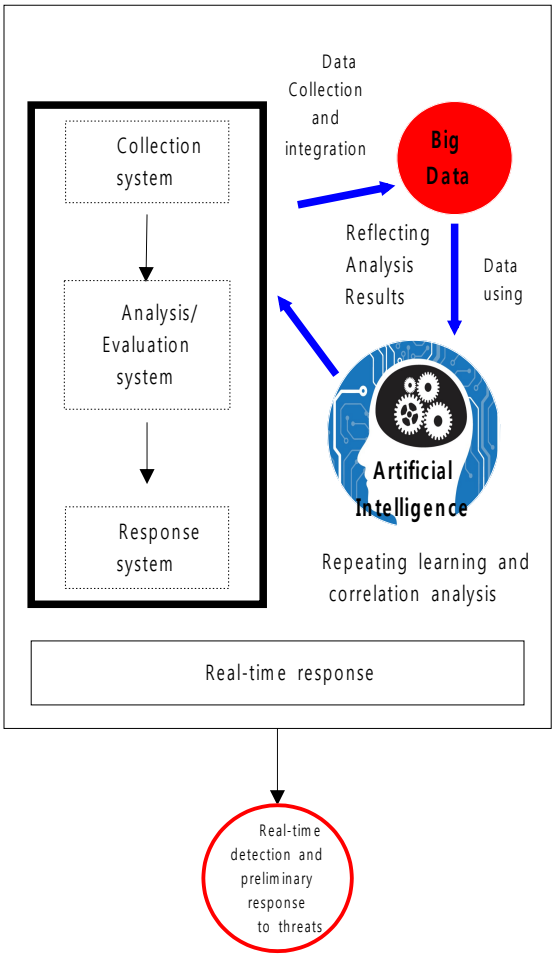

Fig. 1 System concept of SIEM advanced to Big Data

As Figure 1 describes, in terms of security information and event management system, advanced security information & event management system which detects threats in advance using big data analysis on log information of information technology system is important. Once the suggested system is successfully materialized, it will function as a big data analysis technology with thorough observation on input and output rate of the data regardless of increase in data diversity. In other words, it can function to expand security in the centralized big data and to proactively respond according to increased amount and speed of the relevant data.

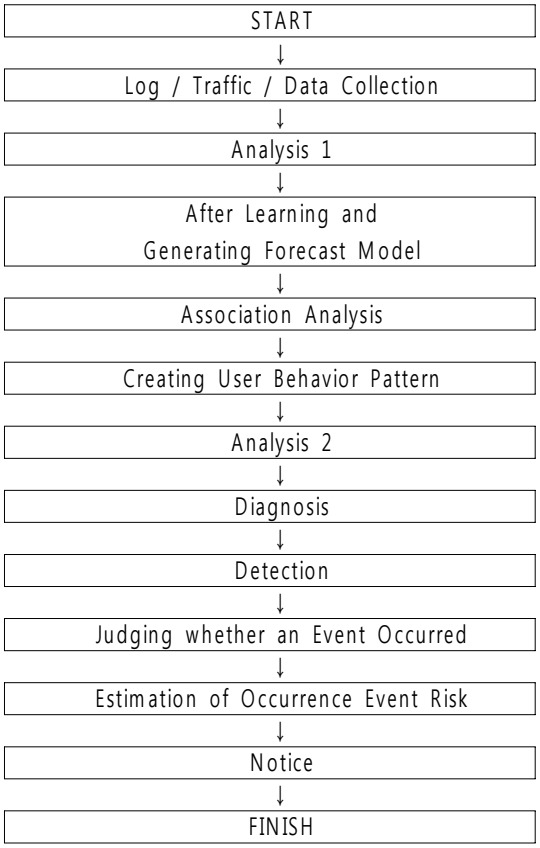

Fig. 2 SIEM systems and Big Data processing flowchart with operation algorithm

Therefore, Figure 2 shows an example of a detailed configuration of a big data processing work that functions in the above-mentioned SIEM

system. As shown in Figure 2, it is possible to improve the understanding of cyber security technology system of big data security intelligence level which is pending as present patent application proposed by this study.

Ⅴ. Conclusion

This paper seeks a desirable form of the future e-government in terms of government research aspect in response to new cyber security intelligence services in the fourth industrial revolution. Especially it contemplated strategic plans of future government with attention to big data cyber security technology in terms of centralization and intellectualization which are major characteristics in the fourth industrial revolution. Existing analysis technology which simply classifies big data by data capacity has limitation to the future e-government. In other words, existing database process methods for the centralized data in cloud are insufficient to solve the problems. Thus, big data security analytics technology is critical to respond to core technologies to analyze and expect big data in the fourth industrial revolution. The system suggested after the research is applied with security analysis technology and advanced correlations analysis to surpasses the limitations of existing system. Also, in terms of security information and event management system establishment appropriate to the fourth industrial revolution, the system where analyzed big data detects threats and responses proactively, such as SIEM(Security Information & Event Management), is suggested. Once the system is materialized, it will not only function proactively from detection to response according to the increase amount of data and its accelerated process speed but also expand object of centralized big data in the e-government of the fourth industrial revolution.

