JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 26, No. 3, pp. 787-798, Mar. 2025

Check for updates

프라이빗 블록체인을 적용한 전술적 마이크로그리드 사이버 보안 체계 개발

최 연 호[1] · 손 태 식[2*]
[1]아주대학교 정보통신대학원 정보통신공학과 석사과정
[2]아주대학교 정보통신대학원 사이버보안학과 교수

Developing a Tactical Microgrid Cybersecurity System Using Private Blockchain

Yeon-ho Choi[1] · Taeshik Shon[2*]

[1]Master's Course, Graduate School of Information and Communication Technology, Ajou University, Suwon 16499, Korea
[2]Professor, Department of Cyber Security, Ajou University, Suwon 16499, Korea

[요 약]

현대 문명의 발전과 함께 전력 수요 급증하고 있다. 중앙집중식 전력망은 대규모 정전, 송전 손실, 재생 가능 에너지 통합의 어려움과 같은 여러 한계를 안고 있다. 이러한 문제를 해결하기 위해 마이크로그리드가 등장했으며, 이는 지역적 독립성과 유연성을 바탕으로 중앙 전력망의 약점을 보완하고, 군사적 전력망에서도 효율적이고 안정적인 전력 공급을 가능하게 한다. 마이크로그리드의 보안은 특히 중요하다. 분산된 에너지 시스템은 사이버 공격과 데이터 위변조에 취약하며, 마이크로그리드에서 데이터의 기밀성, 무결성, 가용성이 보장되지 않으면 운영 차질이 발생할 수 있다. 프라이빗 블록체인은 이러한 문제를 해결할 수 있다. 본 논문은 마이크로그리드의 보안을 강화하기 위해 프라이빗 블록체인의 보안 요소를 결합하여, 전력 운용을 더욱 효율적이고 안전하게 관리할 수 있는 방안을 제시한다.

[Abstract]

Electricity demand is rapidly increasing with the advancement of modern civilization. Centralized power grids have several limitations, such as large-scale blackouts, transmission losses, and difficulties in integrating renewable energy. To solve these problems, microgrids have emerged, which complement the weaknesses of centralized power grids based on regional independence and flexibility and enable efficient and stable power supply even in military power grids. The security of microgrids is particularly important. Distributed energy systems are vulnerable to cyberattacks and data falsification, and if the confidentiality, integrity, and availability of data in microgrids are not guaranteed, operational disruptions may occur. Private blockchains can solve these problems. This paper proposes a method to manage power operations more efficiently and safely by combining the security elements of private blockchains to strengthen the security of microgrids.

색인어 : 에너지 통합, 마이크로그리드, 분산 에너지 시스템, 사이버 공격, 프라이빗 블록체인
Keyword : Energy Integration, Microgrids, Distributed Energy Systems, Cyber Attacks, Private Blockchain

http://dx.doi.org/10.9728/dcs.2025.26.3.787

Received 25 December 2024; **Revised** 4 February 2025
Accepted 14 March 2025

Corresponding Author; Taeshik Shon
Tel: +82-31-219-3321
E-mail: tsshon@ajou.ac.kr

Ⅰ. 서 론

급격한 문명 발전과 함께 전기의 사용은 필수적이 되었으며, 문명이 발전할수록 전기 사용량은 급증하고 있다. 알베르트 아이슈타인(Albert Einstein)은 전기와 에너지에 대한 연구에서 중요한 기여를 했으며, 그의 이론은 현대 물리학과 기술 발전에 큰 영향을 미쳤다. 최근 암호화폐, 인공지능(AI), 클라우드 서비스 등 다양한 기술 분야에서 전기 사용량이 급격히 증가하고 있다.

현재 가장 널리 사용되고 있는 중앙집중식 전력망은 대규모 정전, 송전 손실, 재생 가능 에너지의 통합 어려움 등의 문제를 안고 있다. 마이크로그리드는 이러한 문제를 해결할 수 있는 대안으로, 지역적 독립성과 유연성을 제공하며, 재생 가능 에너지의 효율적 통합을 가능하게 하다. 마이크로그리드는 중앙집중식 전력망에 비해 여러 가지 중요한 장점을 가지고 있다. 우선, 독립성과 유연성이 뛰어나 특정 지역에서 독립적으로 운영될 수 있어 중앙집중식 전력망에서 발생할 수 있는 대규모 정전이나 장애 상황에서도 전력 공급이 유지될 수 있다. 또한, 마이크로그리드는 전력을 현지에서 생산하고 소비하기 때문에 송전 거리가 짧아 에너지 손실이 최소화되며, 이는 중앙집중식 전력망에서 흔히 발생하는 송전 손실 문제를 효과적으로 해결한다. 더 나아가, 마이크로그리드는 태양광, 풍력 등 재생 가능 에너지원의 통합이 용이해, 지역별 자원과 수요에 맞추어 에너지 공급을 조절할 수 있어 재생 가능 에너지의 변동성에도 유연하게 대응할 수 있다. 또한, 분산된 구조 덕분에 사이버 공격이나 자연재해와 같은 외부 위협에 대한 복원력이 높아 보안성이 강화되며, 지역별 수요에 맞춘 맞춤형 에너지 관리가 가능하여 전력 사용의 효율성을 극대화할 수 있다. 이러한 점에서 마이크로그리드는 중앙집중식 전력망의 한계를 보완하고, 더욱 안정적이고 효율적인 전력 공급을 실현할 수 있는 중요한 대안으로 평가받고 있다.

전술적 마이크로그리드는 군사 작전 영역에서 분산된 에너지 생산과 지능형 그리드 관리를 결합하여 독립적이고 신속한 전력 공급체를 제공한다. 이는 정상적인 전력 공급망이나 민간 환경에서의 전력 공급과는 다르게 군사적인, 특수성을 고려한 안정성과 탄력성 있는 에너지 솔루션을 제공하는 것을 목표로 한다. 육군비전 2050 수정 1호에서는 시간과 장소에 구애받지 않고 지속적인 전력 공급이 가능한 에너지 지원 체계가 필요하다고 피력했다[1]. 이러한 요구를 충족시키기 위해 스마트그리드와 소형 원자로의 도입이 필수적이다. 스마트그리드는 전력 공급의 효율성을 높이고, 실시간으로 전력 분배와 관리가 가능하게 하여 에너지 사용을 최적화한다. 또한, 소형 원자로는 전력의 자급자족을 가능하게 하여 전력의 안정적 공급을 보장하고, 이를 통해 지속지원능력 확보와 전투원의 생존성 향상에 크게 기여한다.

전술적 마이크로그리드 구성으로 다양한 전력 생성 소스, 에너지 저장 장치, 분배 시스템, 제어 시스템 및 부하 장치로 이루어져 있다. 이러한 시스템의 복잡성과 상호 연결성은 네트워크 공격, 악성 소프트웨어, 내부 위협, 물리적 공격 등 다양한 사이버 보안 위협에 취약하게 만든다. 특히, 전술적 마이크로그리드는 실시간 제어와 데이터 전송이 필수적이므로, 데이터의 기밀성, 무결성, 가용성이 보장되지 않으면 심각한 문제를 초래할 수 있다.

