사물인터넷융복합논문지 Vol. 10, No. 1, pp. 53-58, 2024 https://doi.org/10.20465/KIOTS.2024.10.1.053

스마트 팜 환경에서 보안 위협 및 대응 방안에 관한 연구

김선집*
한세대학교 ICT 융합학과 교수

A Study on Security Threats and Countermeasures in Smart Farm Environments

Sun-Jib Kim*
Professor, Division of ICT Convergence Engineering, Hansei University

요 약 4차 산업혁명의 핵심 기술인 IoT, Big-data, AI, Cloud 기술들이 최근 다양한 분야에서 신성장 동력의 핵심 기반 기술로 활용되고 있다. 이에 농업 분야에도 예외 없이 이러한 핵심 기술들이 적용되어 시공간의 제약 없이 원격 및 생산의 자동화를 통해 농업 분야의 문제점인 노동력 부족 현상 해결, 생산비 절감, 환경 부담 절감 등에 기여하고 있다. 그러나 이러한 핵심 기술을 활용함에 따라 농업 분야에도 보안 사고 사례가 발생하고 있다. 이에 본 연구에서는 스마트 팜을 기초, 중간, 고도의 3단계로 구분하여 단계별 특성, 보안 위협 및 대응 방안을 제시하고자 한다. 특히 클라우드 플랫폼하에서 컨테이너 기반 다양한 서비스 및 연구가 증대됨에 따라 이에 대한 보안 위협을 중심으로 대응 방안을 제시하고자 한다.

주제어 : 스마트 팜, IoT, 클라우드 플랫폼, 컨테이너, 파이프라인

Abstract IoT, Big-data, AI, and Cloud technologies, which are core technologies of the 4th Industrial Revolution, have recently been applied to various fields and are being used as core technologies for new growth engines. Accordingly, these core technologies are applied to the agricultural field without exception, contributing to solving the problem of labor shortage, reducing production costs, and reducing environmental burden through remote and automated production without time and space constraints. However, as these core technologies are utilized, security incidents are occurring in the agricultural field as well. Accordingly, this study divides smart farms into three stages(Basic, Middle, and High) and presents the characteristics and security threats of each stage. In particular, as the number of container-based services and research increases under cloud platforms, we would like to suggest countermeasures focusing on security threats.

Key Words : Smart Farm, IoT, Cloud Platform, Container, Pipeline

1. 서론

1.1 연구 배경 및 목적

디지털 전환은 국가 산업의 혁신을 견인할 수 있다는 관점에서, 우리나라는 2020년 7월에 코로나 이후 시대의 국가 프로젝트로 '한국판 뉴딜'을 발표하였다[1]. 이러한 한국판 뉴딜은 주로 디지털과 그린 뉴딜의 두 가지 큰 축으로 구성되어 있다. 이 계획은 국가경쟁력을 결정하는 핵심적인 요소로서 디지털 뉴딜, 즉 디지털 전환에 대응하고 변화를 주도하기 위한 대규모 투자로 구성되어

본 논문은 2023년 한세대학교 교내 특성화 사업으로 수행되었음.
*교신저자 : 김선집(kimsj@hansei.ac.kr)
접수일 2023년 12월 04일 수정일 2024년 01월 27일 심사완료일 2024년 02월 02일

있으며, 이러한 투자는 4대 분야와 12개의 추진 과제로 구성되어 제시되었다.

특히, 한국판 뉴딜은 스마트 팜 등 19개 사업이 농식품 분야에 선정되어 이루어지고 있으며 이를 통해 농업과 식품 산업에서도 뉴딜 계획에 참여하여 발전 변화해 나가고 있다.

이러한 디지털 시대의 농업은 4차 산업혁명 이후 농업 생산, 유통, 소비 전반에서 네트워크 연결을 통한 생산성과 지속 가능성 향상의 모든 과정에 걸쳐 4차 산업혁명 기술의 핵심인 사물인터넷(IoT), 인공지능(AI) 기술 등과 연계 활용하고 있다.

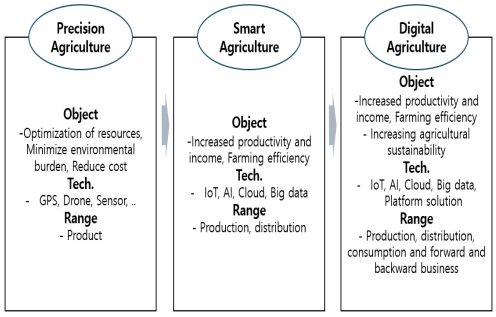
이러한 활성화 방안이 지속 연구되면서 스마트 팜 구축의 높은 비용의 문제점과 각종 해킹 등 보안과 관련된 위험이 증대되고 있다는 문제점이 제기되고 있다[2]. 또한, 다양한 형태로 스마트 팜의 연구와 구축이 이루어지고 있어 적절한 보안 대책을 수립하는 것이 쉽지 않다.

