정 보 보 호 학 회 지
제 33 권 제6호, 2023. 12

엣지 컴퓨팅 기반 IIoT 보안 연구 동향

전 규 현*, 이 진 규**, 전 승 호***, 서 정 택***

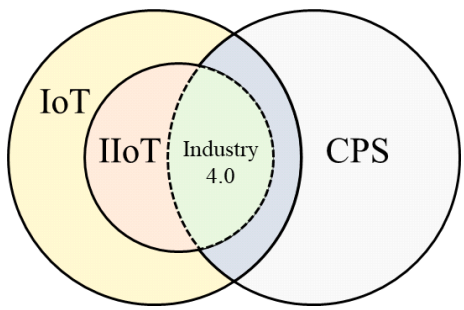
요 약

산업용 사물 인터넷(IIoT)은 자원 관리 및 최적화, 신속성, 지속가능한 생산, 자동화 등의 특징으로 인해 다양한 산업 분야에서 활발하게 사용되고 있다. 수많은 IIoT 기기에서 발생된 데이터를 처리하는 것은 기존 중앙 처리 시스템에 큰 부담을 주게 된다. 이러한 데이터들의 효과적인 관리를 위해 데이터가 발생한 엣지 기기, 엣지 서버 등 로컬 위치에서 실시간으로 프로세스를 실행하여 네트워크 대역폭 절약, 낮은 지연 시간 등 특징을 가진 엣지 컴퓨팅 기술을 사용한다. 하지만, 엣지 컴퓨팅 적용 시, 인터넷과 연결된 IIoT 기기 수 증가, 취약한 IIoT 기기, 분산된 환경으로 인해 공격 표면 확장되어 엣지 컴퓨팅 환경에서의 새로운 보안 위협이 발생할 수 있다. 이에 본 논문에서는 IIoT 및 엣지 컴퓨팅 정의, 아키텍처, 각 산업 분야별 적용한 사례에 대해 살펴보고, 엣지 컴퓨팅에서 발생 가능한 보안 위협을 분석하였다. 또한, 엣지 컴퓨팅 기반 IIoT에 대한 각 산업 분야별 보안 연구 동향에 대해서 분석하였다.

Ⅰ. 서 론

Industry 4.0는 정보통신기술(ICT: Information & Communications Technology), 운영 시스템, 사물인터넷(IoT: Internet of Things) 기술이 통합되어 사이버물리시스템(CPS: Cyber Physical System)을 형성하는 새로운 산업 단계를 의미한다[1]. CPS에서 사용되는 IoT 는 서로 데이터를 수집, 처리, 전송 및 수신할 수 있는 수많은 지능형 기기로 구성되있기 때문에 각 기기들에 대한 연결, 정밀 제어, 모니터링 등이 가능하다[2]. 이렇게 산업 환경에서 사용되는 IoT를 산업용 사물 인터넷(IIoT: Industrial Internet of Things)이라고 한다. IIoT를 통해 액추에이터, 센서, 컨트롤러 및 지능형 제어 시스템 등 산업 구성 요소들을 상호 연결하여 효과적으로 제어할 수 있으므로 Industry 4.0의 주요 기술이다. TechNavio社의 'Global Industrial Internet of Things Market 2023-2027' 보고서에 따르면, 글로벌 IIoT 시장 규모는 2022년부터 2027년까지 1,239억 8천만 달러로 성장할 것으로 예측하고 있는데, 이는 산업 분야에서 인터넷에 연결된 IIoT 기기들의 수가 계속 늘어나고 있으며, End-Device가 IIoT 기기로 구성된 센서, 컨트롤러, 기계 등으로 변화하고 있음을 의미한다[3]. [그림 1]은 IoT, IIoT, CPS, Industrial 4.0간 관계를 나타낸 것이다[4].

이러한 IIoT 기술을 사용한 대표적인 산업 분야에는 스마트 공장이 있다. 기존의 공장과는 달리, IIoT 기기를 사용하여 이벤트, 프로세스, 현장 기기를 모니터링하고 제조 산업 운영을 제어하는데 사용되는 OT(Operation Technology) 시스템과 데이터 기반 컴퓨팅 기술을 다루는 IT(Information Technology) 시스템의 융합을 통한 지능화를 구현하는데, 이를 통해 기



〔그림 1〕 IoT, IIoT, CPS, Industry 4.0 관계도

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (RS-2023-00241376, 해양선박 공공 서비스·인프라의 암호화 사이버위협에 대한 네트워크 행위기반 보안관제 기술 개발).
* 가천대학교 정보보호학과 (대학원생, pengchan88@gachon.ac.kr)
** 가천대학교 기계공학과 (학부생, lee990107@gachon.ac.kr)
*** 가천대학교 컴퓨터공학부 (교수, shjeon90@gachon.ac.kr, seojt@gachon.ac.kr)

존 공장에서의 공정 프로세스를 개선, 연결성, 확장성, 실시간성 등의 이점이 생긴다[5]. 하지만, 급격히 수가 증가한 IIoT 기기에서 생성되는 수많은 데이터를 처리하는 것은 중앙 집중 처리 시스템이나 클라우드 서버에 큰 부담을 준다. 또한, 대량의 데이터를 클라우드 서버에 전송하는 과정에서 데이터 처리 지연과 네트워크 혼잡이 발생할 수 있으므로 스마트 공장 등 빠른 실시간 처리가 요구되는 산업 분야에서 문제가 될 수 있다[6].

이는, 데이터가 생성된 위치로부터 가까운 곳에서 데이터를 실시간으로 처리하는 분산 컴퓨팅 프레임워크인 엣지 컴퓨팅을 사용하여 문제를 해결할 수 있다[7]. 엣지 컴퓨팅 기술을 사용하면 IIoT 기기에서 생성된 대용량 데이터를 엣지 기기 근처에서 분석할 수 있으므로 클라우드 서버와 IIoT 기기 간의 데이터 전송 및 네트워크 트래픽이 줄어들고 IIoT 엣지 시스템의 응답성과 신뢰성이 향상시킬 수 있다[8]. 이러한 장점을 통해 엣지 컴퓨팅은 스마트 공장, 교통, 에너지 등 다양한 산업 분야에서 엣지 컴퓨팅 적용 및 관련 연구가 진행되고 있다.

하지만, 엣지 컴퓨팅을 적용할 시, 인터넷에 연결된 IIoT 기기의 수가 늘어나게 되고, 이에 따른 공격 표면도 확장되어 엔터프라이즈 네트워크 침입, DDoS 공격, 데이터 도난 및 유출 등의 공격 위협에 많이 노출될 수 있다[9]. IIoT 환경에 엣지 컴퓨팅 기술을 적용하여 네트워크 대역폭 감소, 실시간 처리 및 지연 시간 감소 등 여러 장점이 존재하지만, 동시에 새로운 보안 문제도 발생한다. 따라서, 엣지 컴퓨팅 환경에서 발생하는 보안 위협에 대응하기 위한 연구가 필요하다.

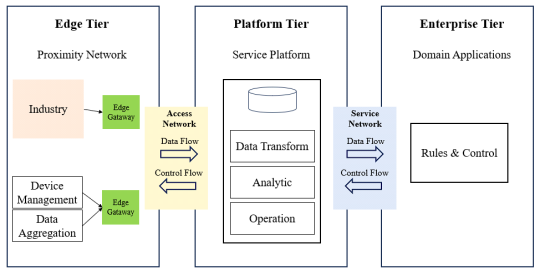
이에, 본 논문에서는 IIoT 및 엣지 컴퓨팅 동향과 엣지 컴퓨팅 기반의 IIoT 보안 기술을 분석하기 위해 2장에서는 IIoT 개요 및 산업 분야 별 적용 사례, 3장에서는 엣지 컴퓨팅 개요, 산업 분야 별 적용 사례, 발생 가능한 보안 위협, 4장에서는 엣지 컴퓨팅 기반 IIoT 보안 기술 연구 동향, 5장에서는 연구 동향 분석을 통한 논의, 6장에서 본 논문의 결론에 대해 기술하였다.

