Journal of the Korea Academia-Industrial cooperation Society
Vol. 25, No. 2 pp. 764-770, 2024

https://doi.org/10.5762/KAIS.2024.25.2.764
ISSN 1975-4701 / eISSN 2288-4688

ICT 기반 전력시스템에서 APT 공격탐지를 위한 온톨로지 모델링

김기훈[1], 박재표[2*]
[1]숭실대학교 대학원 금융기술융합학과, [2]숭실대학교 정보과학대학원

Ontology Modeling for APT Attack Detection in an ICT-Based Power Systems

Gi-Hoon Kim[1], Jae-Pyo Park[2*]
[1]Department of Financial Technology Convergence, Soongsil University
[2]Graduate School of Information Science, Soongsil University

요 약 스마트그리드 기술은 기존의 전력망에 ICT를 접목하여 공급자와 소비자 간의 양방향 의사결정 작용을 통해 에너지 효율성을 높인 차세대 지능형 전력망 기술이다. 신재생 에너지원 확대와 안정적인 전력 운영 보장을 위해 확대되고 있지만, 관련 취약성을 공격하는 보안 위협 가능성이 있다. 상호간의 정보를 양방향으로 교환하는 스마트그리드 기술의 개방형 아키텍처 특성상 다양한 형태의 사이버 공격에 노출되는 취약점이 나타난다. 이러한 다양한 형태의 사이버 공격은 국가에 큰 피해를 끼칠 가능성이 있으므로 이에 대비해 다양한 침입을 탐지, 분석하여 신속하게 대응이 가능한 지능형 보안 관제 시스템이 필요하다. 대표적인 공격 방법 중 하나인 APT공격은 기존 탐지기술을 우회하여 장기간 잠복했다 공격하는 지능적이고 정교한 공격으로, 본 논문에서는 이러한 APT공격을 패턴분석을 통해 조기에 탐지하여 대응하고자 온톨로지를 기반으로 한 공격 탐지를 위한 시스템을 제안한다. 제안하는 방법은 전력 시스템의 보안 취약점을 수집, 분석 및 분류하고, 주요 전력 시스템에 추론 엔진을 적용하여 공격을 조기에 파악하고 대응하는 것을 특징으로 한다.

Abstract The smart grid is a next-generation intelligent power grid technology that increases energy efficiency through two-way decision-making between suppliers and consumers by incorporating ICT in the existing power grid. Although it is expanding into renewable energy sources, and ensures stable power operations, there is the possibility of security threats owing to related vulnerabilities. The open architecture of smart grid technology exchanges information in both directions, so vulnerabilities to various types of cyber-attack appear. Because cyber-attacks are likely to cause extensive damage in a country, an intelligent security control system that can detect and analyze intrusions and respond quickly is needed. A typical APT attack bypasses existing detection technology and goes undercover for a long time. This paper proposes an ontology-based attack detection system to respond to these APT attacks early through pattern analysis. The proposed method collects, analyzes, and classifies security vulnerabilities in power systems, applying inference engines to major power systems to identify and respond to attacks early.

Keywords : SmartGrid, APT, Cyber Attack, Ontology, ICT

*Corresponding Author : Jae-Pyo Park(Soongsil Univ.)
email: pjerry@ssu.ac.kr
Received November 28, 2023 Revised December 26, 2023
Accepted February 6, 2024 Published February 29, 2024

1. 서론

기존 전력망에 ICT((Information and Communication Technology) 기술을 접목한 차세대 전력망 기술을 본 논문에서는 스마트그리드라 통칭한다. 공급자와 소비자 간의 실시간 정보를 양방향으로 교환하는 개방형 아키텍처의 구조로 되어 있으므로 다양한 형태의 사이버 공격에 노출될 수 있다[1]. 스마트그리드 산업이 점차 활성화되면서 이에 대한 보안 위협의 철저한 대비가 필요하다[2]. APT(Advanced Persistent Threat)공격은 대표적인 공격방법의 하나로써 사용자의 단말기, 스마트미터기 등에 잠복해 있던 악성코드가 데이터 송수신 시 단계적으로 서버 시스템을 감염시켜 국가적으로 큰 피해를 줄 수 있으므로 이에 대한 보안대책을 마련해야 한다. 따라서 본 논문에서는 ICT 기반 전력시스템에서 APT 공격이 의심되는 행동을 탐지하기 위해 시스템에 가해지는 공격 방식과 상황 정보를 분석하고, 이를 기반으로 온톨로지 관련 규칙을 설계하여 전력시스템의 지능형 탐지 시스템을 제안하고자 한다.