이에 본 연구에서는 다양한 형태로 발전하고 있는 스마트 팜에 대해 특성을 고려한 보안 위협과 적절한 대응 방안을 제시하기 위한 3단계 스마트 팜을 제시하고, 단계별 특성을 고려한 보안 위협과 이에 대한 대응 방안을 제시하고자 한다.

2. 이론 고찰

4차 산업혁명 이후 IoT와 AI와 같은 기술이 주목받아 다양한 분야에서 융합되고 적용되면서, 우리의 일상에서 쉽게 접할 기회가 증가하고 있다[3]. 특히, 노동 집약적인 농업 분야에서는 정밀농업(Precision Agriculture)과 스마트 농업(Smart Agriculture)을 포함한 디지털 농업(Digital Agriculture)이라는 개념이 정립되었다[1].

이러한 디지털 농업은 최신 정보통신기술(ICT)을 농업에 접목하여 시공간의 제약 없이 원격 및 생산의 자동화를 통해 생산성 향상과 영농작업의 효율성을 높이는 기술로 정의된다. 디지털 농업은 전 세계적인 농업 분야의 농가인구 감소 등으로 인한 노동력 부족 현상을 해결하고자, IoT, 빅데이터, 지능형 네트워크와 함께 AI 기술을 활용하여 관련 정보를 수집, 분석하고 적절한 방안을 제시함으로써 농업 부문의 문제점을 해결하고 생산비 절감, 환경 부담 절감, 생산성 향상 등을 통한 농업의 지속 가능성을 확보할 수 있다. 이러한 디지털 농업은 [Fig. 1]에서 보듯이 세부적으로 3단계로 나누어 볼 수 있다[1, 4].



[Fig. 1] Smart Farm Steps

[Fig. 1]의 정밀농업은 농업에 필요한 비료와 농약 등의 영양분을 적시 적량만 사용함으로써 생산성과 환경 부담을 최소화하는 방식으로 정의된다. 스마트 농업은 첨단 ICT 기술을 농업에 통합하여 생산성과 작업의 효율성을 높이는 방식으로 정의되며, 디지털 농업은 IoT와 지능형 네트워크를 활용하여 생산데이터, 유통데이터, 소비데이터 등 농업 전체의 데이터를 수집하고 플랫폼상에서 AI로 데이터를 분석하며 최적의 의사결정을 내리고 다시 현장에 적용함으로써, 농업의 전 과정인 생산, 유통, 소비가 플랫폼 내에서 통합되어 이루어지는 방식으로 자원 사용의 최적화를 추구하고자 하는 노력이 반영되는 농업의 형태이다[1, 4].

3. 관련 연구

3.1 스마트 팜 연구

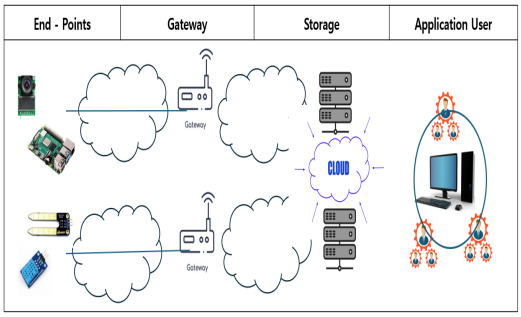
최근 스마트 팜 연구는 단순히 정밀농업 분야를 넘어서, 영농 효율화를 통해 생산성과 소득 증대를 목표로 IoT를 활용함과 더불어 더 나아가 클라우드와 빅데이터 기반 서비스 구조 설계 및 AI 기술을 IoT 기술과 융합하여 스마트 팜 프레임워크를 설계하는 등 다양한 연구가 활발하게 이루어지고 있다[3].