Ⅱ. IIoT

2.1. IIoT 개요

IIoT는 IoT가 산업 현장에 적용되면서 발생한 개념으로, 산업 환경에서의 자원 간 네트워크 상호 연결, 데이터 및 시스템 상호 운용성을 활용하여 유연한 자원 할당, 프로세스의 온디맨드 실행, 프로세스 최적화 및 기기 간 신속한 통신을 통해 효율적이고 지속 가능한 생산을 수행한다. 이러한 IIoT 시스템은 이기종 유무선 네트워크를 통해 상호 연결된 수많은 이기종 노드 기기로 구성된다. 이기종 네트워크에는 이동통신 3G/4G/LTE/5G 네트워크, 무선 Wi-Fi 네트워크, 센서 네트워크 및 산업용 버스 전용 네트워크가 포함된다[10]. 산업 환경에서의 다수의 분산된 이기종 산업기기들은 서로 엣지 네트워크를 형성하여 산업 데이터를 실시간으로 수집하고 해당 데이터들을 클라우드 서버로 전송하여 산업 기기들의 컴퓨팅 및 제어를 수행할 수 있다.

IIoT 기기의 사용률이 증가함에 따라 복잡성, 보안 문제, 통합과 관련된 문제가 발생했다. 산업 분야는 다양한 기술, 플랫폼, 프로토콜을 사용하는데, 서로 간의 통합과 호환성을 강화하기 위한 표준화된 프레임워크가 필요하다. 이를 해결하기 위해 [그림 2]와 같이, 미국 GE, AT&T, IBM, Intel, Cisco 등의 기업에서출범한 IIC(International Industrial Consortium)는 IIoT 시스템의 설계, 구축, 관리를 위한 지침을 제공하기 위해 ISO/IEEE/IEC 42010 표준을 기반으로 IIRA (Industrial Internet Reference Architecture)를 개발 및 IIoT 아키텍처로 채택했다[11]. IIRA는 총 3계층으로 각각 Edge Tier, Platform Tier 및 Enterprise Tier로 구성되어 있다. 먼저, 무선 및 유선 연결을 통해 Edge Gateway에 연결된 다양한 기기, 센서, 노드, 제어 시스템 및 자산이 근접 네트워크를 형성한다. Edge Gateway는 기기 데이터 관리 및 집계를 수행한 다음, 액세스 네트워크를 통해 관련 데이터를 Platform Tier로 보낸다. Platform Tier는 데이터 변환, 운영 및 분석을 수행한다. 이후, 서비스 네트워크를 통해 Enterprise



〔그림 2〕 IIRA 3계층 IIoT 시스템 아키텍처

Tier로 정보를 보낸다. Enterprise Tier에서 사용자는 도메인 애플리케이션에서 모니터링 및 제어를 수행하고 제어 흐름 프로세스를 통해 제어 명령을 Platform Tier로 다시 보낸다. 마지막으로, Platform Tier는 해당 정보를 Edge Tier로 보내어 관련 작업을 수행한다[12].

2.2. IIoT 적용 사례

IIoT는 스마트 공장, 교통, 에너지, 의료, 항공 등 다양한 산업 분야에서 사용되고 있다[13-15]. 스마트 공장에서는 생산 과정의 효율성과 품질 관리를 향상시키는 데 사용되며, 교통 분야에서는 차량 및 교통 신호 간 교통 흐름 제어, 위험 감지를 통한 안전성 향상 등에 사용된다. 에너지에서는 발전소 데이터 수집 및 원격 제어를 통한 효율적인 관리를 하는데 사용되며, 의료 분야에서는 의료 장비 모니터링 및 대용량 의료 영상 저장/전송 등 환자 치료에 사용되며, 항공 산업에서는 수하물 관리, 기내 온도 조절, 정비 데이터 관리 등 항공기 유지보수 및 운영 최적화에 도움이 된다. 이를 통해, IIoT의 적용은 다양한 산업 분야들에서의 운영 효율성과 유지보수 능력을 향상시킬 수 있음을 알 수 있다. [표 1]은 각 산업 분야별 IIoT 적용 사례를 나타낸 것이다.

〔표 1〕 산업 분야별 IIoT 적용 사례

산업 분야	사례	설명
스마트 공장	〔15〕	- Siemens社, Insight Hub - IIoT를 이용한 스마트 공정 프로세스를 수행 - 고급 분석 및 AI를 사용해 커넥티드 제품, 플랜트 및 시스템의 데이터를 사용해 Edge-Cloud간 IIoT 솔루션 강화
	〔16〕	- GM社, Factory ZERO - 단일 공장 내 IoT, 5G, 모바일 네트워크, AI, 클라우드 컴퓨팅, 빅데이터 분석 등의 기술을 적용
교통	〔17〕	- CISCO社, ITS를 위한 IoT 트래픽 제어 - IoT 솔루션을 활용하여 동적 메시지 표지판에서 디지털 메시지 신호를 근처 캐비닛에 있는 산업용 스위치/라우터에 연결 및 운영 센터와 통신
	〔18〕	- FIBERROAD社, IIoT를 사용한 스마트 버스 시스템 - IIoT 센서 및 기기를 통해 버스의 위치, 속도, 연료 소비 및 기타 매개변수에 대한 실시간 데이터를 생성 - 해당 데이터를 분석하여 버스 경로를 최적화하고 정류장에서 유휴 시간을 줄이며 시스템의 전반적인 효율성을 향상시킴
발전 시설	〔19〕	- PAN-CO社, PV-DREAMS 태양광 발전 모니터링 시스템 - ADLINK社의 MXE-210 IIoT Gateway를 사용하여 분산된 태양광 발전소를 효율적으로 관리하기 위한 생산 데이터를 수집 - 태양광 발전 생산 상태 항시 모니터링 가능
	〔20〕	- WILDTHING社, RTU 기기 'WT-R100LM' - 신재생에너지 발전량 데이터 및 원격 모니터링 기기 - 태양광, 태양열, 지열, 풍력 등 각종 에너지원의 발전량, 발전효율 등을 개별 수용가나 발전소 단위로 데이터를 수집 가능
의료	〔21〕	- PEOPLE AND TECHNOLOGY社, IndoorPlus+ 플랫폼 - IoT, IoMT 기술을 활용한 병원 원내 업무 프로세스 효율 개선 - 위치, 센서 데이터의 범위를 확장하여, 환자들의 실시간 체온 및 심박 변화 데이터를 지속적으로 수집
	〔22〕	- HID社, 의료 IoT를 사용한 HID 위치 서비스 - 의사, 환자, 장비에 대한 실시간 위치 확인 및 모니터링을 지원
항공	〔23〕	- MACHBASE社, 실시간 IIoT 데이터 처리기술를 적용한 수하물확인시스템(AIRBRS) 개선
	〔24〕	- Boeing社, IoT 기술을 사용한 신형 항공기 787 Dreamliner 개발 - 항공기의 다양한 부분에 IoT 센서를 배치하여 성능 및 유지관리와 관련된 실시간 데이터 수집 후 분석