2. 관련연구

2.1 스마트그리드 보안기술

스마트그리드란 지능형(Smart)과 전력망(Grid)이 합쳐진 융합·복합 기술로써 Fig. 1과 같이 표현 할 수 있다.

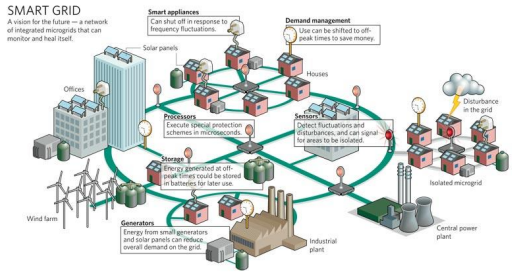

Fig. 1. Smart Grid Diagram

ICT기술을 적용한 스마트그리드 기술은 전력의 효율성과 안정성을 높여주기 위해 전력 공급자에게 실시간으로 전력 사용량 정보를 전송해야 한다. 이를 위해 전력 사용량을 정확하게 측정해주는 스마트미터기가 필요하며, 스마트미터기에서 전력 사용 정보를 분석하는 기술을 EMS(Energy Management System)라 하고, 이러한 전력망을 실시간 감시 및 제어를 위한 원격 감시 제어시스템이 존재한다. 기존 전력망과 비교해 차별성을 가지는 특징으로는 중앙집중식 단방향 전력공급 방법과 다르게, 스마트그리드는 지역별 분산체계로 이루어진 전원들이 네트워크 구조로 연결되어 생산된 전력을 사용하며, 양방향으로 정보 전달을 함으로써 다양한 소비자 선택권이 주어진다[3,4]. 이로 인해 생산자의 역할과 소비자의 역할을 동시에 수행할 수 있게 할 수 있다.

스마트그리드의 보안기술은 전력 인프라와 ICT가 결합되어 전력 사용 및 관리를 최적화 하는 것을 말하며, ESS(Energy Storage System), 폐쇄망 보호 시스템 등으로 구성되어 있다. 기술적 요소를 분류하여 Table1에 나타냈다.

Table 1. Classification of SmartGrid Security Technology

SmartGrid Security Technology	
Power Supply Security	SCADA system
	Automated power restoration system
	Power transportation and distribution disturbance detection technology
	Energy management and security technologies
	AMI disturbance detection technology (FDS)
Power Consumption Security	Access control technology (smart metering, AMI certification/approval, etc.)
	Firmware Manipulation Prevention Technology
	Encryption Communication Schemes (PLC, Zigbee, etc.)
	Communication Privacy Protection Technology
	AMI·HAN Hacking Prevention Technology
Smart Service Security	Fee System and Secure Power Trading Technology
Power Supply Security	Charging Infrastructure Certification & Approval Technology
	Blockchain Integration Technology

2.2 APT 공격

APT공격은 전통적인 보안 솔루션이 결합된 체계에서 예방, 진단, 차단이 어려운 공격방식을 의미한다. NIST (National Institute of Standards and Technology)에서는 APT 공격을 다음과 같이 정의하고 있다[5]. APT 공격은 전문지식과 많은 자원을 가진 공격자가 여러 다른 공격 경로를 통해 그들의 목적을 달성하는 공격이다. APT 공격은 방어자의 노력에 적응하면서, 목적을 실행하기 위해 필요한 수준의 상호 작용을 유지하며 오랜 기간 동안 반복적으로 목적 달성을 시도한다[4]. 이는 특정

한 목표 대상에 대하여 취약점을 파악하고, 다양한 방법을 이용한 지속적인 공격활동을 통해 정보 탈취, 시스템 파괴 등의 시스템 손상을 입히려는 공격 형태를 의미한다.