이중 컨테이너 기반의 연구는 스마트 팜의 연구가 센서의 데이터 수집, 자동화를 위한 액추에이터, 정보 취합 및 원격 제어를 위한 통신 기술의 요구사항을 반영하여 개발되면서 특정 벤더의 제품에 의존적인 환경을 벗어나 제품 간의 호환성 및 서비스 확장성을 확보하기 위한 컨테이너 기반 스마트 팜 서비스 구조를 설계하여 제시하고 있다[3]. 또한, IoT를 활용하여 농작물의 생육 정보에 관련된 환경정보를 추출, 각 데이터 간의 비선형 상관관계의 특징 정보를 확인할 수 있는 분석과 이를 통한 다양

한 예측을 위해 인공지능 기술을 적용한 프레임워크를 제시하고 이를 통한 생산성을 확보하고자 하는 연구가 진행되고 있다[5].

3.2 스마트 팜의 보안 위협 및 대응 연구

스마트 팜의 구조는 [Fig. 2]와 같이 네 개의 단계를 통해 연결 구축될 수 있다. 이에 첫 번째 단계는 센서 등 사물로부터 데이터를 수집하는 단계로 정의할 수 있으며, 두 번째 단계는 사물인터넷 네트워크, 센서링된 데이터를 수집하여 네트워크 망을 통해 전송하는 게이트웨이 단계, 세 번째 단계는 수집된 데이터의 분석 및 처리하고 마지막 단계는 사용자가 활용하는 단계로 정의할 수 있다[6]. 이에 단계별 위협 요소는 [Tab. 1]과 같이 정리할 수 있다.



[Fig. 2] Overview of Digital Agriculture Steps

〈Table 1〉 The Threats to digital agriculture

Step	Threats
End-points	Physical attacks, device/sensor alteration, side-channel attacks, eavesdropping, malicious code, forgery, etc.
Gateway	Protocol vulnerabilities, authentication, routing, jamming, DoS/DDoS, etc.
Storage	SQL injection, IP sniffing/spoofing, encryption, confidentiality and integrity, cloud infra attack, flooding attacks in the cloud, etc.
Application User	Social engineering, phishing, privacy attack, access control, service interruption, etc.

이러한 IoT를 활용하는 환경에서 보안상의 위협 요소의 문제를 해결하기 위해서 국내·외 다양한 단체들이 보안 요구사항을 검토하고 있다. 이에 대표적으로 OWASP Internet of Things Project에서 2014년 IoT에서 발생할 수 있는 10가지 주요한 보안 취약점 및 해결 방안을 제시하고 있으며, 국제 이동통신사업자 협회인 GSMA에서는 IoT 서비스 제공자, IoT 기기 제조자, IoT 개발자, 네트워크 통신 사업자를 대상으로 GSMA IoT Security Guidelines를 공개하였다. 또한, 국제 클라우드 보안 협의체인 CSA 등에서 IoT 기기기의 보안 설계, 개발 및 안전한 서비스 운영 등에 필요한 보안에 관련된 요구사항과 대책을 포함한 가이드라인을 제시하였다[7].

국내에서는 한국인터넷진흥원에서 IoT 공통 보안 가이드를 IoT 제품 및 서비스의 설계·개발 단계, 배포·설치·구성 단계, 운영·관리·폐기 단계별로 제시된 7대 IoT 공통 보안 원칙을 기반으로 15가지 세부 공통 보안 요구사항을 제시하고 있다[8].

4. 제안하는 방안

4.1 스마트 팜 단계별 보안요구사항

본 연구에서는 스마트 팜을 기초, 중간, 고도로 3단계의 수준으로 정리 제시하고 각 스마트 팜의 요구사항과 이에 부합하는 보안요구사항을 제시하고자 한다.

〈Table 2〉 Characteristics of Smart Farms by Stage

Cat.	Field automation	Farm operation	Resource management	Supply chain
HIGH	Full Automation	Big data and AI-based diagnostics and operations	Linkage of all farms (based on cloud platform)	Producer Consumer Linked Value Production
MIDDLE	Automate automatic aggregation and control of farm equipment data	Real-time farm control	Single farm operation	Collaborate on Single Variety Development
BASIC	Automation of farm equipment	Modernization of farm equipment	Operational functional focus	Single Equipment Center

〈Table 2〉는 본 연구에서 제시하는 스마트팜의 3단계의 특성을 구분하여 제시한 내용이다. 1단계(Basic)는 농장 설비의 자동화로 농장의 시스템을 자동화하는 것으로 단일 업무 중심의 반복적인 업무를 자동화하는 단계이다. 2단계(Middle)는 농장 설비 전체를 통제하고 각 장비로부터 생성되는 데이터 기반 종합적인 분석을 통해 단일 농장의 생산량 증대를 위한 단계이다. 마지막으로 3단계(High)는 단일 농장의 개념을 넘어선 개념으로 특정 지역 또는 전 지역의 스마트 팜을 네트워크로 연결 생산과 소비의 가치 사슬 연계를 통한 스마트 팜의 완성 단계이다.