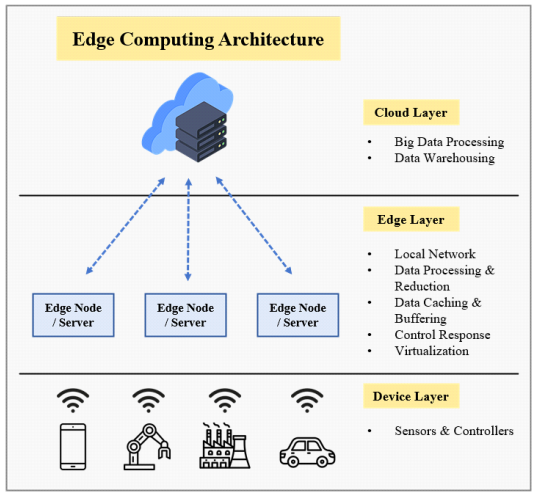
Ⅲ. 엣지 컴퓨팅

3.1. 엣지 컴퓨팅 개요

엣지 컴퓨팅은 엣지 기기가 생성하는 데이터를 클라우드 등의 데이터 센터에서 중앙 집중적으로 처리하는 것이 아닌, 사용자나 데이터 소스가 존재하는 실제 위치, 또는 그 근처인 네트워크 엣지에서 컴퓨팅 작업을 수행하는 것이다. 즉, 클라우드에서 프로세스를 실행하지 않고 데이터가 발생한 엣지 기기나 로컬 엣지 서버 등의 로컬 위치에서 실시간으로 프로세스를 실행한다. 로컬 위치에서 프로세스를 수행하면 클라이언트와 클라우드 사이에 통신이 감소하여 네트워크 대역폭 사용량을 줄일 수 있다. 또한, 근거리에서 실시간으로 데이터 처리를 수행하므로 데이터 처리 시간을 크게 단축할 수 있다. 네트워크 엣지는 엣지 기기 및 엣지 기기를 포함하는 로컬 네트워크가 인터넷과 통신하는 곳으로, 클라이언트 라우터, IoT 기기 내부 프로세서, ISP, 로컬 엣지 서버 등이 해당된다[25, 26]. 이러한 엣지 컴퓨팅 기술에 대한 시장 규모는 계속해서 성장하고 있다. Stratistics MRC社의 “Edge Computing Market Forecasts to 2030“에 따르면, 세계 엣지 컴퓨팅 시장은 2023년 기준, 535억 5,000만 달러이다. 2030년 까지 연평균 성장률 19.8%를 예상하며 성장하여 시장 규모는 1,896억 5,000만 달러까지 성장할 것으로 예상하고 있다[28].

엣지 컴퓨팅을 통해 얻는 이점은 다음과 같다. 먼저, 네트워크 대역폭 사용 및 서버 자원을 최소화하는데 도움이 된다. 일반적인 중앙 집중형 데이터 처리 구조에서는 IIoT 기기에서 대량의 데이터가 생성 시, 소모되는 네트워크 대역폭 및 데이터 스토리지 비용이 증가한다. 엣지 컴퓨팅은 발생한 데이터를 근접한 위치에서 실시간으로 처리하므로 클라우드로 전송하는 데이터가 감소하기 때문에 서버의 자원을 절약할 수 있고, 이는 곧 클라우드 유지 비용의 절감으로 이어진다. 그리고 수집한 데이터를 근처에서 처리하므로 네트워크 대기 시간이 감소한다. 만약, 거리가 먼 곳의 클라우드 서버로 데이터를 보낼 시, 응답을 받는데 까지 상당히 지연될 가능성이 높다. 엣지 컴퓨팅의 특성상 데이터가 생성되는 위치에서 컴퓨팅 작업을 수행하면 지연 시간을 크게 줄일 수 있다. 또한, 클라우드와 클라이언트간 연결을 계속 유지할 필요가 없으므로 인터넷 연결이 불완전 하더라도 컴퓨팅 작업을 수행할 수 있다. 이러한 서비스 측면에서의 유연성과 비용 절감 외에도 기기의 배터리 절약 및 성능을 향상시킬 수 있다는 장점이 있다[25, 27].

엣지 컴퓨팅에서의 아키텍처는 [그림 3]과 같다. 총 3계층으로 데이터 탐색 및 간단한 처리 업무를 수행하는 디바이스 계층, 데이터를 실시간으로 처리를 수행하는 엣지 계층, 각각 포괄적인 데이터를 처리 및 저장을 수행하는 클라우드 계층으로 구성되어 있다. 먼저, 디바이스 계층에는 모든 종류의 센서, 휴대용 단말기, 계측기 및 계량기, 스마트 기계, 스마트 차량, 로봇 및 기타 기기가 포함된다. 해당 기기를 통해 데이터를 수집하며, 이를 위해 다양한 유형의 산업용 유선 네트워크 또는 무선 네트워크를 사용한다. 해당 과정에서, 매개변수 데이터가 엣지 계층으로 전송되고 엣지 계층의 제어 명령을 기다리면서 디바이스 계층과 엣지 계층 간 데이터 및 제어 흐름을 수행한다. 엣지 계층는 엣지 컴퓨팅의 핵심 계층으로 주로 디바이스 계층으로부터 데이터 및 제어 흐름을 수신, 처리 및 전달하는 역할을 수행한다. 또한, Edge 데이터 분석, 지능형 컴퓨팅, 프로세스 최적화 및 실시간 제어 등의 역할도 수행한다. 수집된 데이터를 엣지 계층에서 처리할 수 없을 경우, 클라우드로 데이터를 전송한다. 클라우드 계층은 엣지 계층을 통해 수집된 데이터가 처리 가능한지 여부를 판단하며, 데이터가 클라우드를 통해 처리되어야 할 경우, 데이터를 클라우드 계층으로 전송되게 한다[26, 27].



〔그림 3〕 엣지 컴퓨팅 3계층 아키텍처

3.2. 엣지 컴퓨팅 적용 사례

엣지 컴퓨팅은 낮은 지연 시간, 네트워크 대역폭 절약을 통한 비용 감소, 불완전한 네트워크 환경에서의 동작 가능, 실시간 데이터 분석 등의 특징은 여러 산업 분야에서 필요한 부분이다. 그렇기 때문에, 엣지 컴퓨팅은 스마트 공장, 교통, 에너지, 의료, 항공 등 다양한 산업 분야에서 사용되는 기술이다[29-38]. [표 2]는 각 산업 분야별 엣지 컴퓨팅 적용 사례를 나타낸 것이다.

〔표 2〕 산업 분야별 엣지 컴퓨팅 적용 사례

산업 분야	사례	설명
스마트 공장	〔29〕	- Mitsubishi社, MELIPC - 생산 현장과 IT 시스템의 중간 계층에서 데이터 처리를 수행하는 엣지 컴퓨팅 기능 탑재 - 데이터 수집, 분석, 시각화 및 현장 기기에 대한 실시간 피드백
	〔30〕	- LS ElECTRIC社, Edge Hub - 설비 모니터링용 센서, 설비 제어용 PLC, MES 등과 연동돼 설비 데이터의 수집·저장·처리 및 제어가 가능한 엣지 컴퓨팅 역할을 수행
교통	〔31〕	- Intel社, VITI(Wipro Visual Intelligence in Traffic Intersection) 솔루션 - 비디오 인프라를 활용하여 실시간 교차로 영상을 캡처 - 엣지에서 AI 및 분석을 실시간으로 실현하여 차량 흐름을 관리
	〔32〕	- 한국건설기술연구원(KICT), 스마트 도로조명 플랫폼 - AI를 통해 현장에서 엣지 컴퓨팅으로 작동하므로 빠르게 상황에 대응 가능 - 가로등간 통신이 가능하므로 가시영역 뿐만 아니라 원거리에서의 위험도 감지해 상황 전파 가능
발전 시설	〔33〕	- 한전 KDN, Edge 컴퓨팅 기반 PD (Partial Discharge, 부분방전) 진단시스템 - PD 발생 시에만 Edge Device가 데이터를 전송하므로 기존 대비 네트워크 트래픽 감소 및 대규모 시스템 구축 시에도 진단 속도가 저하되지 않음
	〔34〕	- FirstEnergy社, NVIDIA Jetson Xavier NX - 전신주 및 전력선 검사를 위한 이미지 데이터를 엣지 기기에서 모니터링 및 수집/분석/처리
의료	〔35〕	- NVIDIA社, IGX 플랫폼 - 로봇 보조 수술과 환자 모니터링 등의 의료 애플리케이션을 위한 다양한 기기와 센서에서 필요한 정보 제공 - 엣지, 온프레미스 데이터센터와 클라우드 서비스를 연결
	〔36〕	- GE HealthCare社, Edison HealthLink - 네트워크로 연결된 의료기기의 데이터를 수집하고, 서로 연계하여, 분석하고, 결과를 보여주고 공유 - 검사와 진단이 이루어지는 현장에 컴퓨터를 설치 데이터의 분석 속도가 향상
항공	〔37〕	- Thales社, Thales FlytLink Edge Computing - 클라우드에 연결된 초소형 컴퓨터를 사용하여 탑재된 센서 및 항공 전자 기기에서 데이터를 수집 및 실시간 전송 - 최신 알고리즘을 사용하여 비행 중 또는 지상에서 데이터를 처리
	〔38〕	- CLEARBLADE社, IoT 및 Edge 플랫폼 - 카메라, 센서 및 인프라의 데이터를 처리하기 위해 항공기의 특정 위치에 배포 및 플랫폼으로 전송됨 - 시스템은 데이터를 기록 시스템으로 정규화 및 처리