이에 전술적 마이크로그리드의 사이버 보안 위협을 체계적으로 분석하고, 이에 대한 해결책으로 프라이빗 블록체인을 기반으로 한 사이버 보안 관리 시스템을 제안한다. 군 특성에 맞게 프라이빗 블록체인은 높은 보안성을 제공하며, 합의 알고리즘과 분산 원장을 통해 데이터의 투명성을 유지하고, 암호화된 데이터 전송으로 외부로부터의 정보 유출을 효과적으로 차단한다. 또한, 스마트 계약을 통해 자동화된 보안 프로세스를 구축하고, ID 관리 및 접근 제어 기능을 통해 권한 부여와 관리가 체계적으로 이루어진다. 이러한 기술들은 전술적 마이크로그리드의 복잡한 데이터 관리와 보안 요구 사항을 충족시키며, 안전하고 효율적인 사이버 보안 환경을 구축하는 데 기여할 것이다.

본 연구는 2장 전술적 마이크로그리드에 관한 국내외 실태 분석, 3장 현재 국내·외 마이크로그리드 민간 및 군 적용 사례. 4장 국내·외 마이크로그리드 표준에 대한 확인 및 분석, 전술적 마이크로그리드 접목 방안 제시, 5장 전술적 마이크로그리드 프라이빗 블록체인 보안 체계 적용 및 운영 전략을 제시한다. 본 논문은 프라이빗 블록체인을 활용해 한국군 전술적 마이크로그리드의 보안을 강화하고, 안정적인 전력 공급과 통신 신뢰성을 확보하는 방안을 제시한다.

Ⅱ. 관련연구

한국에서는 아직 전술적 마이크로그리드 개념이 본격적으로 도입되지 않았지만, 마이크로그리드 자체에 대한 연구는 활발하게 진행되고 있다. “2050 육군 비전의 미래 전장을 뒤흔들 8대 게임체인저 8) 에너지 공급체계” 따르면, 한국 육군은 미래 전장 환경에 맞춘 지속 가능한 에너지 지원 체계를 마련하기 위해 다양한 연구를 추진 중이다[2]. 여기에는 전투원의 움직임을 통해 전력을 생산하는 에너지 하베스팅 기술, 무공해 전력 생산이 가능한 수소 연료전지, 그리고 극한 환경에서도 사용 가능한 원자력 전지 개발 등이 포함된다. 이들 기술은 전술적 환경에서 에너지 자립성을 높이고, 전투원이 장시간 작전을 지속할 수 있도록 지원하는 데 중점을 두고 있다. 또한, 프라이빗 블록체인 기술을 마이크로그리드에 적용하여 보안과 운영 효율성을 강화하려는 연구도 꾸준히 이루어지고 있다. 프라이빗 블록체인은 데이터 투명성과 보안성을 보장하는 동시에, 분산된 에너지 시스템에서 발생할 수 있는 사이버 보안 위협을 방지할 수 있는 기술이다. 이러한 기술을 적용하면 마이크로그리드 운영의 안정성과 효율성을 높일 수

있으며, 특히 한국은 “육군의 전·평시 안정적인 에너지 확보를 위한 마이크로그리드 적용방안 연구”, “블록체인 기술의 국방분야 적용사례와 시사점”, “마이크로그리드 보안 모델링 및 현장실증에 관한 연구”, “하이버레저 패브릭 기반 프라이빗 블록체인 성능 향상 : 자원 할동과 채널 구성을 중심으로” 등 여러 관련 논문과 연구 자료들이 이를 뒷받침하고 있다[3]-[6]. 한국이 전술적 마이크로그리드를 도입한다면, 이러한 프라이빗 블록체인 기술을 기반으로 전술적 운영의 안정성과 효율성을 극대화할 수 있을 것이다. 이 기술을 활용하면 실시간 데이터 관리 및 보안 체계가 강화되며, 전력 공급의 안정성을 보장하는 동시에 군사 작전의 성공 가능성을 높일 수 있다.

미군은 전술적 마이크로그리드를 실제로 운용하며, 이를 통해 전장에서의 에너지 공급과 통신망 회복력을 극대화하고 있다. “MIL-STD-3071”은 미군의 전술적 마이크로그리드 표준으로, 다양한 군사 작전 환경에서 신속하게 에너지를 배치하고 관리하기 위한 기준을 제시한다. 이 표준은 전술적 마이크로그리드 시스템의 설계, 운영, 유지보수에 필요한 요구사항을 정의하여 다양한 장비와 에너지 자원이 원활하게 통합되고 상호 운용될 수 있도록 돕는다. 이를 통해 신속한 설치와 철수, 에너지 효율성 향상, 그리고 표준화된 인터페이스 및 통신 프로토콜을 통한 장비 간 상호 운용성을 목표로 하여 군사 작전 중 에너지 공급의 안정성과 유연성을 극대화한다[7]. 그러나 전술적 마이크로그리드 보안 측면에서는 프라이빗 블록체인의 적용이 아직 연구 단계에 있으며, 미군은 블록체인의 높은 보안성과 투명성 덕분에 물류 및 데이터 관리에서 이 기술의 잠재력을 인식하고 있다. 블록체인 기술은 실시간 데이터 검증과 스마트 계약을 활용한 자동화된 물류 및 전력 관리의 장점을 제공하며, 이를 통해 민감한 군사 작전 데이터와 에너지 관리의 보안을 강화할 수 있는 가능성을 연구 중이다. 향후 미군은 이러한 기술을 전술적 마이크로그리드에 통합함으로써 에너지 관리뿐만 아니라 군사 작전의 데이터 보안을 더욱 강화할 가능성이 크다.

Ⅲ. 국내·외 마이크로 그리드 적용 및 사례

3-1 국내 마이크로그리드 적용 및 사례

국내 마이크로그리드의 민간 및 군 현황은 최근 몇 년간 큰 발전을 이루어왔다. 국내 전술적 마이크로 그리드는 주로 군사 기지와 국가 중요 시설에서 사용되며, 보안 측면에서 강력한 물리적 보안과 사이버 보안이 적용된다. 한국은 스마트 그리드 기술을 기반으로 하여 사이버 보안을 강화하고 있으며, 특히 전력망의 제어 시스템에 대한 외부 침입을 방지하기 위해 여러 계층의 보안 솔루션을 도입하고 있다. 이는 침입 탐지 시스템(IDS), 방화벽, 그리고 암호화 기술 등을 포함한다. 또한, 국내 전력망의 안정성을 유지하기 위해 정기적인 보안 점검과 모의 해킹 테스트를 실시하고 있으며, 이를 통해 잠재적인 보안 취약점을 사전에 발견하고 개선하고 있다.

1) 국내 민간 부문 마이크로그리드 적용 사례

민간 부문에서는 한국전력공사(KEPCO)가 다양한 산업 단지와 지역 사회에 마이크로그리드 시스템을 구축하여 신재생에너지와 지능형 전력망을 통합하는 노력을 기울이고 있다. 그림 1은 가시도의 독립형 MG 기술이 적용되기 전후의 개념도를 보여준다. 가시도는 제주도의 작은 섬으로, 전통적으로 외부 전력망에 의존해왔다. 하지만 이 프로젝트를 통해 가시도는 재생에너지와 에너지 저장 시스템(ESS)을 활용한 독립형 마이크로그리드를 구축했다. 이러한 시스템은 에너지 효율성을 높이고, 분산 자원의 효율적인 이용을 통해 전력 공급의 안정성을 강화했다.