〈Table 3〉 Smart Farm Threats by Stage

Cat.	Security threats
High	Contains a medium level of threat and has risks from cloud platforms
Middle	Includes the risk of the basis and Tab. 1, has security risks for storage, but is not cloud-based and has security risks for legacy systems.
Basic	Tab. 1 End-points and gateway security risks and physical security risks

〈Table 4〉 Threat Factors by Cloud Attack Target

	Description	
Attacks	User	Spoofing, Repudiation
	Cloud Service	Data tampering, Information disclosure, DoD, Elevatin of Privilege
Threats	Abuse functionality, Data Structure attack, Embedded malicious code, Exploitation of authentication, Injection, Resource manipulation	

〈Table 3〉은 〈Table 2〉에서 제시된 단계별 스마트 팜의 보안 위험 요소이다. 이에 기초 단계에서는 물리적 보안 위험과 센서 등과 직접적으로 연계된 위험 요소가 주라고 하면, 중간 단계에서는 센서와 게이트웨이, 스토리지, 그리고 사용자 측면의 보안 위험까지 예상될 수 있다. 마지막으로 고도화 단계에서는 기초와 중간 단계의 위험 요소와 더불어 클라우드 플랫폼을 활용함에 따라 클라우드 기반의 위험 요소로 예측된다. 이에 기초, 중단 단계의 위험에 대한 대응책은 그 위험 요소의 특성을 고려 시 기존 연구의 대응책과 동일하다 볼 수 있다[6-8]. 다만, 본 연구에서 중점적으로 제시하고 있는 스마트 팜 고도화 단계는 그 특성과 구축 형태에 대해 본 연구에서 정의 제시함에 따라 위협 요소와 이에 대한 대응책을 제안한다.

4.2 스마트 팜 고도화 단계에서 보안 위협의 대응 방안

본 절에서는 스마트 팜 단계 중 클라우드 환경을 활용하는 고도화 단계를 중심으로 공격과 위협에 대해 살펴보고 이에 대한 적절한 대응책을 제시하고자 한다. 일반적으로 클라우드 보안에 대한 책임 분담은 주로 클라우드 서비스를 제공하는 서비스 제공자에게 있었지만, 최근 서비스 개발 기업들은 클라우드를 통한 비즈니스 전환으로 보안 측면에서의 주도권을 점진적으로 가져가고 있다. 이러한 경향에 따라 사이버 공격자들도 전략을 조정하여 클라우드를 더 유리한 표적으로 인식하게 되었다. 즉, 클라우드 컴퓨팅은 스마트 팜에서 생성된 다양한 데이터를 저장하고 활용하는 중요한 수단으로 쓰이고 있으며, 이는 언제든지 접속할 수 있으며 대용량 데이터를 전송하는 편리한 방법을 제공하고 있어, 클라우드 기반의 스마트 팜은 보안 위협에서 벗어날 수 없다[9].

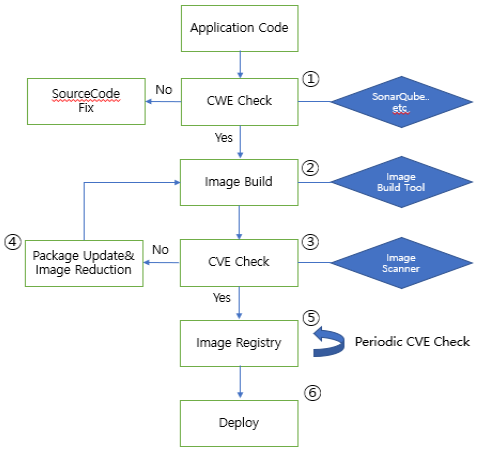
〈Table 4〉에서 보듯 클라우드 환경을 활용하는 스마트 팜 고도화에서는 클라우드 환경을 사용함에 따라 클라우드 환경을 이용하는 사용자와 서비스 모두에 공격이 이루어질 수 있다. 이에 이러한 공격으로 기능의 남용, 데이터 구조에 대한 공격, 내장된 악성코드 전파, 인증 악용, 리소스 조작 등의 위협이 발생할 수 있다. 이는 기존 레거시한 시스템에서의 보안 위협에 대응하기 위한 관리적 통제와 암호화 등 다양한 기술적인 대응으로는 클라우드 환경에 부합되는 보안 위협에 적절한 대응을 할 수 없음을 알 수 있다. 이는 클라우드 시스템에서 많이 사용되고 있는 컨테이너 보안 위협에 대한 명확한 대응책을 제시할 필요성을 의미한다.