Table 2. APT Attack process

Seq.	Phase	Details
1	Preparation	Collecting and Analyzing
		Information of the Attack Target
		Tampering the Web-site
		Securing C&C
2	Intrusion	Tampering Software Updater
		Tampering Web-hard and Web Noticeboard
		Sending Malicious E-mail
3	Inside activity	Spreading Malicious Code
		Collecting Additional vulnerabilities
		Getting Access to the database
4	Achievement	Exfiltration Important Data Destroying the System

일반적으로 APT 공격 단계는 Table 2와 같이 사전준비, 내부망 침투, 내부 활동, 목적달성의 4단계로 정의된다[6]. 사전준비 단계는 공격자가 다음 단계로 들어가기에 앞서 준비하는 과정으로써 공격대상의 정보를 수집·분석하고, 내부에 악성코드로 감염된 시스템과 통신 및 제어를 하기 위한 C&C 서버 확보와 같은 작업으로 구성된다.

내부망 침투단계는 사회 공학적 기법 및 취약점을 이용하여 시스템의 IT 인프라에 침투하는 단계이다.

내부 활동 단계는 내부망 침투단계가 완료된 시스템을 기반으로 공격 목표를 달성하기 위해 공격대상의 IT 내부 인프라에 대한 정보를 수집하는 단계이다.

목적 달성 단계는 APT 공격의 목적을 달성하기 위해 백도어 등의 프로그램을 설치해 지속적인 정보 유출을 하거나, 악성파일로 공격대상 내부 IT 인프라를 감염시켜 파괴하는 단계이다.

APT 공격은 은밀하고 장기적인 공격을 통해 목적을 달성하기 때문에 피해자는 침해사고의 발생 가능성을 쉽게 인지하기가 어렵다[7]. 이러한 APT 공격을 대응하기 위한 방안은 여러 가지가 존재하지만[7-9], 본 논문에서는 침입탐지시스템(Intrusion Detection System)을 기준으로 온톨로지 모델링을 하고자 한다.

2.3 온톨로지 기반 공격탐지 모델링의 필요성

일반적으로 온톨로지는 도메인 내의 개념 및 개념 사이의 관계, 개념의 속성 및 특성, 속성 및 특성에 부여된 제약 조건 및 객체들로 표현되는 개념 계층 구조이다[10]. 이를 이용해서 특정 도메인의 단어를 공통으로 정의하고, 지식을 공유할 수 있다.

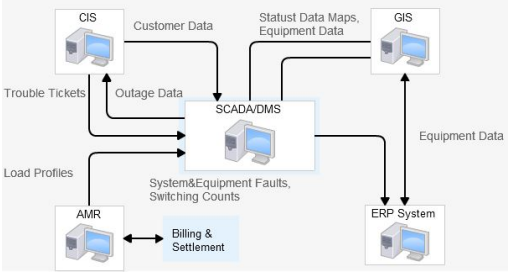

Fig. 2. Smart Grid Management System

스마트그리드는 Fig. 2와 같이 DMS(Distribution Management System), SCADA(Supervisory Control And Data Acquisition), AMR(Automated Meter Reading), GIS(Geographical Information System), ERP(Enterprise Resource Planning) 등 다양한 시스템이 결합된 매우 복잡한 시스템이다. 다양한 공격을 방어하기 위해 시스템의 데이터 모델은 최신 상태로 유지해야 하지만 고전적인 관계형 모델기반 데이터베이스 시스템에서는 이러한 처리가 어렵다. 온톨로지를 사용할 경우 기존 시스템의 단점인 데이터 모델링 유지뿐만 아니라 데이터 통합에서도 유리한 옵션을 가지고 있다[11]. 지식베이스 구축에 있어서 온톨로지의 유연한 시스템은 데이터의 최신성 유지 및 데이터의 유용성, 위협분석 정보 활용에 큰 이점이 주어진다[12].