3.3. 엣지 컴퓨팅 보안 위협

IIoT에 엣지 컴퓨팅을 적용함으로써 네트워크 대역폭 리소스 절약 및 지연 시간 감소, 유지 비용 절감 등의 여러 장점을 얻을 수 있지만, 해당 과정에서 인터넷에 연결된 IIoT 기기 수가 증가하게 되어 공격 표면이 확장된다. 이는 곧 새로운 공격 위협이 발생할 수 있음을 의미한다. 예로 들어, 취약한 엣지 기기, 엣지 서버, 엣지 네트워크 등을 악용하거나 취약한 IIoT 기기를 사용하여 공격을 수행할 수 있다. 만약, 산업 환경을 대상으로 사이버 공격이 수행될 시, 공정 중단, 인명 피해 등 실제 물리적인 피해가 발생할 수 있으므로 엣지 컴퓨팅 보안은 매우 중요하다. 따라서, [표 3]과 같이, 엣지 컴퓨팅 네트워크 계층별 발생 가능한 대표적인 보안 위협을 식별 및 구분하였다. 이를 기반으로 추후 적절한 방어 기술을 적용하여 엣지 컴퓨팅에 대한 공격에 대응할 수 있다[39-40].

〔표 3〕 엣지 컴퓨팅 네트워크 계층별 보안 위협

대상 자산	보안 위협	설명
엣지 기기	데이터 주입	- 일부 취약한 엣지 기기를 악용하여 엣지 컴퓨팅 프로세스 전체를 손상시킬 수 있음 - 악성 데이터 주입을 통한 서비스 방해 및 시스템 침입 시도
	서비스 조작	- 취약한 엣지 기기를 통한 제어 권한 획득 및 특정 서비스에 대한 조작 가능
엣지 네트워크	서비스 거부공격 (DoS, DDoS)	- 손상된 엣지 기기 등 분산 리소스를 기반으로 하며, 공격 목표 기기에게 많은 패킷을 송신함으로써 서로 다른 서버에서 제공하는 정상적인 서비스를 중단시킴
	중간자 공격 (MITM)	- 통신 네트워크를 제어하기 위해 도청, 트래픽 주입 등 공격 수행 가능 - 네트워크 스트림 정보를 탈취해 엣지 네트워크의 모든 기능적 요소에 악영향을 미칠 수 있음
	악성 게이트웨이 (Rogue Gateway)	- 공격자가 악성 게이트웨이를 배포하여 엣지 네트워크 전체 인프라에 트래픽이 주입 - 중간자 공격과 동일한 피해 유발
엣지 서버	개인정보 유출	- 내/외부 공격자 모두 엣지 서버에 접근하여 개인 정보를 훔치거나 변조 가능
	서비스 거부공격	- 손상된 엣지 기기 등 분산 리소스를 기반으로 하며, 공격 목표 기기에게 많은 패킷을 송신함으로써 서로 다른 서버에서 제공하는 정상적인 서비스를 중단시킴
	권한 상승	- 공격자가 엣지 서버에 대한 권한을 취득 후, 권한 남용 및 상위 권한으로 상승 가능
	서비스 조작	- 공격자가 엣지 서버에 대한 권한을 취득 후, 서비스 허위 표시 등 조작 가능
	물리적 손상	- 엣지 인프라의 물리적 보호가 약하거나 부주의할 때 발생 - 엣지 서버가 배포된 특정 영역의 서비스에 영향을 미칠 수 있음
	악성 데이터센터 (Rogue Data Center)	- 공격자가 엣지 서버 전체를 제어하거나 위조할 가능할 정도의 권한을 취득 시, 모든 서비스를 제어 및 정보 흐름을 공격자가 설정한 악성 데이터센터로 송신 가능
클라우드	개인정보 유출	- 클라우드는 제3자 공급업체에 의해 관리될 수 있음 - 해당 업체에 대한 공격 성공 시, 개인정보 유출 가능
	데이터 변조	- 공격자가 통신 채널을 통해 전송되거나 스토리지에 저장된 데이터를 변조 가능
	서비스 거부공격	- 공격자의 서비스에 대한 하이재킹, 허위 정보 주입을 통해 정상 기능을 마비시켜 중요 서비스 실행 방해, 시스템 과부하 등 문제 발생
	서비스 조작	- 권한을 가진 내부 공격자가 서비스 조작하여 다른 개체에 허위 정보 및 서비스가 전달될 수 있음

Ⅳ. 엣지 컴퓨팅 기반 IIoT 보안 기술 연구

본 장에서는 엣지 컴퓨팅 기반의 최신 IIoT 보안 연구 동향에 대해 소개한다. 연구 동향은 각 산업 분야별 총 5가지로 구분하였고, 교통, 에너지, 스마트 공장, 항공, 의료 분야로 구성하였다. [표 4]는 엣지 컴퓨팅 기반 연구 동향에 대해 산업 분야, 보안 방법, 적용 기술로 분류하였다[41-50].

〔표 4〕 엣지 컴퓨팅 보안 연구 사례 분석

산업 분야	연구 사례	보안 방법	적용 기술		
			인공지능	블록체인	암호화
교통	〔41〕	침입탐지	○		
	〔42〕	인증		○	○
에너지	〔43〕	침입탐지	○		
	〔44〕	인증		○	○
스마트 공장	〔45〕	침입탐지	○		
	〔46〕	인증			○
항공	〔47〕	침입탐지 및 인증		○	○
	〔48〕	침입탐지	○		
의료	〔49〕	인증		○	○
	〔50〕	인증	○		○

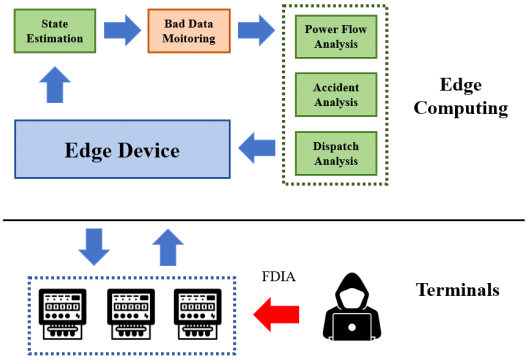
4.1. 교통 분야

Kohli 등 4인[41]은 교통 분야 보안을 위한 엣지 컴퓨팅 및 AI 기반 프레임워크인 MbRE(Multi-branch Reconstruction Error) IDS를 제안하였다. 5G 네트워크 기술과 엣지 컴퓨팅을 접목한 MEC(Multi-access Edge Computing)를 사용하는 교통 네트워크 환경에서의 sybil, DoS 공격 등을 탐지하기 위해 먼저 교통 데이터를 다중 시퀀스 분기로 나눴다. 다중 시퀀스는 차량의 주파수(F), ID(I), 위치, 속도, 가속도, 방향 데이터(M)가 좌표 형태로 구성되어 있으며, 각 시퀀스 데이터 분기마다 각 공격 별 데이터를 포함하여 탐지된 공격 기법마다 좌표 데이터가 다르다. 제안된 IDS는 총 3개의 CNN(Convolutional Neural Network) 모델을 사용하여 훈련되었고, 약 97.5% 이상의 탐지율을 보였다.