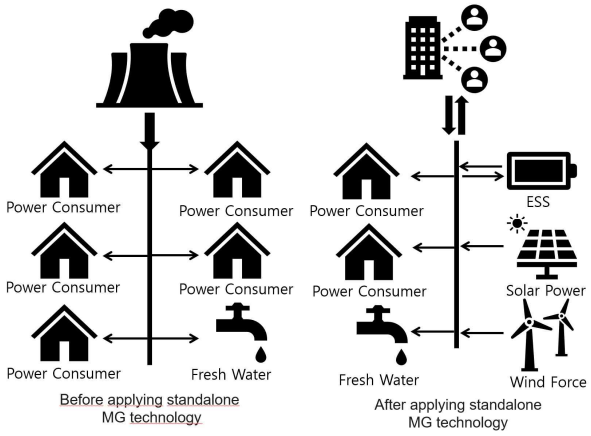

그림 1. 가시도 독립형 MG 개발내용 및 개념도[8]
Fig. 1. Visibility independent MG development details and concept diagram

2) 국내 군 부문 마이크로그리드 적용 사례

군 부문에서는 “육군 비전 2050”을 통해 에너지 공급 체계를 혁신하고 있다. “육군 비전 2050: 미래 전장을 뒤흔들 8대 게임체인저” 중 에너지 공급체계는 미래의 신개념 무기체계를 효과적으로 운용하고 변화무쌍한 작전 환경에 신속히 대응하기 위해 후속 군수지원 없이 지속적으로 단독작전을 수행할 능력을 갖추는 것이 매우 중요한 요소라고 강조하고 있다[2]. 대체 에너지원 확보는 미래 전쟁의 승패를 결정할 정도로 핵심적인 사안으로 언급했다. 그림 2는 2016년 2월 24일 한국전력공사와 공군이 협력을 통해 ‘공군 지능형전력망 구축사업’ 수행을 위한 합의서를 체결했다. 이 프로젝트는 2024년까지 총 3단계로 순차적으로 시행되며, 모든 비행장에 마이크로그리드를 구축하여 비상시에 독립적이고 안전한 전력을 공급할 수 있는 시스템을 구축하는 것을 목표로 하고 있다. 이를 통해 공군의 비상 상황 대응 능력을 크게 향상시킬 뿐만 아니라, 안정적인 전력 공급을 통해 공군 작전의 연속성을 보장할 수 있다.

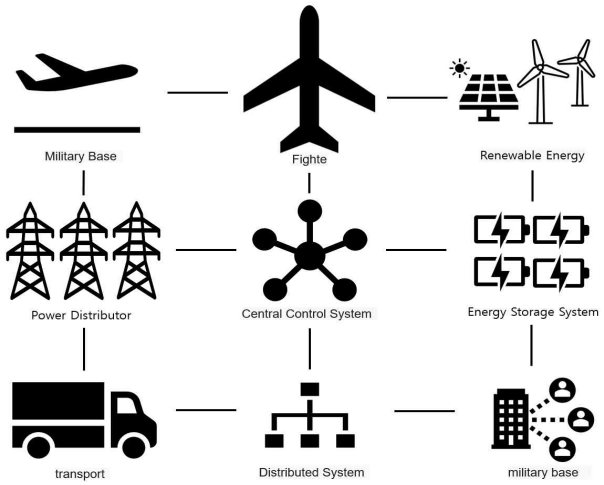

그림 2. 한전 공군 마이크로그리드, 지능형전력망 구축 사업[9]
Fig. 2. KEPCO Air Force microgrid, intelligent power grid construction project[9]

3-2 국외 마이크로그리드 적용 및 사례

여러 나라에서 다양한 환경에서 마이크로 그리드 기술을 도입하여 에너지 효율성과 안정성을 높이고 있다.

1) 일본 마이크로그리드 적용 사례

일본은 지진과 같은 자연재해에 대응하기 위해 마이크로그리드 시스템을 적극적으로 도입하고 있다. 일본의 마이크로그리드 프로젝트는 재생 에너지원과 에너지 저장 시스템을 통합하여, 비상 상황에서도 독립적으로 전력을 공급할 수 있는 시스템을 구축하는 데 중점을 두고 있다. 예를 들어, 후쿠시마 원전 사고 이후 일본은 후쿠시마 지역에 마이크로그리드 시스템을 설치하여 재생 에너지와 연계된 에너지 자립도를 높이고 있다[10].

2) 유럽 마이크로그리드 적용 사례

유럽은 재생 가능 에너지원의 증가와 함께 전력망의 안정성을 높이기 위해 마이크로그리드 시스템을 적극적으로 도입하고 있다. 그림 3은 유럽 내 마이크로그리드와 관련된 TYNDP(Trans-European Network for Energy) 프로젝트를 시각화한 지도이다. 마이크로그리드 시스템은 소규모 지역 또는 커뮤니티 단위에서 독립적으로 운영되는 전력망으로, 분산형 에너지 자원을 활용해 지역 내 전력 수요를 충족시킨다. 이러한 시스템은 특히 환경 개선과 에너지 효율성 향상, 그리고 전력 공급의 신뢰성을 높이는 데 중요한 역할을 한다. 유럽은 프로젝트를 통해 에너지 통합과 재생 가능 에너지의 최적화를 하고 있다.

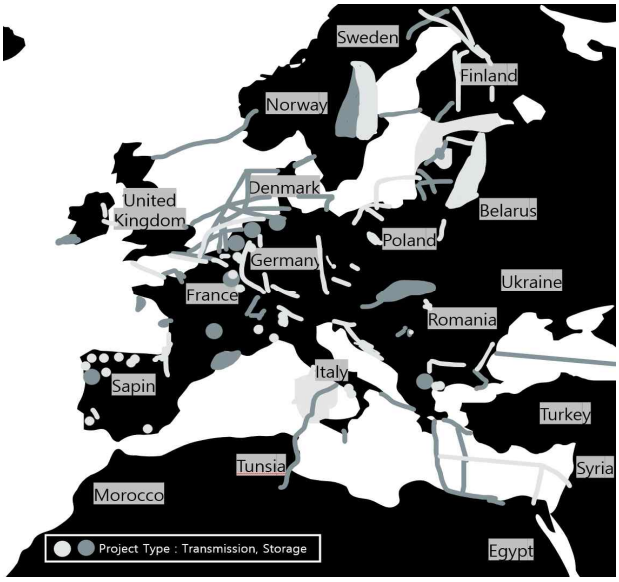

그림 3. 유럽(TYNDP) 프로젝트 지도[11]
Fig. 3. Map of the TYNDP projects[11]

3) 미국 마이크로그리드 적용 사례

미국에서는 마이크로그리드가 다양한 분야에서 광범위하게 적용되고 있으며, 각각의 목적에 맞춰 설계되어 다양한 방식으로 운영되고 있다. 이는 전력망의 안정성 향상, 재생에너지 통합, 에너지 비용 절감, 비상 상황 대응 등 여러 목표를 달성하기 위한 수단으로 활용되고 있다. 그림 4는 미국 내 다양한 마이크로그리드 활동의 분포를 보여주는 지도이다. 마이크로그리드 활동 포트폴리오는 여러 유형의 프로젝트들을 구분하고 있으며, 분야별로 적용된 다양한 사례들을 통해 마이크로그리드의 높은 유연성과 잠재력을 확인할 수 있다.