3. APT 공격 탐지를 위한 온톨로지 모델링

안전한 스마트그리드 환경을 위해서 본 장에서는 APT공격의 시나리오 상황을 유추해 보고, 이를 기반으로 추론규칙을 설계하여 APT 공격에 대한 상황을 인지하고자 한다.

Fig. 3는 본 논문에서 제안하는 온톨로지 기반 전력 시스템의 보안 시스템 구성도이다. 시스템에 가해지는 공격 탐지를 위해 취약점을 수집,분석,추출 작업을 하여 공격에 대한 행위를 분류한 후 분석데이터를 기반으로 보안 온톨로지를 구축하고, 추론 규칙을 통해 상황에 대한 정보를 추론한다. 공격발생시 탐지가 되어 상황을 인식 후 알리며, 발생된 공격정보를 추가해 지식베이스가 확장되게 합니다.

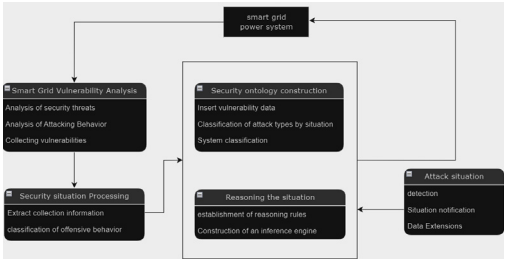

Fig. 3. System Configuration Chart

3.1 스마트그리드 APT 공격 시나리오 분석

스마트그리드 환경에서의 APT 공격 시나리오의 단계별 예시를 Table 3에 나타냈다. 공격 정보 수집에서부터 공격루트 설정, 바이러스를 이용한 침투, 백도어 삽입, 내부 활동, 목적달성 후 침입흔적 삭제 단계로 나눠진다. 정보수집과 공격루트 설정 단계의 경우 공격 대상이 명확히 드러나 있지 않고, 공격대상 또한 자신이 공격당한다는 행위를 감지하지 못하기 때문에 이 단계는 추론에서 제외한다. 마찬가지로 흔적 삭제 단계 또한 공격자가 공격을 끝낸 후 흔적을 지우는 단계이기 때문에 제외한다. 제외한 나머지 단계를 기초로 하여 온톨로지를 모델링한다.

Table 3. step-by-step Smart Grid APT Attack Scenario

Phase	APT Attack Activity
Preparation	Corporate Websites
	Search Engines
	Internal Spies
Attack route setup	Wireless Vulnerabilities
	Internal Staff
Intrusion	Zero-day Attack
	E-Mail
	USB
	Remote Management Tool
	C&C Server
	GPS
4. Backdoor	Remote Control
	Keylogger
5. Inside activity	Access to the Server Attack
	C&C Server Based D-Dos Attack
	GPS Receiver Attack
	Control System Attack
	Information Exploitation
6. Cleanup	Malware Toolkit Deletion

3.2 온톨로지 설계

온톨로지로 지식 베이스를 구축함으로써 실시간으로 위협정보들을 확인할 수 있다. 악성코드의 행위를 클러스터링 하기 위해 사용한 도구는 protégé로써 오픈소스 온톨로지 편집기이다. protégé를 사용함으로써 종합적인 분석을 통해 새로운 공격 시도를 빠르게 찾을 수 있다.

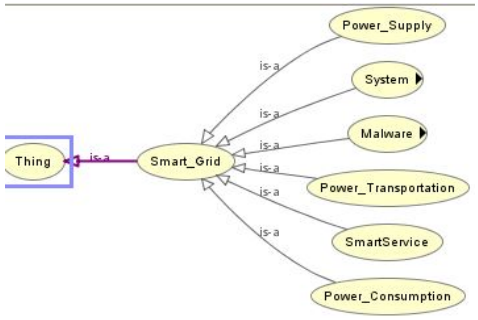

Fig. 4. Smart Grid Basic Logical Graph

Fig. 4는 보안 온톨로지를 설계하기 위한 기본 논리 그래프이다. Table 1의 행위별로 분류한 카테고리를 이용하였다. Level 1값인 Smart_Grid는 공격이 이루어지는 목표물을 정의하며 Level 2에 해당하는 Power_Supply, System, Malware, Power_Transportation, Smart Service, Power Consumption과 같은 하위 클래스를 가진다.