Mei 등 5인[42]은 엣지 컴퓨팅 환경의 교통 사이버 물리 시스템에서 블록체인 기반의 개인정보 보호 인증 시스템을 제안하였다. 제안된 인증 시스템에서는 랜덤 오라클 모델의 타원곡선 이산대수 문제(ECDLP: Elliptic Curve Discrete Logarithm Problem)를 기반으로 타원 곡선 암호화 알고리즘과 페어링이 없는 링 서명방식을 사용하였다. 이를 통해, 신원인증의 효율성을 향상시키고, Replay 및 위치 위조 공격에 대해 효과적인 대응이 가능하다. 페어링이 없는 링 서명 방식을 통해 리소스 오버헤드를 크게 줄였으며 데이터 무결성 및 데이터 소유자의 완전한 신원 익명성을 보장하였다. 또한 기존 시스템과의 성능 비교를 통해 제안된 인증 시스템이 사용 가능함을 증명하였다.

4.2. 에너지 분야

Chen 등 8인[43]은 엣지 컴퓨팅 아키텍처 기반의 스마트 그리드 환경에서의 허위 데이터 주입 공격(FDIA: False Data Injection Attack) 탐지를 위해 Infinite-norm 및 2-norm 기반으로 추정한 회귀식과 실제 관측 값의 차이인 잔차를 분석하며 이를 벡터 자동 회귀(VAR: Vector Auto Regression) 모델과 통합하여 사용하는 방안을 제안하였다. VAR은 시간별 변화하는 변수 간의 관계를 캡처하는 데 사용되는 통계 모델이며 FDIA의 단기 예측을 수행한다. 잔차 분석 방법에 사용되는 Infinite-norm 및 2-norm 방정식을



〔그림 4〕 엣지 컴퓨팅에서의 FDIA 모델

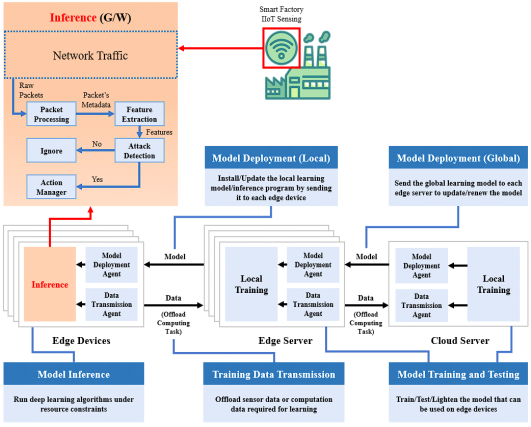
FDIA 분류 검출기에 정규화하여 생성한다. FIDA 분류 검출기 값이 0이면 공격이 없음을, 1이면 공격이 존재함을 나타낸다. [그림 4]는 엣지 컴퓨팅에서의 FDIA 모델을 나타낸 것이다. 제안된 모델은 IEEE 14-Bus 전력망 시스템을 대상으로 성능 평가하였고, 약 87~95% 이상의 탐지율을 보였다. 이를 통해, 스마트 그리드 애플리케이션의 안정적인 전원 공급 및 안전한 작동을 수행할 수 있음을 확인하였다.

Iindombo 등 2인[44]은 스마트 그리드 환경에서의 엣지 컴퓨팅 사용 시 발생 가능한 IIoT 기기의 다양한 보안 문제를 해결하기 위해 블록체인 보안 계층 구현 분석 및 엣지 컴퓨팅과 블록체인의 통합과 관련된 연구를 진행하였다. 블록체인을 안전하게 유지하기 위해 P2P 방식의 비대칭 암호화를 사용하며, 분산 방식으로 작동되므로 탈중앙화적인 특징을 보인다. 또한, 블록체인의 각 블록에는 이전 블록의 해시가 표현되어 있어 블록을 통해 블록체인의 시작점까지 추적 가능하다. 즉, 블록이 형성된 후에는 IIoT 기기 간의 트랜잭션을 변경하는 것 어려우므로 IIoT 기기 트랜잭션이 지속되므로 블록체인은 신뢰 가능한 데이터베이스 역할을 수행할 수 있다. 이러한 장점을 기반으로 스마트 엣지 컴퓨팅에 블록체인 보안 계층을 구현하고 스마트 그리드와 IIoT 기기 사이에 배치함으로써 IIoT 기기에서 수집된 데이터를 블록체인 보안 계층을 통해 보호한 후, 스마트 그리드로 처리할 수 있다. 하지만, 블록체인 기술의 복잡성, 암호화 방식의 한계성 등 아직까지 보완할 점이 많음을 확인하였다.

4.3. 스마트 공장

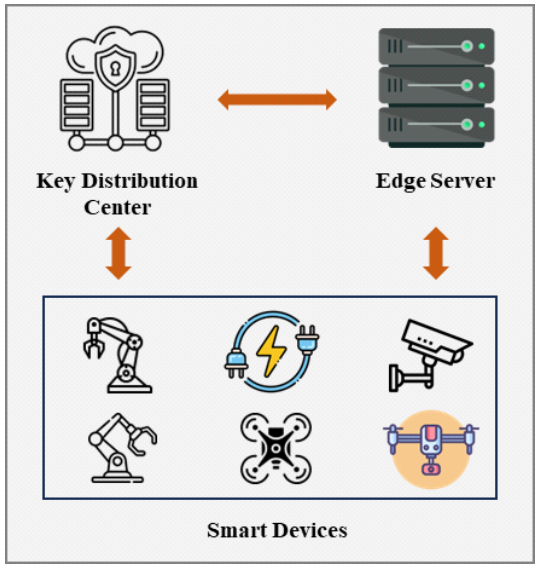
Kim 등 2인[45]은 스마트팩토리 IIoT 트래픽 정보

를 엣지 서버에 분산시켜 딥러닝 처리를 함으로써 다양한 악성코드를 효율적으로 탐지하는 엣지 컴퓨팅 기반 악성코드 탐지 시스템을 제안하였다. 탐지 시스템의 주요 기능은 엣지 컴퓨팅 3계층 아키텍처를 기반으로 개발되었다. [그림 5]는 제안한 엣지 컴퓨팅 기반 악성코드 탐지 시스템 주요 기능이다. 먼저, 분석할 악성코드 데이터는 IIoT 센서에서 엣지 기기로 전송되며, 엣지 기기에서는 IP Port, 프로토콜, Flow 메타데이터 등 수집된 분석할 악성코드 데이터의 Feature을 추출한다. 추출된 Feature 데이터는 로컬에서 딥러닝 모델 학습을 수행하여 생성된 모델과 함께 엣지 서버로 전송된다. 이후, 여러 엣지 서버 및 네트워크에서 생성된 로컬 정보를 수신하여 딥러닝 모델을 업데이트하고, 최적화된 보안 모델을 로컬 엣지 네트워크에서 공유 및 적용한다. 한편, 악성코드를 탐지하기 위해 9개의 컨볼루션 레이어로 구성된 CNN 모델 및 이미지 시각화 기술을 결합하였다. 제안된 탐지 시스템은 25가지 악성코드 유형에 대해 약 98.93%의 탐지율을 보였다.