애플리케이션의 개발 및 배포 방식이 모노리스(Monolith)에서 마이크로서비스(Micro service)로 전환되며 경량 가상화 기술인 컨테이너(Container)가 IT의 핵심 기술로 자리 잡았으며 컨테이너는 하이퍼바이저(Hypervisor) 기반의 가상머신과 달리 동일한 운영체제 커널을 공유함에 따라 사용자가 애플리케이션을 배포하는 데 필요한 자원과 시작 소요 시간을 단축해 클라우드 환경에 대대적인 활성화를 견인하였다[10].

이에 본 연구에서는 스마트 팜의 3단계인 고도화 단계에서 클라우드 인프라 환경 보안과 클라우드 환경에서의 플랫폼 개발 보안으로 양분하여 보안 대응 방안을 제안한다.

우선 클라우드 환경에 대한 보안 대응 방안으로 IaaS(Infrastructure as a Service)를 제공하는 클라우드 서비스 제공자(Cloud Service Provider) 또는 관리 운영하는 MSP(Managed Service Provider)는 서버, 네트워크 등의 인프라에 대하여 CIS Benchmark 등에서 요구하는 보안 모범사례를 준수하도록 서비스 환경을 제공해 줄 필요가 있다. 이를 통해 CCE(Common Configuration Enumeration)의 취약점에 대응할 수 있다[10].

다음으로 [Fig. 3]와 같은 클라우드 플랫폼 개발 환경에서의 취약점 점검을 통해 보안 위협에 대응할 수 있을 것으로 본다.



[Fig. 3] Automatic Deployment Pipeline Diagram for Security Consideration

각 단계의 보안 대응책은 다음과 같다.

① 기능단위로 개발된 애플리케이션에 대하여 CWE (Common Weakness Enumeration) 취약점 점검을 수행하여 시큐어 코딩 준수 여부를 점검해야 한다.(SonarQube와 같은 CWE 점검 도구를 이용)

② CWE 취약점 점검을 통해 정적 코드 분석이 완료된 애플리케이션 소스 코드를 컨테이너화하기 위해 Docker, Kaniko, Buildah 등의 이미지 빌드 도구를 통해 컨테이너 이미지를 빌드한다.

③ Anchore, Vuls, Clair, Singularity Tools 등과 같은 이미지 스캐너를 통해 빌드된 컨테이너 이미지에 존재하는 CVE(Common Vulner- abilities and Exposures) 보안 취약점을 검출한다. 이를 통해 컨테이너 이미지의 루트 파일 시스템(rootfs)과 설정 정보(config.json)에 존재하는 다양한 보안 취약점을 검출할 수 있다.

④ 검출된 CVE 보안 취약점의 정·오탐 여부 및 영향도를 검토하고 애플리케이션 의존성을 검토하여 컨테이너 이미지에서 불필요한 패키지를 제거하고, 패키지 업데이트를 통해 이미지에 존재하는 CVE 보안 취약점을 제거한다.

⑤ 패키지 업데이트 및 이미지 축소를 통해 CVE 보안 취약점이 제거된 골든 이미지를 재 빌드하여 이미지 레지스트리(이미지 저장소)에 저장한다.

⑥ 컨테이너 레지스트리에 저장된 신뢰된 이미지를 사용하여 운영환경에 배포하여 서비스를 제공한다. 다만, CVE 보안 취약점의 경우 시간이 지남에 따라 새로운 취약점이 발견될 수 있으므로 레지스트리에 저장된 이미지들에 대해서도 주기적인 취약점 점검을 수행하여야 한다. 이미지 빌드 시점이 필요로 하는 보안패치 빈도와 호환되기 어려우므로 런타임(Runtime)시에 확인이 필요하다.

위와 같이 개발자가 애플리케이션 소스 코드를 컨테이너 형태로 패키징하여 빌드하는 시점부터 운영환경에 배포되는 시점까지 아르고 워크플로우, 에어플로우와 같은 도구를 통해 배포 파이프라인 구성함으로써 작업을 자동화하여 안전한 컨테이너 환경을 제공할 수 있다.