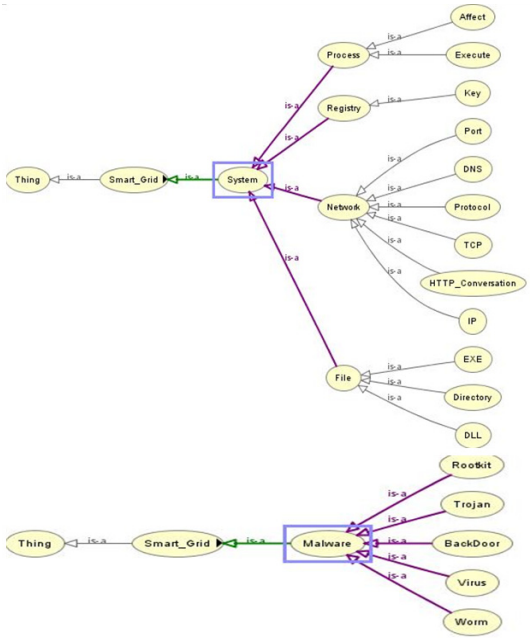

Fig. 5. Relationships Between Malware and Subclasses of the System Class

System과 Malware 클래스의 경우 동일 레벨의 각 클래스에 이들의 하위클래스를 대입시킬 경우, 중복 흐름이 표현될 가능성이 높기 때문에 Level 2로 설계하였으며 하위 클래스와의 관계는 Fig. 4와 같다.

Fig. 5는 Malware와 System 클래스의 하위클래스와의 관계를 나타낸 그래프이며, 각 클래스마다 나타나는 행위별로 다르게 발생하는 값을 이용해 표현하였다.

4. 실험 및 평가

본 논문에서는 스마트그리드의 핵심적인 시스템중 하나인 AMI(Advanced Metering Infrastructure)에서 발생 가능한 이상상황 공격탐지 시나리오를 가정하고 공격상황을 규칙을 통해 추론한다. 규칙 제정에 앞서 SmartService의 하위단계인 AMI시스템의 하위 클래스를 규정하여 Fig. 6에 나타내었다.

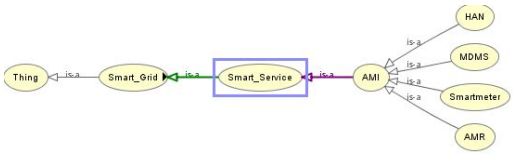

Fig. 6. AMI System Class Relationship Diagram

4.1 AMI APT 공격탐지 시나리오 추론식

protégé에 내장된 SWRL언어를 기반으로 AMI의 취약점을 이용한 각 공격 단계별 규칙을 설계해 APT공격 상황 탐지 추론식을 Table 4와 같이 정의하였다.

Table 4. Malicious behavior SWRL Rules

Attack Behavior	Inference Rule
PacketSniffing	(?T behaviour PacketSniffing)∧(PacketSniffing resultIn PacketDecoding)∧(PacketDecoding resultIn KeyAcquisition)∧(KeyAcquisition resultIn DataGathering) ⇒ (?T step MITMAttack)
USBConnect	(?T USBConnect)∧(USBConnect resultIn SystemInfection)∧(SystemInfection resultIn RemoteAcces) ⇒ (?T step BackDoor)
ModifyPacket	(?T KeyValue_Modulation)∧(KeyValue_Modulation resultIn ModifyPacket)∧(ModifyPacket reslutIn SystemAccess) ⇒ (?T step SystemConnect)
SystemAttack	(?T DataGathering)∧(DataGathering resultIn SystemAccess)∧(SystemAccess resultIn SystemControl)∧(SystemControl resultIn SystemDestruction) ⇒ (?T step APTAttack)

첫 번째 단계는 사전조사를 마친 펌웨어 취약점을 기반으로 스마트미터에서 방출되는 패킷을 가로채 분석하여 환경설정 정보, 암호화 키, 펌웨어 등 주요정보 데이터를 획득하는 단계이며, 이를 MITM_Attack(Man-In-The-Middle Attack)이라 정의한다.