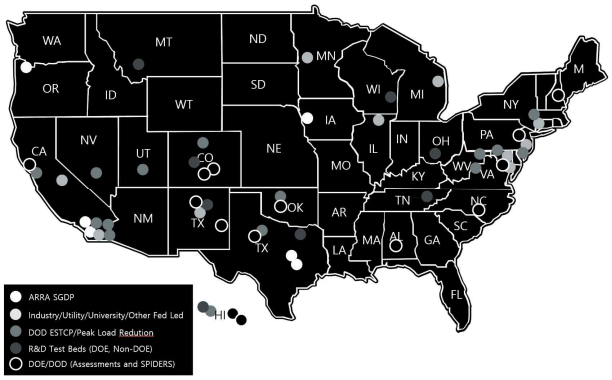

그림 4. 미국 마이크로그리드 활동 포트폴리오[12]
Fig. 4. U.S. microgrid portfolio of activities[12]

표 1 마크로그리드 분야별 적용 사례로 국방부(DoD)의 연구개발 시험대와 같은 프로젝트는 군사 기지의 독립적인 에너지 공급을 위해 활용되며, 재생에너지를 적극적으로 도입하여 에너지 자립을 목표로 하고 있다. 또한, DOE(에너지부)와

DOD의 계약 기반 프로젝트는 주거 및 상업용 구역에서 에너지 관리의 효율성을 높이는 데 중점을 두고 있다. 이 외에도 산업, 연구 기관, 대학 등 다양한 부문에서도 마이크로그리드를 적용하여 에너지 효율성과 재생 가능성에 대한 실험 및 연구가 활발히 이루어지고 있다. 이러한 프로젝트들은 마이크로그리드가 단순한 전력 공급 이상의 기능을 하며, 국가 전체의 에너지 시스템 혁신에 기여할 수 있는 중요한 기술임을 보여준다.

표 1. 미국 마이크로그리드 분야별 적용 사례[13]-[16]
Table 1. Brief examples of U.S. microgrid sectors[13]-[16]

Application field	Application example	Key Features
Military and tactical applications	Fort Bragg Military Base	Strengthens energy independence, reduces dependency on external power grids, protects against cyber/physical attack
Strengthening disaster response and resilience	Hampton Bays, New York, Sonoma County, California	Stable power supply in disaster situations and strengthening local power resilience
Energy Efficiency and Sustainability	Kodiak Island, Alaska	Maximizing the use of renewable energy, energy independence and environmentally friendly system
Educational and research institutions	University of California, San Diego	Make campus power independent, provide research and education opportunities, and develop new energy management technologies
Civil and commercial applications	Brooklyn Microgrid	Promote distributed power production and consumption, manage transparent and safe energy transactions based on blockchain

특히 미국의 전술적 마이크로 그리드는 사이버 보안 위협에 대한 대비가 중요한 요소로 강조된다. 미국은 군사 시설의 마이크로 그리드를 EMP(전자기 펄스) 공격 및 사이버 공격으로부터 보호하기 위해 고급 보안 프로토콜을 사용하고 있다. 예를 들어, 군사 기지에서의 전술적 마이크로 그리드는 독립적으로 운영될 수 있는 '섬형' 전력 시스템으로 설계되어 있어 외부 네트워크와의 연결을 차단함으로써 공격을 방지한다. 또한, 핵심 전력 인프라에 대해 지하에 설치된 전력 라인과 보호된 데이터 센터를 활용하여 물리적 및 디지털 보안을 강화하고 있다.

표 2는 국내와 국외 모두 전술적 마이크로 그리드의 보안은 중요한 요소로, 각각의 환경에 맞춰 다양한 보안 기술과 프로토콜을 적용하고 있다. 한국은 스마트 그리드 기술을 활용한 사이버 보안 강화에 중점을 두고 있으며, 미국은 독립적인 운영을 통한 물리적 및 디지털 보안을 동시에 강화하고 있다.

표 2. 국내·외 전술적 마이크로그리드 보안 비교 분석[17]-[19]
Table 2. Comparative analysis of domestic and foreign tactical microgrid security[17]-[19]

division	Korea Tactical Microgrid	U.S. Tactical Microgrid
cyber security	through smart grid technology Apply multi-layered security	External attacks through independent operation Block and use advanced security protocols
physical security	Focusing on national important facilities Enhanced Physical Securit	Utilize underground power lines and secure data centers
Prepare for major threats	To prevent external intrusion and hacking Regular security checks	Prepare for various threats such as EMP attacks and cyber attacks
Security checks and improvements	Regular security checks and mock hacking Improve through testing	Advanced monitoring system Real-time security inspection and response through

Ⅳ. 국내·외 마이크로그리드 보안 표준

4-1 국내 마이크로그리드 보안 표준

국내에서 마이크로그리드의 사이버 보안을 강화하기 위한 여러 연구와 표준이 제정되고 있다. 마이크로그리드는 신재생에너지와 분산전원을 포함한 지역적 에너지 공급체계로서, 다양한 정보통신기술이 결합되어 있어 사이버 보안의 중요성이 높다.

국내 마이크로그리드 사이버 보안 프레임워크 및 표준은 스마트그리드 보안과 밀접하게 연계되어 발전하고 있다. 한국정보통신기술협회(TTA)를 중심으로 다양한 보안 요구 사항과 시스템 보안 기능 요구 사항이 제정되었다. 예를 들어, TTAK.KO-12.0182는 스마트그리드 보안 요구 사항을, TTAK.KO-12.0209는 스마트그리드 시스템 보안 기능 요구 사항을 다루고 있다. 이 표준들은 마이크로그리드와 스마트그리드 환경에서 발생할 수 있는 다양한 보안 위협을 효과적으로 대응할 수 있도록 설계되었다[20],[21].

제주 스마트그리드 실증단지에서는 그림 5 Korea Micro Energy Grid (K-MEG) 프로젝트를 통해 실증 사이트 구축과 함께 보안 대책을 수립하고 있다. 이 프로젝트에서는 실증단지 구축 기관들이 준수해야 할 보안 지침과 가이드라인을 개발하여 배포하고, 이러한 지침의 준수 여부를 점검하는 활동을 수행한다. 이러한 노력은 국내 마이크로그리드의 사이버 보안을 강화하고, 보다 안전한 에너지 관리 시스템을 구축하는 데 기여하고 있다.

이와 같은 연구와 표준화 작업을 통해 국내 마이크로그리드 사이버 보안 프레임워크는 지속적으로 발전하고 있으며, 이는 신재생에너지와 분산전원을 포함한 지역적 에너지 공급체계의 안전성과 효율성을 높이는 데 중요한 역할을 하고 있

다. 다만, 각 분야별 구분하여 표준화 작업을 함께 추진할 필요성이 있으며, 특히 향후 사이버 보안에서 블록체인 기술을 도입하는 데 있어 이러한 표준화 작업을 병행하는 것이 중요하다. 이는 마이크로그리드 시스템의 보안성과 신뢰성을 더욱 강화하는 데 기여된다.

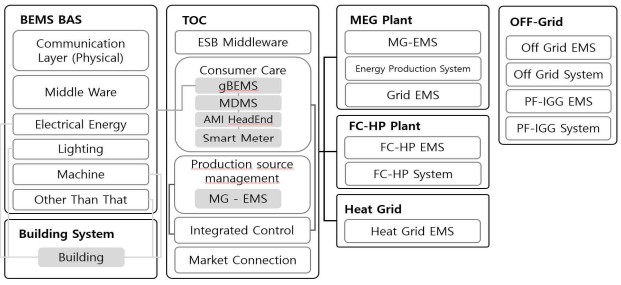

그림 5. K-MEG 시스템 구성도[22]
Fig. 5. K-MEG system configuration diagram[22]

4-2 국외 마이크로그리드 보안 표준

국제적으로, 마이크로그리드의 사이버 보안을 강화하기 위해 다양한 표준과 프레임워크가 마련되고 있다. 대표적으로 IEEE 1547 및 IEEE 2030 시리즈가 있다. IEEE 1547.4는 마이크로그리드 상호연결을 다루고, IEEE 2030 시리즈는 스마트 그리드의 상호운용성을 다루며, 마이크로그리드 제어 및 테스트에 대한 구체적인 지침을 제공한다. 이러한 표준들은 에너지 시스템의 안정성과 보안을 높이는 데 중요한 역할을 하고 있다[23].