〔그림 5〕 Kim 등 2인〔45〕이 제안한 엣지 컴퓨팅 기반 악성코드 탐지 시스템 주요 기능

Cui 등 5인[46]은 스마트 공장에서 사용되는 스마트 기기가 실시간으로 생성하는 메시지를 인증하는 과정에서, 기존 IIoT 환경의 메시지 인증 방식은 각 메시지를 개별적으로 인증하는 특징으로 인해 중복된 작업이 많이 발생하게 된다. 이를 개선하기 위해 IIoT 환경에서 엣지 컴퓨팅 기반의 메시지 일괄 인증 방식을 제안하였다. 먼저, 엣지 서버를 사용한 스마트 기기의 메시지 인증은 스마트 기기의 연산 부담 감소 및 효율성



〔그림 6〕 Cui 등 5인〔46〕이 제안한 IIoT 시스템 모델

을 향상시켰다. 또한, 엣지 서버의 알림 메시지 서명 비용을 줄이기 위해 해시 체인과 타원곡선암호(ECC: Elliptic Curve Cryptography) 기반의 경량 서명 알고리즘을 설계하여 데이터 보안성 향상 및 엣지 서버의 알림 메시지 서명 비용을 감소시켰다. [그림 6]은 제안한 IIoT 시스템 모델을 나타낸 것이며, 스마트 기기의 실제 신원을 확인하는 키 배포 센터(KDC), 스마트 기기의 인증을 지원하는 엣지 서버(ES), 스마트 기기(SD)로 구성되어 있다. 먼저, 메시지의 암호화, 암호해독, 서명 및 확인 기능을 구현하기 위해 KDC에서 시스템 매개변수를 생성한다. 그리고 데이터의 익명성을 보장하기 위해 SD 가명 사용 및 비밀 키를 생성한다. 이후, 메시지 암호화 및 서명 단계를 거쳐 ES에서 일괄 인증을 수행한다. 인증 후, SD의 데이터 검증을 지원하기 위한 데이터 유효성 알림 메시지를 생성한다. 메시지가 유효한 경우, 메시지를 복구한다. 제안된 기법은 C++ 및 Miracl Core 라이브러리, BLS12381 곡선, AES 암호화 및 해시맵을 사용한 FinList 구현을 통해 설계하였다. 성능 평가 결과, 기존 연구 사례들보다 오버헤드가 낮음을 확인하였다.

4.4. 항공 분야

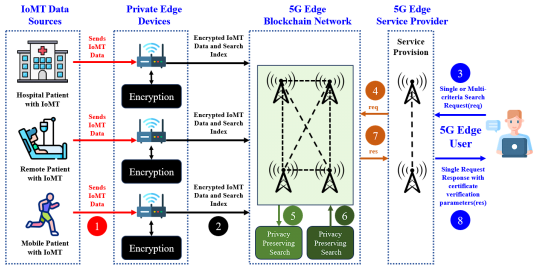
Yao 등 8인[47]은 엣지 컴퓨팅 기반 무인 항공기(UAV: Unmanned Aerial Vehicle) 배송 시스템에서

발생 가능한 네트워크 침입, 인증 등 여러 보안 위협 문제를 해결하기 위해 새로운 보안 프레임워크인 A2DSEC(Authentication, Detection, Defense for Secure Edge Computing)를 제안하였다. A2DSEC 프레임워크는 총 4계층이며, 인프라 계층, 보안 보호 계층, 애플리케이션 계층 및 사용자 상호 작용 계층으로 구분된다. 또한, 사용자/데이터 서비스/블록체인의 구성 요소를 포함하는 인증 모듈, 오용 및 이상탐지, 탐지 관리를 수행하는 탐지 모듈, 데이터 관리와 허니넷 관리를 수행하는 능동 방어 모듈이 존재한다. 실제 엣지 컴퓨팅 기반 UAV 배송 시스템인 UAV-EXPRESS에 A2DSEC 프레임워크를 적용한 후, DDoS 공격을 통해 프레임워크의 효율성을 평가하였다. 10개 그룹의 DDoS 공격을 무작위로 구현하여 방화벽 및 IPS 시스템에서 침입 탐지까지 평균 1.32초의 시간이 소모됨을 보였다.

Xu 등 7인[48]은 UAV의 이상 상태를 통해 네트워크 내 악성 공격을 탐지하기 위한 다중 접근 엣지 컴퓨팅(MEC: Multi-Access Edge Computing) 기반 UAV 배송 시스템의 다중 특징 이상 탐지(MFAD: Multi-Featured Anomaly Protection) 방법을 제안하였다. 먼저, 정상 상태의 여러 일반적인 UAV 데이터를 사용하여 정상적인 UAV 동작을 인식하는 딥러닝 모델을 GRU, RN, LSTM를 비교하여 개발한다. 그리고 비정상적인 UAV 동작을 시뮬레이션하기 위해 정상 데이터에 비정상 데이터를 포함시킨다. 이후, 비정상 데이터를 선택된 정상 상태 모델에 병합하여 입력 데이터와 정상 행위 모델이 제공하는 데이터 간의 NRMSE(Normalized Root Mean Square Error)값을 도출하여 이를 기반으로 임계값을 계산한다. 제안한 방식에서 통합 탐지를 수행할 경우, UAV 센서 데이터에서 5가지 Feature를 감지한다. 이를 기반으로, 성능 평가를 하여 약 98%의 탐지율을 보였고 UAV 시스템의 필수 에너지 소비 감소를 확인하였다.

4.5. 의료 분야

Rahman 등 3인[49]은 5G 통신 기술과 엣지 컴퓨팅 기술이 병합된 5G 엣지 기반 블록체인 네트워크 환경에서의 IoMT(Internet-of-Medical Things) 데이터에 대한 개인 정보 보호 인증 프레임워크를 제안하였다. 5G 엣지 플랫폼에서의 내부자 공격으로 인한 IoMT 데이터의 무결성 및 개인정보보호 위협이 발생할 수 있다. 이에, 제안된 프레임워크에서는 5G 엣지 서버가 포함된 블록체인 플랫폼을 도입 및 5G 엣지 기반 블록체인을 위해 암호화된 데이터 저장 모델과 대칭 키 암호화 기반 개인 정보 보호 검색 메커니즘이 개발되었다. 또한, 효율적인 다중 서명 체계를 활용하여 5G 엣지 기반 블록체인에서 IoMT 데이터에 대한 인증 메커니즘을 설계하였다. [그림 7]은 5G 엣지 기반 개인 정보 보호 IoMT 데이터 인증 프레임워크를 나타낸 것이다. 먼저, IoMT 데이터는 다양한 소스에서 생성되어 Private 엣지 기기로 전송된다. Private 엣지 기기는 IoMT 데이터를 암호화하고 암호화된 검색 인덱스를 생성 및 5G 엣지 블록체인에 저장한다. 5G 엣지 사용자가 검색 요청을 5G 엣지 서비스 제공업체에 전달할 시, 5G 엣지 서비스 제공업체는 해당 요청을 5G 엣지 블록체인 네트워크로 전달한다. 5G 엣지 블록체인 네트워크의 블록체인 노드는 개인 정보 보호 검색을 수행한다. 블록체인 노드는 검색 결과에 대한 인증서를 생성하고, 5G 엣지 블록체인 네트워크는 인증된 검색 결과를 5G 엣지 서비스 제공자에게 전달한다. 마지막으로, 5G 엣지 서비스 제공자는 인증된 검색 결과와 검증 매개변수를 5G 엣지 사용자에게 전송 및 검증에 사용한다.