5. 결론

본 연구에서는 스마트 팜의 운영 및 발전 동향에 근거하여 스마트 팜의 단계를 설정 정의하였으며, 스마트 팜의 단계별 위협 요소를 도출하였다. 또한 스마트 팜의 3단계인 고도화 단계에서 생산자 소비자가 클라우드 플랫폼을 통해 가치 생산이 이루어진다는 전제하에 클라우드 인프라 환경 보안과 클라우드 환경에서의 플랫폼 개발 보안으로 구분하여 보안 대응 방안을 제안하였다. 특히 클라우드 환경의 플랫폼 개발 보안에서는 단계별 주요 보안 수행 작업을 제시함으로써 클라우드 인프라 서비스 제공자뿐만 아니라 클라우드 플랫폼하에서 컨테이너 기반 스마트 팜 서비스 개발자들이 고려해야 할 보안 대응책을 제시하였다. 이를 통해 스마트 팜의 고도화 단계에서 클라우드 플랫폼 기반 서비스 개발자들이 보안 취약점을 가진 이미지가 배포되지 않도록 할 수 있어 안전하고 다양한 컨테이너 기반 클라우드 스마트 팜 서비스를 개발 제공할 수 있을 것으로 기대한다. 또한, 스마트 팜의 다양한 위험 요소에 대한 통제 관점의 체계화와 보안 관점의 스마트 팜 아키텍처 수립의 연구가 지속되어야 할 것이다.

REFERENCES

[1] KREI, AGRICULTURAL OUTLOOK 2021 KOREA, “Chapter 6. The Future of Agriculture, Digital Agriculture,” 2021.

[2] Three Smart Farm Problems and Without countermeasures, serious situations occur[Internet] Https://salaryfarmer.com

[3] H.B.Nam, J.H.Jung, D.K.Choi and S.J.Koh, "Desingn of Container based Smart Farm Service in IoT," *KICS Fall Conference 2021,* pp.933-934, 2021.

[4] A Plan to Establish Precision Agricultural System to Enhance Agricultural Competitiveness[Internet], https://repository.krei.re.kr/handle/2018.oak/30206

[5] Y.S.Jeong, "Designing an Efficient Smart Farm Framework That Combines IoT Technology and Machine Learning Technology," *Journal of Business Convergence,* Vol.8, No.2, pp.137-142, 2023.

[6] A.N. Alahmadi, S.U.Rehman, H.S.Alhazmi, D.G.Glynn, H.Shoaib and P.Sole, "Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture," *Sensors*, Vol.22, No.9, pp.3520-3534. 2022.

[7] D.H.Lee and N.J.Park, "IoT product security certification and security maintenance measures," *The Korean Institute of Communications and Information Sciences*, Information and Communications Magazine, vol.33, No.12, pp.28-34, 2016.

[8] IoT Common Security Guide, KISA [Internet], https://www.kisa.or.kr/2060205/

[9] W.Ahmad, A.Rasool, A.R.Javed, T.Baker and Z.Jalil "Cyber Security in IoT-Based Cloud Computing:A Comprehensive Survey," Electronics, Vol.11, No.16, 2021.

[10] S.J.KO and S.J.Kim, "A Study on Pipeline Design Methods for Providing Secure Container Image Registry," Journal of Internet of Things and Convergence, Vol.9, No.3, pp.21-26, 2023.

[11] S.J.Kim and J. Heo, "A Study On The Cloud Hypervisor ESXi Security Vulnerability Analysis Standard," Journal of Internet of Things and Convergence, Vol.6, No.3, pp.31-37, 2020.

[12] D.W.Lee, K.M.Cho and S.H.Lee, "Research on Efficient Smart Factory Promotion System in IoT Environment," Journal of Internet of Things and Convergence, Vol.6, No.4, pp.59-64, 2020.

[13] Smart Farm Problems[Internet], https://salaryfarmer.com/

[14] Cybersecurity Report: "Smart Farms" Are Hackable Farms[Internet], https://www.techopedia.com/

[15] Container-security-checklist[Internet], https://github.com/krol3/container-security-checklist

[16] Cloud Vulnerability Check Guide[Internet], https://isms.kisa.or.kr/

김 선 집(Sun-Jib Kim) [종신회원]

■ 2014년 3월 ~ 현재 : 한세대학교 IT학부/ICT융합학과 교수

〈관심분야〉

정보보안, 사물인터넷, 클라우드, 환경시스템, 스마트 팩토리, 스마트 팜