미국에서는 국립표준기술연구소(NIST)와 에너지부(DOE)가 마이크로그리드 사이버 보안 표준을 주도하고 있다. 특히, “NREL”(National Renewable Energy Laboratory)은 IEEE 표준 개발에 있어 기술적 리더십을 제공하며, 다양한 마이크로그리드 제어기와 보안 메커니즘을 검증하는 작업을 수행하고 있다. 그림 6 NIST Cybersecurity Framework는 식별, 보호, 탐지, 대응, 복구의 5가지 기능을 통해 조직의 사이버 보안 리스크를 관리하는 데 도움을 준다. NREL의 사이버 에너지 에뮬레이션 플랫폼은 실제 데이터 교환을 통제된 환경에서 테스트하여 사이버 위협을 사전에 발견하고 방지하는 데 중요한 역할을 한다.

미군은 마이크로그리드 보안을 위해 독자적인 표준을 개발하고 있다. 미군의 마이크로그리드는 전술적 운영을 위해 설계되었으며, 높은 보안 요구 사항을 충족해야 한다. 이를 위해 AI 기반 보안 솔루션, 실시간 모니터링 시스템, 그리고 강화된 암호화 프로토콜을 사용하고 있다. 이러한 시스템은 전술적 상황에서도 신뢰할 수 있는 에너지 공급을 보장하는 데 중점을 둔다.

이와 같은 국제적 노력들은 마이크로그리드의 보안을 강화하고, 전 세계적으로 통일된 보안 기준을 마련하여 사이버 위협에 대응하는 데 중요한 역할을 하고 있다. 국내에서도 미군의 독자적인 표준 개발 및 국제적 마이크로 그리드 보안 표준을 참고하여, 국내 마이크로그리드 환경에 맞춘 보안 표준을 정립하면 보다 안전하고 완벽한 시스템이 구축된다.

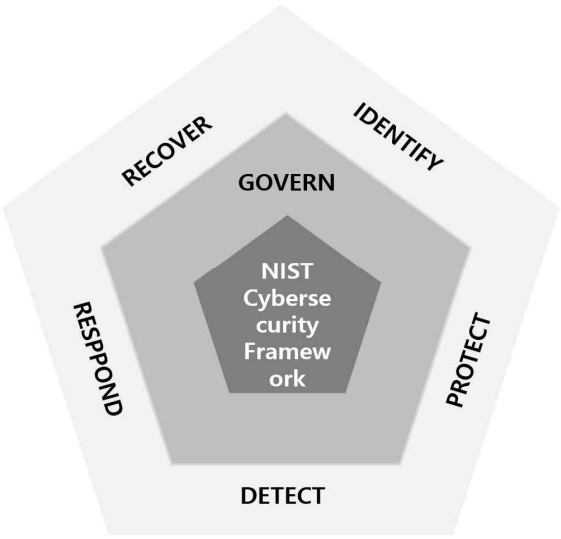

그림 6. CSF 기능[24]
Fig. 6. CSF functions[24]

V. 프라이빗 블록체인 보안 체계 적용 및 운영 전략

5-1 전술적마이크로 그리드 활용 간 보안문제

전술적 마이크로그리드는 중앙 집중식 전력망과 달리 분산된 에너지 관리 시스템과 다수의 통신 네트워크를 기반으로 운영되기 때문에 다양한 보안 위협에 직면할 수 있다[25]. 먼저, 통신 네트워크의 보안 취약점으로 인해 중간자 공격(Man-in-the-Middle Attack, MITM), 신호 방해(Jamming), DDoS(Distributed Denial of Service) 공격과 같은 위협이 발생할 수 있다. 특히, 공격자가 네트워크 패킷을 변조하거나 특정 노드와의 연결을 차단할 경우, 전력 수요 예측 오류가 발생하거나 실시간 전력 관리 기능이 마비될 위험이 있다. 또한, 데이터 무결성(Integrity)과 인증(Authentication) 문제도 주요 보안 위협 중 하나로, 스푸핑(Spoofing) 공격을 통해 가짜 노드가 잘못된 데이터를 송출하거나, 공격자가 데이터베이스를 조작하여 배터리 충전 상태 및 에너지 흐름을 왜곡할 가능성이 존재한다. 이와 함께, 비인가 접근(Unauthorized Access) 및 내부자의 악의적인 행위로 인해 마이크로그리드의 운영이 중단되거나 악용될 수도 있으며, 물리적 보안 위협으로 인해 개별 노드의 손상이나 변조가 발생하면 시스템 전체의 신뢰성이 저하될 수 있다.

이러한 보안 문제를 해결하기 위해 블록체인 기술을 활용하는 것이 효과적인 대안이 될 수 있으며, 특히 프라이빗 블록체인(Private Blockchain)의 도입이 적절한 선택이 될 수

있다. 블록체인은 데이터의 무결성을 보장하며, 모든 트랜잭션을 암호화된 블록으로 저장하여 위변조를 방지할 수 있다. 또한, 스마트 컨트랙트(Smart Contract)를 활용하여 접근 제어 및 인증 절차를 자동화함으로써, 비인가 사용자의 침입을 차단하고, 에너지 관리 및 거래를 신뢰할 수 있는 방식으로 운영할 수 있다. 블록체인의 분산 원장(Distributed Ledger) 구조는 DDoS 공격을 방어하는 데에도 유리하며, 특정 노드가 공격받더라도 나머지 네트워크는 정상적으로 운영될 수 있다. 그러나 공공 블록체인(Public Blockchain)의 경우 처리 속도가 느리고 모든 사용자가 참여할 수 있기 때문에 군사 작전이나 전술적 마이크로그리드와 같은 보안이 중요한 환경에는 적합하지 않다. 반면, 프라이빗 블록체인은 특정 기관이나 조직이 네트워크를 관리하며, 허가된 사용자만 접근할 수 있어 보안성과 운영 효율성이 뛰어나다[26]. 이를 통해 전력망 내 데이터 흐름을 철저하게 통제할 수 있으며, 비인가 노드의 접근을 원천 차단할 수 있다. 또한, 스마트 컨트랙트를 활용하여 운영 프로세스를 자동화하고, 에너지 거래와 인증 절차를 더욱 안전하게 수행할 수 있다. 따라서 전술적 마이크로그리드의 보안 문제를 해결하기 위해서는 개방된 퍼블릭 블록체인이 아닌, 높은 보안성과 신뢰성을 제공하는 프라이빗 블록체인을 적용하는 것이 가장 적절한 해결책이 될 것이다.

5-2 군 조직 체계와 블록체인의 연동 개념

군부대의 계층적 구조를 프라이빗 블록체인 네트워크 내에서 적절히 구성하면, 보안 관리와 책임 부담을 체계적으로 할 수 있다. 각 계층은 블록체인 네트워크에서 고유의 역할을 가지며, 표 3은 군 조직체계와 블록체인의 연동성 방식을 나타낸 표이다. 군 조직은 계층적이고 명확한 명령 체계가 존재하며, 신속하고 안전한 정보 전달이 필수적이다. 프라이빗 블록체인을 도입하여 이러한 정보 흐름을 탈중앙화하고 투명성을 높이며, 통신 보안을 강화할 수 있다.

국방부는 최상위 권한을 가지고 전체 네트워크에 접근하며, 정책을 수립하고 변경할 수 있다. 블록체인 기술을 도입하면 국방부는 중앙에서 블록체인 네트워크의 노드로 작용할 수 있으며, 모든 정책 및 지시사항이 블록체인에 기록되면서 투명성과 무결성을 보장할 수 있다. 이를 통해 모든 군 조직은 국방부의 지시사항을 신뢰할 수 있게 되며, 정책 변경 사항은 실시간으로 기록되어 추적 가능하다.