두 번째 단계는 내부 관리자의 저장매체를 통한 시스템 감염 및 백도어 설치단계이며, 이를 BackDoor라 정의한다.

세 번째 단계는 확보된 데이터를 바탕으로 이를 변조하여 악성파일 생성, 계측된 계량 정보 조작 및 상위시스템 공격수행을 하기 위한 감염된 시스템에 패킷을 전송하는 단계이며, 이를 SystemConnect라 정의한다.

네 번째 단계는 전송 데이터를 토대로 시스템 동작을 컨트롤 하여 계측정보를 수정하거나 시스템 ShutDown 등 시스템을 공격하는 단계이며, 이를 APTAttack이라 한다.

4.2 추론엔진을 이용한 평가

APT 공격은 공격 특성상 여러 공격들이 복합적으로 구성되어 단계별로 진행되기 때문에 행위단계별로 분류된 본 논문에서 제안한 추론식을 온톨로지에 매핑하여 SWRL 추론엔진을 실행시켜 보았다. 성공적으로 실행된 추론규칙 결과 및 상황별 추론 인식 여부를 Fig. 7에 나타내었다.

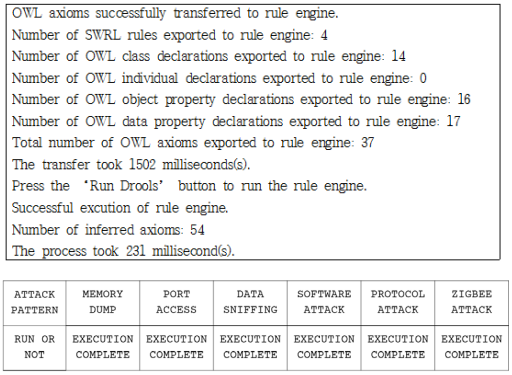

Fig. 7. Inference rule execution result

5. 결론

ICT 기반 전력시스템 네트워크의 규모가 커지고 이에 따라 복잡성이 증가하면서 다양한 사이버 공격 또한 늘어나고 있다. 본 논문에서는 네트워크 공격 방법 중 하나인 APT 공격을 탐지하고자 온톨로지 기반 지능형 탐지 시스템을 제안하였다. 본 논문에서 제안된 방법은 AMI 보안위협 정보 모델링을 기초로 적용한 것으로 상황모델링에 중점을 두었다. 스키마를 이용한 추론식의 모델 구조는 개별 상황들을 토대로 단계별 정의를 하였다.

제안한 추론 규칙을 통해 APT 공격을 행위별로 분석하고, 이에 대한 공격 시나리오를 유추해 추론 규칙을 적용했다. 추론 및 탐지의 기본 프레임워크를 구축해 국가기반시설에 가해지는 지능적이고 정교한 공격을 탐지 할 수 있으며, 공격을 조기에 파악하고 대응하는 것을 특징으로 한다. 향후 추가, 수정, 확장을 통하여 온톨로지 설계의 추가 개발을 위한 지표로 활용 될 수 있을 것이다. 공격이 발생한 이벤트 사건 데이터들을 기반으로 미리 공격에 대응할 수 있는 관련 규칙을 추가해 시스템을 개선할 계획이다.