〔그림 7〕 Rahman 등 3인[49]이 제안한 5G 엣지 기반 개인 정보 보호 IoMT 데이터 인증 프레임워크

Singh 등 2인[50]은 전자 스마트 헬스케어 시스템(SHS: Smart Healthcare System)을 위한 엣지 컴퓨팅 기반의 SEoT(Secure Edge of Things) 보안 프레임워크를 제안하였다. 제안된 프레임워크에는 낮은 비용과 대기 시간으로 높은 수준의 개인정보보호와 접근 제어를 유지하기 위해 접근 정책이 포함된 ABE 암호화 기술이 포함되었다. ABE 암호화 기술을 적용하면 클라우드 계층에 민감한 개인 의료 데이터 정보를 왜곡하

여 저장할 수 있다. 암호화 키 생성 작업에 사용되는 알고리즘은 총 3가지이며, 각각 ATREE_GEN(), MKEY_GEN(), TOK_GEN() 알고리즘으로 구성된다. 접근 정책은 전자 건강 기록(EHR: Electronic Health Record)의 각 속성에 대해 EHR의 접근 구조를 기반으로 생성된다.

Ⅴ. 논 의

연구 동향 조사를 통해, 엣지 컴퓨팅 기반 IIoT 보안 방법은 주로 침입탐지 및 인증 강화 방식이 많았음을 확인하였다. 침입 탐지를 위해 주로 머신러닝 및 딥러닝 등 인공지능 기술을 사용하였고, 인증 강화를 위해 주로 블록체인 및 암호화 기술을 사용하였다. 하지만, 블록체인 등 적용하려는 기술의 구현에 대한 복잡성, 한계성 등으로 인한 실제 구현에서의 일부 어려운 부분이 존재함을 확인하였다.

IIoT 환경에서의 엣지 컴퓨팅 채택률이 높아짐에 따라 인터넷과 연결되는 IIoT 기기, 엣지 컴퓨팅을 쉽게 활용할 수 있는 엣지 컴퓨팅 플랫폼, 오픈소스 등은 계속 증가할 것으로 예상된다. 이를 대상으로 발생 가능한 새로운 보안 위협들로 인해 산업 환경에서 큰 피해가 발생할 수 있으므로 이에 대한 지속적인 연구가 필요할 것으로 판단된다. 또한, 향후 엣지 컴퓨팅과 5G, 블록체인 등 타 기술 간 결합에 대한 중요성은 보안 및 성능 측면에서 지속적으로 높아질 것으로 예상된다.

Ⅵ. 결 론

본 논문에서는 IIoT와 엣지 컴퓨팅에 대해 분석하고 엣지 컴퓨팅 기반 IIoT에 대한 각 산업 분야별 최신 보안 연구 동향에 대해서 조사하였다. 현재까지 IoT는 다양한 산업 분야에서 사용되고 있으며 IIoT를 기반으로 엣지 컴퓨팅 기술을 산업 분야에 적용하여 낮은 지연 시간, 네트워크 대역폭 절약, 유지 비용 감소 등 여러 장점을 보인다. 엣지 컴퓨팅 적용 과정에서 새로운 공격 위협이 발생할 수 있으며, 이에 대응하기 위해 인공지능, 블록체인, 암호화 등의 다양한 기술을 적용한 침입 탐지, 인증 강화 등 보안 방법들을 각 산업 분야에 적용한 최신 연구 사례를 분석하였다. 엣지 컴퓨팅 사용을 위한 플랫폼, 오픈소스 등의 지속적인 증가, 엣지 컴퓨팅과 5G, 블록체인 등 타 기술과의 융합에 대한 중요성 강조 및 지속적인 연구가 필요할 것으로 예상하였다.

참 고 문 헌

[1] Wang, L., et al. "Current status and advancement of cyber-physical systems in manufacturing", Journal of manufacturing systems 37, pp. 517-527, 2015.

[2] Shishehgarkhaneh, M. B., et al. "Blockchain in the Construction Industry between 2016 and 2022: A Review", Bibliometric, and Network Analysis. Smart Cities, 6(2), pp. 819-845, 2023.

[3] technavio, “Global Industrial Internet of Things Market 2023-2027”, https://www.technavio.com/report/industrial-internet-of-things-market-industry-analysis?now=, accessed: 2023-11-30

[4] Kebande, V. R., "Industrial internet of things (IIoT) forensics: The forgotten concept in the race towards industry 4.0", Forensic Science International: Reports 5, 100257, 2022.

[5] Mantravadi, S., "devices: design considerations for industry 4.0", IEEE Access, 8, pp. 200305-200321, 2020

[6] e4dsnews, “방대한 IIoT 데이터 처리, 클라우드만으론 한계 "시계열 데이터베이스 필요해”, https://www.e4ds.com/sub_view.asp?ch=1&t=0&idx=11144, accessed: 2023-11-30

[7] TechTarget, “What is edge computing? Everything you need to know”, https://www.techtarget.com/searchdatacenter/definition/edge-computing, accessed: 2023-11-30

[8] Industrial Internet Consortium, “Introduction to Edge Computing in IIoT”, 2018

[9] ciokorea, “엣지 컴퓨팅이 보안 위협 모델에 가져올 4가지 큰 변화, https://www.ciokorea.com/news/153932?page=0,0#csidx8a6096bae09fbdd850139e46148ee89, accessed: 2023-11-30

[10] Qiu, T., et al. "A novel shortcut addition algorithm with particle swarm for multisink Internet of Things", IEEE Transactions on Industrial Informatics, 16(5), pp. 3566-3577, 2019

[11] Lin, Shi-Wan, et al. "Industrial internet reference architecture." Industrial Internet Consortium (IIC), Tech. Rep, 2015

[12] IIC, “A Common IoT Framework”, https://www.iiconsortium.org/iira/, accessed: 2023-11-30

[13] Intel, “Intelligent Transportation System(ITS) Solutions”, https://www.intel.com/content/www/us/en/transportation/overview.html, accessed: 2023-11-30

[14] CONTROL AUTOMATION, “Growing IIoT Capabilities in the Healthcare and Medical Industries”, https://control.com/technical-articles/growing-iiot-capabilities-in-the-healthcare-and-medical-industries/, accessed: 2023-11-30

[15] SIEMENS, “Insights Hub”, https://plm.sw.siemens.com/ko-KR/insights-hub/, accessed: 2023-11-30

[16] GM, “Factory ZERO, Our First Fully Dedicated EV Assembly Plant”, https://www.gm.com/stories/factory-zero-first-dedicated-ev-plant, accessed: 2023-11-30

[17] Cisco, “Connecting DOTs with IoT for Intelligent Transportation Systems”, https://blogs.cisco.com/transportation/connecting-dots-with-iot-for-intelligent-transportation-systems, accessed: 2023-11-30

[18] Fiberroad Technology, “HOW IIOT CAN OPTIMISE SMART BUS SYSTEM”, https://fiberroad.com/solutions/security-solutions/how-iiot-can-optimise-smart-bus-system/, accessed: 2023-11-30

[19] ADLINK, “IIoT Gateway for Monitoring Photovoltaic Power Station”, https://www.adlinktech.com/en/iiot-gateway-monitor-pv-power-station, accessed: 2023-11-30

[20] 스타트업, “IIoT스타트업 와일드싱, 신재생에너지 사업자를 위한 PaaS 클라우드 서비스 ‘솔라게이트’ 출시”, https://www.startupdaily.kr/news/articleView.html?idxno=677, accessed: 2023-11-30

[21] PEOPLE AND TECHNOLOGY, “IndoorPlus+ SmartCare”, https://smartcare.indoorplus.io/?page_id=952, accessed: 2023-11-30

[22] HID, “Healthcare IoT”, https://www.hidglobal.com/solutions/healthcare-iot, accessed: 2023-11-30

[23] 전자신문, “마크베이스, 인천국제공항 수하물확인 시스템(AIRBRS) 개선 사업 수주…실시간 IIoT 데이터 처리기술 적용”, https://www.etnews.com/20230908000057, accessed: 2023-11-30