육군 본부는 국방부의 지휘를 받아 중간 권한을 행사하며, 블록체인을 통해 보안 조치를 감시하고 정책을 적용할 수 있다. 이때 블록체인에 기록된 보안 조치는 수정할 수 없으므로, 육군 본부가 시행한 모든 보안 조치와 정책 적용은 완전한 투명성을 확보할 수 있다. 또한 각 지역에서 발생한 사건을 빠르게 분석하고 대응하기 위해 블록체인에 기록된 데이터를 신속하게 확인할 수 있다.

군단은 지역 내 전술적 마이크로그리드 운영과 보안을 관리한다. 블록체인을 활용해 군단은 각 지역의 전력망 및 통신망 데이터를 실시간으로 기록 및 감시할 수 있으며, 해당 데이터는 신뢰성이 보장된다. 지역 내에서 발생한 보안 위협이나 공격 시도는 블록체인 네트워크를 통해 즉시 상위 계층으로 전송되고 기록되어, 신속한 대응이 가능하다.

표 3. 군 조직 체계와 블록체인의 연동성[27]
Table 3. Interconnection between military organizational system and blockchain[27]

organ	role	Scope of authority
Ministry of Defense	Establishment of security policy and top management	Top privileges – full access and policy changes
army headquarters	Supervision of corps/division security management	Middle authority – enforce security measures, enforce policies
corps	Operations and security management within the region	Local authority – situation monitoring and respons
Division / brigade	On-site power grid and communication network management	Field Operations Authority – Operations and Reporting
battalion/ company	Field data collection and reporting	Data Collection Rights – Data Reporting

사단/여단은 현장에서 직접 전력망과 통신망을 관리한다. 블록체인은 이들이 수집하는 데이터를 실시간으로 기록하며, 상위 계층에서 해당 데이터를 확인할 수 있게 해준다. 현장에서 수집된 모든 데이터는 조작할 수 없기 때문에 데이터의 신뢰성이 높아진다. 블록체인을 통한 데이터 기록은 또한 상위 계층에서 현장 상황을 빠르게 파악하고 필요한 조치를 내릴 수 있게 해준다.

대대/중대/소대는 최전선에서 실시간으로 데이터를 수집하여 상위 계층에 보고한다. 이때 수집된 데이터는 블록체인에 기록됨으로써 중간에 변조되지 않으며, 상위 계층에 전달될 때도 안전하게 전송된다. 블록체인은 데이터의 투명성과 무결성을 보장해 현장에서 일어나는 모든 활동이 신뢰성 있게 관리되도록 한다.

이러한 군 조직 내에서 블록체인을 도입하는 것은 보안성을 강화하고 정보의 투명성을 유지하며, 실시간으로 상위 계층과 하위 계층 간의 데이터 교환이 원활하게 이루어지도록 하는 데 도움을 준다. 블록체인은 정보의 변경 불가성과 투명성 덕분에 각 계층이 신뢰할 수 있는 데이터 기반 의사결정을 내릴 수 있게 하며, 군 전체의 보안 관리 체계를 더 강력하게 만드는 데 기여할 수 있다.

5-3 프라이빗 블록체인을 통한 통신 보안 강화

전술적 마이크로그리드는 프라이빗 블록체인을 기반으로 한다. 표 4는 프라이빗 블록체인의 보안요소로, 분산 원장과 암호화를 통해 통신 데이터의 무결성을 보장하고, 사이버 공격으로부터 보호할 수 있다. 이를 통해 민감한 군사 정보와

전력 관리 데이터를 안전하게 관리하며, 스마트 계약과 ID 관리를 통해 무단 접근을 방지하고 실시간 데이터 전송의 보안을 강화할 수 있다.

표 4. 프라이빗 블록체인 보안요소[28],[29]
Table 4. Private blockchain security element[28],[29]

security element	explanation
consensus algorithm	Data integrity guaranteed and node verification with PoA and PBFT
distributed ledger	Data transparency, prevention of forgery and alteration, and network maintenance
encryption	Protecting military information with encrypted transmission, using hash functions
smart contract	Automatic energy distribution and communication, rapid decision-making
Identity management and access control	ID management for each user, prevention of unauthorized access, multi-authentication

합의 알고리즘 : PoA (Proof of Authority) 또는 PBFT (Practical Byzantine Fault Tolerance) 같은 합의 알고리즘을 사용하여 데이터의 무결성을 보장하고, 네트워크 내에서 신뢰할 수 있는 노드가 데이터를 검증하게 설정한다. 특히, 전술적 환경에서는 실시간 데이터 처리가 중요하기 때문에 빠르고 안정적인 합의 알고리즘이 필요하다.

분장 원장 : 분산 원장을 사용해 군 조직 내의 전력 데이터 및 통신 내용을 투명하고 안전하게 기록한다. 각 블록은 이전 블록과 연결되어 있어 데이터 위변조가 어렵다. 분산 원장 통해 중앙 서버에 대한 의존 없이 각 노드가 독립적으로 데이터를 관리하므로, 전력망의 특정 지점이 손상되더라도 전체 네트워크는 계속해서 정상적으로 작동할 수 있다. 이러한 특성은 전술적 마이크로그리드의 보안성을 크게 높인다.

암호화: 암호화된 데이터 전송을 통해 민감한 군사 정보나 전력 관리 데이터가 외부로 유출되는 것을 방지하며, 네트워크 참여자만이 정보를 접근할 수 있다. 블록체인에 기록되는 모든 데이터는 암호화되어 저장되므로, 통신 중간에 데이터가 탈취되더라도 해독할 수 없다. 특히, 비대칭 암호화는 공개키와 개인키를 사용해 안전한 데이터 전송을 보장하며, 해시 함수는 데이터의 무결성을 확인하는 데 필수적이다. 해시 함수는 입력 데이터에서 고정된 크기의 출력값을 생성하여 데이터가 변조되지 않았음을 보증한다. 또한, 디지털 서명을 통해 송신자의 신원을 인증하고, 데이터 위변조를 방지할 수 있다. 디지털 서명은 송신자의 개인키로 생성되고, 수신자는 공개키를 통해 이를 검증하여 데이터의 진위 여부를 확인할 수 있다. 이러한 암호화 기술과 해시 함수, 디지털 서명은 군사 통신 보안을 강화하는 필수적인 요소이다.

스마트 계약 : 특정 조건 하에 자동으로 에너지 분배나 통신을 수행할 수 있으며, 이를 통해 즉각적이고 신속한 의사결정을 지원한다. 스마트 계약을 사용하여 군사적인 명령이나 전력 분배 시 특정 조건이 충족될 때 자동으로 실행되는 시스템을 구축할 수 있다. 이를 통해 명령의 지연 없이 즉각적인 대응을 가능하게 하고, 특정 상황에 따라 자동화된 통신 프로토콜을 설정할 수 있다.

ID 관리 및 접근 제어(Identity Management and Access Control) : 군 조직 내 노드 및 사용자별 ID 관리와 접근 제어 시스템을 프라이빗 블록체인으로 구현하여, 기밀 데이터를 관리하고 적합한 권한을 부여할 수 있다. 이를 통해 무단 접근이나 데이터 유출을 방지하고, 통신의 신뢰성을 높일 수 있다. 다중 인증 시스템(Multi-Factor Authentication)도 이러한 보안 체계를 강화하는 데 도움이 된다.