References

[1] S. Lee and M. Chung, “An Exploratory Study on Construction of Electronic Government as Platform with Customized Public Services: to Improve Administrative Aspects of Administrative Processes and Information Systems," *J. of Digital Convergence*, vol. 14, no. 1, 2016, pp. 1-11.

[2] S. Lee and M. Chung, “A Study on ‘Platform’ e-Government for Reducing the digital divide in a Multicultural Society of S. Korea,” *J. of Digital Convergence*, vol. 12, no. 1, 2014, pp. 1-12.

[3] S. Lee, “A Study on Policy of National Informatization with Electronic Government of S. Korea : Governance Strategy for Government by the Application of ‘scenario planning’,” *J. of the Korean Association For Regional Information Society*, vol. 20, no. 1, 2017, pp. 21-55.

[4] S. Lee and H. Yoon, “A Study on Smart Eco-city and Ubiquitous Administrative Spatial Informatization : In terms of Water Pollution and Disaster Prevention of Busan Ecodeltacity,” *J. of the Korea Institute of Electronic Communication Sciences,* vol. 11, no. 9, 2016, pp. 827-839.

[5] S. Lee and H. Yoon, “A Study on the Administrative Spatial Informatization and Ubiquitous Smart City: Focus on Busan Centum City,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 4, 2016, pp. 351-364.

[6] S. Lee and H. Yoon, “A Study on the Ferry Sewol Disaster Cause and Marine Disaster Prevention Informatization with Big Data : In terms of ICT Administrative Spatial Informatization and Maritime Disaster Prevention System development,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 6, 2016, pp. 567-579.

[7] S. Lee and H. Yoon, “The Study on Development of Technology for Electronic Government of S. Korea with Cloud Computing analysed by the Application of Scenario Planning,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 7, no. 6, 2012, pp. 1245-1258.

[8] S. Lee and H. Yoon, “The Study on Strategy of National Information for Electronic Government

of S. Korea with Public Data analysed by the Application of Scenario Planning," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 7, no. 6, 2012, pp. 1259-1273.

[9] S. Lee and H. Yoon, "A Study on System for Policy Promotion of Korean Nuclear Power: Risk Governance with Additional Construction of Nuclear Power Plants," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 10, no. 1, 2015, pp. 81-94.

[10] S. Lee, "The study of Internet Electronic Voting of S. Korea with Spatial Information System analysed by the Application of Scenario Planning," *J. of Korea Technology Innovation Society*, vol. 15, no. 3, 2012, pp. 604-626.

[11] S. Lee, "A Study on Technology Policy with Spatial Information System of S. Korea Analysed by the Application of Scenario Planning," *J. of Korea Technology Innovation Society*, vol. 16, no. 1, 2013, pp. 130-155.

저자 소개

이상윤(Sang-Yun Lee)

2002년 부산대학교 조선해양공학과 졸업(공학사)
2009년 부산대학교 대학원 정치외교학과 졸업(정치학석사)
2011년 부산대학교 대학원 공학박사(STS)수료
2013년 한국행정학회 학술정보이사
2014년 부산대학교 대학원 공공정책학 박사
2014년 ~ 한국전자통신학회 총무이사
2013년 ~ 2014년 부경대학교 공간정보연구소 소장
2015년 ~ 현재 부경대학교 행정공간정보화연구소 부연구소장
2015년 한국이민정책학회 학술정보이사
2016년 (사)한국생태공학회 부회장
※ 관심분야 : 정보기술정책, 전자정부, 행정공간정보화, 이민다문화와 사이버안보, 빅데이터 디지털정책

윤홍주(Hong-Joo Yoon)

1983년 부경대학교 해양공학과 졸업(공학사)
1985년 부경대학교 대학원 해양공학과 졸업(공학석사)
1997년 프랑스 그르노블 I 대학교 대학원 위성원격탐사전공 졸업(공학박사)
2010년 부산대학교 대학원 융합기술정책 박사수료
1997년~1999년 기상청 기상연구소 원격탐사연구실 기상연구관
1999년~2002년 전남대학교 해양공학과 교수
2002년~현재 부경대학교 공간정보시스템공학 교수
2012년~2013년 부경대학교 공간정보연구소 초대소장
2013년 (사)한국클라우드협회 부회장
2014년 한국전자통신학회 부회장
2015년 공간정보 Big Data 센터장
2015년 행정공간정보화연구소 소장
2016년 (사)한국생태공학회 회장
2017년 부산시 지능정보산업협의체 위원장
2017년 부산시 4차산업혁명 대응협의체 위원
※ 관심분야 : 원격탐사 & GIS, 공간정보정책학