[24] nasscom community, “ROLE OF LEADING IOT COMPANIES IN THE AVIATION INDUSTRY”, https://community.nasscom.in/communities/iot/role-leading-iot-companies-aviation-industry, accessed: 2023-11-30

[25] CloudFlare, “What is edge computing?”, https://www.cloudflare.com/learning/serverless/glossary/what-is-edge-computing/, accessed: 2023-11-30

[26] Qiu, T., et al. "Edge computing in industrial internet of things: Architecture, advances and challenges", IEEE Communications Surveys & Tutorials, 22(4), pp. 2462-2488, 2020

[27] NordVPN, “엣지 컴퓨팅이란?”, https://nordvpn.com/ko/blog/edge-computing-meaning/, accessed: 2023-11-30

[28] GII, “엣지 컴퓨팅 시장 예측(-2030년) - 컴포넌트별, 조직 규모별, 전개별, 용도별, 산업별, 지역별 세계 분석”, https://www.giikorea.co.kr/report/smrc1308681-edge-computing-market-forecasts-global-analysis-by.html?CODE=smrc1308681-edge-computing-market-forecasts-global-analysis-by.html&TYPE=0, accessed: 2023-11-30

[29] Mitsubishi Electric, “MELIPC”, https://kr.mitsubishielectric.com/fa/ko/product.do?act=productList&parent_id=932&cate_id=2, accessed: 2023-11-30

[30] 인더스트리 뉴스, “SKT ‘그랜드뷰’와 LS일렉트릭 ‘엣지 허브’ 결합, ‘엣지-투-클라우드’ 출시”, https://www.industrynews.co.kr/news/articleView.html?idxno=42128, accessed: 2023-11-30

[31] Intel, “Smart Roads Start with Smart Infrastructure”, https://www.intel.com/content/www/us/en/transportation/smart-road-infrastructure.html

[32] KICT, “인공지능 스마트 도로조명 플랫폼으로 국민안전 지킨다”, https://www.kict.re.kr/board.es?mid=a10105060000&bid=pressrls&list_no=16435&act=view, accessed: 2023-11-30

[33] 한전KDN, “전력산업과 인공지능 기술”, 2022

[34] Nvidia, “Startup Surge: Utility Feels Power of Computer Vision to Track Its Lines”, https://blogs.nvidia.com/blog/power-utility-ai-edge/, accessed: 2023-11-30

[35] 로봇신문, “엔비디아, 의료 로봇기업과 디지털 수술 스타트업에 의료 엣지 컴퓨팅 플랫폼 제공”, http://m.irobotnews.com/news/articleView.html?idxno=29619, accessed: 2023-11-30

[36] GE리포트 코리아, “헬스케어 엣지 컴퓨팅 - 인공지능을 환자와 의료진에 더욱 가깝게”, https://www.gereports.kr/edge-computing-can-give-doctors-access-to-ai-and-faster/, accessed: 2023-11-30

[37] Thales, “Thales and VoltAero to bring innovative data collection and computing solutions to the Cassio electric-hybrid aircraft”, https://onboard.thalesgroup.com/thales-and-voltaero-data-collection-and-computing-cassio/, accessed: 2023-11-30

[38] Avionics, “New Products: Aircraft Edge Computing”, https://interactive.aviationtoday.com/avionicsmagazine/july-august-2023/new-products-aircraft-edge-computing/, accessed: 2023-11-30

[39] Alwakeel, A. M., “An overview of fog computing and edge computing security and privacy issues”, Sensors, 21(24), 8226, 2021

[40] Zeyu, H., et al. “Survey on edge computing security”, In 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), IEEE, pp. 96-105, 2020

[41] Kohli, V., et al. “MbRE IDS: an AI and edge computing empowered framework for securing intelligent transportation systems”, In IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, pp. 1-6, 2022

[42] Mei, Q., et al. “Blockchain-enabled privacy-preserving authentication mechanism for transportation cps with cloud-edge computing”, IEEE Transactions on Engineering Management, 2022

[43] Chen, Y., et al. “Vector auto-regression-based false data injection attack detection method in edge computing environment”, Sensors, 22(18), 6789. 2022

[44] Iindombo, S., et al. “An Analysis of the Implementation of Blockchain Technology in Smart Grid Edge IoT Devices”, In 2023 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), IEEE, pp. 1-5, 2023

[45] Kim, H. M., et al. “Iiot malware detection using edge computing and deep learning for cybersecurity in smart factories”, Applied Sciences, 12(15), 7679. 2022

[46] Cui, J., et al. “Efficient batch authentication scheme based on edge computing in iiot”, IEEE Transactions on Network and Service Management, 20(1), pp. 357-368, 2022

[47] Yao, A., et al. “A novel security framework for edge computing based uav delivery system”, In 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE, pp. 1031-1038, 2021

[48] Xu, L., et al. “Multi-Featured Anomaly Detection for Mobile Edge Computing Based UAV Delivery Systems”, In Proceedings of the 2023 Australasian Computer Science Week, pp. 58-65, 2023

[49] Rahman, M. S., et al. “Privacy aware internet of medical things data certification framework on healthcare blockchain of 5G edge”, Computer Communications, 192, pp. 373-381, 2022

[50] Singh, A., et al. “Edge computing based secure health monitoring framework for electronic healthcare system”, Cluster Computing, 26(2), pp. 1205-1220. 2023

〈저 자 소 개〉

전 규 현 (GyuHyun Jeon)

학생회원

2023년 2월 : 가천대학교 컴퓨터공학과 학사 졸업
2023년 3월~현재 : 가천대학교 정보보호학과 석사과정
<관심분야> CPS 보안, AI 보안

이 진 규 (Jin Gyu Lee)

2022년 2월 : 인하공업전문대학교 메카트로닉스학과 졸업
2022년 3월~현재 : 가천대학교 기계공학과 학사과정
<관심분야> CPS 보안, IoT 보안

전 승 호 (Seungho Jeon)

2018년 2월 : 고려대학교 정보보호학과 석사 졸업
2022년 8월 : 고려대학교 정보보호학과 박사 졸업
2023년 1월~현재 : 가천대학교 컴퓨터공학부 스마트보안 전공 연구교수
<관심분야> 딥러닝, 시스템 보안

서 정 택 (Jung Taek Seo)

종신회원

1999년 2월 : 한국교통대학교 컴퓨터공학과 학사 졸업
2001년 2월 : 아주대학교 컴퓨터공학과 석사 졸업
2006년 2월 : 고려대학교 정보보호공학 박사 졸업
2016년 3월~2021년 2월 : 순천향대학교 정보보호학과 부교수
2021년 3월~현재 : 가천대학교 컴퓨터공학부 부교수
2000년 11월~2016년 2월 : 국가보안기술연구소 책임연구원/연구부장
2014년 6월~2015년 6월 : University of Florida 초빙연구원
2009년 12월~2013년 5월 : 제주 스마트그리드 실증단지 보안센터 센터장
2013년, 2018년 : 한국철도공사 정보화자문단 자문위원
2016년 1월~2016년 12월 : ㈜ SR 철도안전자문단 자문위원
2017년 1월~현재 : 한국정보보호학회 CPS보안연구회 위원장
2017년 2월~현재 : 한국남동발전 사이버보안자문단 자문위원
2017년 11월~현재 : 인천국제공항공사 사이버보안 자문위원회 자문위원
2018년 12월~현재 : 한국서부발전 사이버보안 자문위원
2020년 6월~현재 : 한국전력공사 보안위원회 자문위원
<관심분야> CPS보안, 제어시스템 보안, 스마트그리드 보안, 원자력 발전 사이버보안, 스마트팩토리 보안, 스마트시티 보안, 자율주행인프라 보안, 해양선박 보안, 항공우주 보안