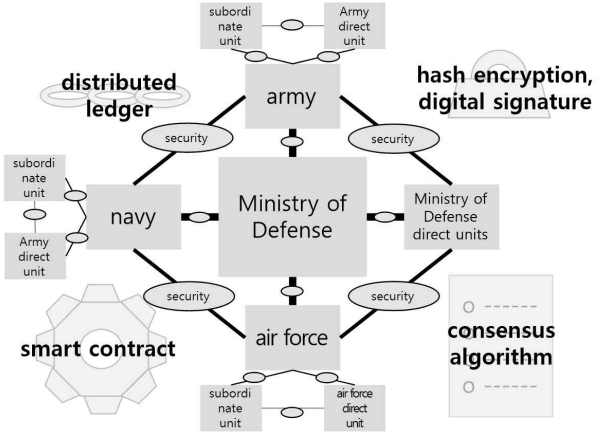

그림 7. 군 계층별 프라이빗 블록체인 연동 및 보안요소[30],[31]
Fig. 7. Private blockchain linkage and security elements by military hierarchy[30],[31]

그림 7은 군 계층별 프라이빗 블록체인 연동과 보안요소를 표현한 것으로 프라이빗 블록체인을 활용하여 상위 계층으로부터 최상위 권한을 보유한 상태에서 각 계층별로 세분화된 보안 관리가 가능하다. 이를 통해 보다 정밀하고 체계적인 보안 관리를 실현할 수 있다. 또한 블록체인의 핵심 보안 요소인 합의 알고리즘, 분산 원장, 암호화, 스마트 계약, ID 관리 및 접근 제어 기능을 통합하여 안전하고 신뢰성 높은 보안 환경을 유지할 수 있다.

5-4 분산 에너지 자원(DER) 및 가상 발전(VPP)에 대한 블록체인 기반 VPP(BVPP)구현 방안

전술적 마이크로그리드의 주요 구성 요소 중 하나는 분산 에너지 자원(DER, Distributed Energy Resources) 및 가상 발전소(VPP, Virtual Power Plant)이다. DER은 태양광, 풍력, 연료전지, 배터리 저장 시스템(BESS) 등 다양한 형태의 분산

형 전력 생산 및 저장 장치를 포함하며, VPP는 이러한 DER을 하나의 통합된 시스템으로 운영하여 최적의 전력 공급을 가능하게 한다. 그러나 기존 VPP는 중앙 집중식 시스템을 통해 운영되기 때문에 데이터 조작, 보안 취약점, 단일 장애점(Single Point of Failure)과 같은 문제가 발생할 수 있다. 이를 해결하기 위해 블록체인 기반 VPP(BVPP, Blockchain-based Virtual Power Plant)를 구축하면 탈중앙화된 에너지 관리, 보안 강화, 데이터 무결성 보장 및 스마트 계약 기반의 자동화된 운영이 가능하다.

1) BVPP의 핵심 구성 요소 및 필요 기술

BVPP는 기존 VPP의 중앙 집중식 운영 방식을 블록체인 기반으로 전환하여 운영된다. 표 5는 BVPP의 핵심 구성요소이며 이를 통해 VPP의 보안 취약점을 보완한다. 블록체인은 DER 데이터를 안전하게 관리하며, 스마트 컨트랙트는 에너지 거래와 운영을 자동화하여 비용을 절감한다. 또한, 분산 원장은 DDoS 및 사이버 공격을 방어하며, ID 기반 인증을 통해 비인가 접근을 차단하여 시스템의 신뢰성을 높인다.

표 5. BVPP의 핵심 구성요소[32],[33]
Table 5. Private blockchain security element[32],[33]

component	explanation
Private blockchain-based energy data	DER production and consumption data is recorded on the blockchain to ensure integrity
Smart contract-based automation	Automate energy trading and DER operations and reduce transaction costs
Distributed ledger-based security	Application of distributed ledger to prevent DDoS and cyber attacks
Identity-based encryption and authentication	Access control to ensure that only authorized users access the network

2) BVPP운영 모델 및 단계별 적용 방안

BVPP 운영 모델은 DER 등록 및 인증, 블록체인 원장에 데이터 기록, 스마트 컨트랙트 기반 에너지 거래, AI 기반 부하 관리의 네 가지 주요 단계로 구성된다[34]. 먼저, DID(분산 식별자)를 활용하여 DER(분산 에너지 자원)을 등록하고, 허가된 장치만 블록체인 네트워크에 접근할 수 있도록 인증하여 보안성을 강화한다. 이후, 각 DER의 전력 생산 및 소비 데이터는 블록체인 원장에 기록되어 데이터 무결성을 보장하며, 조작 가능성을 원천 차단한다. 스마트 컨트랙트는 P2P 에너지 거래를 자동화하고, 수요와 공급에 맞춰 실시간으로 가격을 책정하여 운영의 효율성을 극대화한다. 또한, AI 및 머신러닝을 적용한 부하 관리 시스템을 통해 전력 수요를 예측하고, 배터리 충·방전 및 부하 분배를 최적화하여 에너지 활용도를 높인다. 이를 통해 BVPP는 기존 VPP의 한계를 극복하고, 보다 자율적이고 안전한 분산형 에너지 관리 시스템을 구축할 수 있다.

2) BVPP 적용 시 기대 효과

BVPP(Blockchain-based Virtual Power Plant)를 적용함으로써 전력 관리와 거래의 신뢰성을 높이고, 보안성과 운영 효율성을 극대화할 수 있다. 블록체인을 활용하여 DER(Distributed Energy Resources)의 에너지 데이터를 분산 원장에 저장함으로써 데이터 무결성(Data Integrity) 및 보안(Security)이 강화되며, 스마트 컨트랙트를 통해 에너지 거래 및 부하 관리가 자동화됨으로써 운영 비용 절감 및 거래 투명성 확보가 가능하다. 또한, DDoS 및 해킹과 같은 사이버 공격에 대한 저항성을 증가시켜, 기존의 중앙 집중식 VPP의 보안 취약점을 보완할 수 있다. 더 나아가, BVPP는 신재생 에너지 활용을 극대화하여 탄소 배출 저감(Carbon Footprint Reduction)에 기여하고, P2P 에너지 거래 시스템을 통해 소비자가 직접 에너지 시장에 참여할 수 있도록 함으로써 에너지 시장의 탈중앙화 및 효율적 자원 분배를 촉진할 수 있다. 특히, 프라이빗 블록체인(Private Blockchain)을 적용하면 보안성과 성능을 최적화할 수 있으며, 제한된 허가된 사용자만이 네트워크에 접근할 수 있어 신뢰성과 확장성이 높은 에너지 관리 시스템을 구축할 수 있다. 이를 통해 BVPP는 전력망의 안정성과 보안성을 동시에 강화하는 혁신적인 솔루션이 될 수 있다.

5-5 전술적 마이크로그리드와 프라이빗 블록체인 연동 운용방식

프라이빗 블록체인 기반 전술적 마이크로그리드 보안 관리에서 통합관리가 아닌 계층적 관리로 인한 제한사항이 있다. 이를 효율적이면서도 유연한 접근을 제공하기 위해 프라이빗 블록체인 기술을 사용간 관체계를 일상적인 상황과 전시 상황 모두에서 보안 격차를 줄이고 효과적인 관리를 할 수 있다.