References

[1] S. H. Oh, S. K. Eun, "Remote user Access control Mechanism in Smart Grid environments", The Transactions of The Korean Institute of Electrical Engineers, Vol. 60, No.2, pp.416-422, Feb. 2011.
DOI: http://dx.doi.org/10.5370/kiee.2011.60.2.416

[2] D. S. Lee, "Security Threat and Policy Analysis to Secure the Safety and Reliability of the Smart Grid", Journal of the Korea Institute of Information and Communication Engineering, Vol.25, No.10, pp.1381-1390, Oct. 2021.
DOI: https://doi.org/10.6109/jkiice.2021.25.10.1381

[3] S. I. Moon, "Smart Grid Concept", Information & communications magazine, Vol.27, No.4, pp.3-9, Apr. 2010.

[4] S. M. Yoo, N. G. Kim, Y. G Kim, "Smart grid security technology trend analysis and response measures", Information & communications magazine, Vol.31, No.5, pp.8-14, May. 2014.

[5] Joint Task Force Transformation Initiative, Guide for Conducting Risk Assessments, Special Publication, NIST, USA, pp.35-36
DOI: https://doi.org/10.6028/NIST.SP.800-30r1

[6] C. Tankard, "Advanced Persistent threats and how to monitor and deter them" Network security, Vol.2011, No.8, pp.16-19, Aug. 2011.
DOI: https://doi.org/10.1016/S1353-4858(11)70086-1

[7] D. S. Moon, H. S. Lee, I. G. Kim, "Host based Feature Description Method for Detection APT Attack", Journal of The Korea Institute of Information Security and Cryptology, Vol.24, No.5, pp.839-850, Oct. 2014.
DOI: https://doi.org/10.13089/JKIISC.2014.24.5.839

[8] K. H. Son, T. J. Lee, D. H. Won, "Design for Zombie PCs and APT Attack Detection based on traffic analysis" Journal of the Korea Institute of Information Security and Cryptology, Vol.24, No.5, pp.491-498, Jun. 2014.
DOI: https://doi.org/10.13089/JKIISC.2014.24.3.491

[9] C. Choi, J. H. Choi, P. K. Kim, "Ontology-based access control model for security policy reasoning in cloud computing", The Journal of Supercomputing, Vol.67, No.3, pp711-722, Mar. 2014
DOI: https://doi.org/10.1007/s11227-013-0980-1

[10] M.Uschold, M.Gruninger, "Ontologies: Principles, methods and applications", The Knowledge Engineering Review, Vol.11, No.2, pp.93-155, Jul. 1996.
DOI: https://doi.org/10.1017/S0269888900007797

[11] E. Doğdu, M. Özbayoğlu, "Ontology-centric data modelling and decision support in smart grid applications a distribution service operator perspective", 2014 IEEE International Conference on Intelligent Energy and Power Systems(IEPS), IEEE, KYiv, UKraine, pp.198-204, June 2014.
DOI: https://doi.org/10.1109/IEPS.2014.6874179

[12] D.Schachinger, W.Kastner, S.Gaida, "Ontology-based abstraction layer for smart grid interaction in building energy management systems", 2016 IEEE International Energy Conference (ENERGYCON), IEEE, Leuven, Belgium, pp.1-6, April 2016.
DOI: https://10.1109/ENERGYCON.2016.7513991

김 기 훈(Gi-Hoon Kim) [정회원]

- 2019년 2월 : 조선대학교 산업기술융합대학원 소프트웨어융합공학과 (공학석사)
- 2019년 4월 ~ 2023년 3월 : (주)디에스티인터내셔날 기업부설연구소 선임연구원
- 2023년 4월 ~ 현재 : 씨엠티정보통신(주) 선임연구원

〈관심분야〉
정보통신, 정보보안(IoT, ICT)

박 재 표(Jae-Pyo Park) [종신회원]

- 1998년 8월 : 숭실대학교 대학원 컴퓨터학과 (공학석사)
- 2004년 8월 : 숭실대학교 대학원 컴퓨터학과 (공학박사)
- 2010년 3월 ~ 현재 : 숭실대학교 정보과학대학원 교수

〈관심분야〉
정보보안, 보안평가 및 인증, 디지털포렌식, FinTech