가. 일상적인 관리 체계: 국방부가 보안을 총괄하며, 각 계층(육군본부, 군단, 사단 등)이 블록체인 기반으로 데이터를 독립적으로 관리하고 보안 절차를 수행한다. 모든 계층은 블록체인 노드 역할을 하며, 역할 기반 접근 제어(RBAC)를 통해 권한을 부여받고, 모든 기록을 변경 불가능한 형태로 저장하여 위변조를 방지한다. 이를 통해 중앙 집중식 관리의 단점을 보완하면서도, 각 부대가 효율적으로 운영될 수 있도록 한다.

나. 정기적인 통합 점검: 국방부와 각 계층이 블록체인 원장과 AI 기반 이상 탐지 시스템을 활용하여 네트워크와 전력 시스템을 주기적으로 점검한다. 스마트 컨트랙트를 통해 네트워크 상태를 자동 모니터링하고, 보안 격차를 실시간으로 분석하여 조치할 수 있다. 점검 후 보안 정책과 시스템 업데이트가 블록체인을 통해 실시간 반영되며, 기록이 남아 향후 감사 및 보완 작업이 용이해진다.

다. 전시 상황에서의 실시간 권한 동기화: 국방부가 모든 계층에 즉각적인 데이터 접근 권한을 부여하여 신속한

정보 공유와 대응이 가능하도록 한다. 스마트 컨트랙트를 활용해 특정 상황이 발생하면 자동으로 권한이 조정되며, 지휘부가 전력 및 통신 자원을 통합 운영할 수 있도록 한다. 이를 통해 명령 체계의 효율성을 유지하고, 네트워크 동기화로 긴급 상황에서도 안정적인 운영을 보장한다.

라. 비정상적인 활동 감지 시스템: AI와 블록체인을 활용하여 실시간으로 네트워크 이상 징후를 감지하고 자동 대응 프로토콜을 실행한다. 데이터 조작, 무단 접근 시도가 탐지되면 스마트 컨트랙트가 즉각 조치를 취하고, 상위 기관에 경고를 전송하여 신속한 대응이 가능하도록 한다. 블록체인 원장에 기록된 로그는 보안 분석에 활용되며, 반복적인 공격 패턴을 학습하여 향후 보안 수준을 더욱 강화한다.

마. 프라이빗 블록체인 기반 에너지 거래 및 배분: 분산 에너지 자원의 효율적 운영이 가능해진다. DER(분산 에너지 자원)의 생산 및 저장 데이터를 블록체인에 기록하고, 스마트 컨트랙트를 통해 실시간 전력 수요에 맞춰 자동 조정함으로써 군사 작전 중 전력 균형을 유지하고 낭비를 줄인다.

바. 비상 상황에서는 에너지 우선 공급 체계를 활용: 블록체인이 자동으로 전력 분배를 최적화하고, 군사 작전에 필수적인 시설(지휘소, 방공 시스템 등)에 전력을 우선적으로 공급한다. 전력망 손상 시 즉각적인 경로 조정이 이루어지며, 안정적인 전력 공급이 보장된다.

사. 물리적 보안과 연계된 블록체인 기반 접근 제어 시스템: 주요 군사 시설의 출입 기록을 변경 불가능한 블록체인 원장에 저장하고, 허가된 인원만 접근할 수 있도록 한다. 비인가 인원의 접근 시 즉각적인 경고가 발송되며, 필요 시 특정 구역의 전력 공급을 차단하는 기능도 설정할 수 있다. 이를 통해 전술적 마이크로그리드와 블록체인의 연계를 최적화하여, 데이터 보안과 에너지 관리의 신뢰성을 극대화할 수 있다.

Ⅵ. 결 론

현재 국내에서는 전술적 마이크로그리드 개념이 명확하게 정립되지 않은 상황이지만, 미군의 사례는 이를 구현하는 데 있어 중요한 참고 자료로 활용될 수 있다. 미군은 이미 전술적 마이크로그리드를 운영하며 군사적 필요에 따라 유연하고 신뢰성 있는 에너지 공급을 가능하게 하고 있으며, 이는 한국군이 유사한 시스템을 도입하는 데 유용한 교훈이 될 수 있다. 특히 한국군의 조직체계와 연동하여 프라이빗 블록체인 기반의 마이크로그리드를 구축할 경우, 분산형 보안 체계를 통해 민감한 데이터를 안전하게 관리할 수 있다. 프라이빗 블록체인의 특성상 네트워크 참여자에게만 접근 권한이 부여되므로, 보안 위험을 최소화하면서도 마이크로그리드의 실시간 통신 및 제어를 가능하게 하여 운영의 신뢰성을 높일 수 있다. 또한, 블록체인 기반 가상 발전소(BVPP, Blockchain-based Virtual Power Plant) 개념을 도입하면, 분산 에너지 자원(DER, Distributed Energy Resources)의 통합 운영을 보다 효율적으로 수행할 수 있다. BVPP는 개별적인 DER을 하나의 가상 발전소처럼 운영하는 기술로, 블록체인 스마트 컨트랙트를 활용하여 에너지 공급 및 수요를 실시간으로 조정하고 자동 거래를 수행할 수 있다. 이를 통해 한국군의 에너지 관리 시스템이 외부 위협에 더욱 강력하게 대응할 수 있으며, 위기 상황에서도 안정적인 전력 공급을 보장할 수 있다. 특히, BVPP는 기존 중앙 집중식 VPP보다 높은 보안성을 제공하며, 블록체인 원장을 기반으로 데이터 무결성을 유지하고, 분산된 에너지 네트워크 내에서 발생할 수 있는 데이터 위·변조 위험을 차단할 수 있는 장점이 있다.

본 연구에서 제안한 방안은 전술적 마이크로그리드의 보안성과 효율성을 높이는 데 기여할 수 있으나, 몇 가지 한계점을 내포하고 있다. 첫째, 한국군 조직체계와의 연동 과정에서 프라이빗 블록체인의 보안 프로토콜이 실제 운영 환경에서 얼마나 효과적으로 작동하는지에 대한 실증적인 검증이 필요하다. 블록체인 기반의 보안 프로토콜이 실제 군사 작전 환경에서 요구되는 고속 데이터 처리 및 네트워크 복원력을 충분히 제공할 수 있는지 분석해야 하며, 특히 BVPP를 적용할 경우 다수의 DER이 실시간으로 데이터를 송수신하면서 발생할 수 있는 지연(latency) 및 스마트 컨트랙트 실행 속도에 대한 최적화가 필요하다. 둘째, 프라이빗 블록체인을 통한 통신 강화 및 데이터 무결성 보장 방법이 다양한 전술적 상황에서 요구되는 실시간 성능을 충분히 충족할 수 있을지에 대한 성능 평가와 최적화가 요구된다. 마이크로그리드의 분산 구조로 인해 발생할 수 있는 데이터 처리 지연이나 보안 인증 과정에서의 병목 현상(Bottleneck)을 해결하지 않으면, 시스템의 신뢰성이 떨어질 수 있으며, 특히 군사 작전에서의 신속한 전력 배분과 비상 전력 전환 과정에서 예측하지 못한 지연이 발생할 경우 작전 수행에 치명적인 영향을 미칠 수 있다. BVPP를 효과적으로 운영하기 위해서는 DER의 실시간 모니터링 및 데이터 검증 기술을 더욱 강화하고, 블록체인 네트워크의 합의 알고리즘을 최적화하여 블록 생성 시간을 단축하고 데이터 트랜잭션 속도를 높이는 방안이 필요하다.

앞으로는 본 논문의 제안 방향을 바탕으로 실질적인 운영 환경에서의 성능 검증과 더불어, 마이크로그리드와 프라이빗 블록체인의 통합 운영에서 발생할 수 있는 기술적, 조직적 문제를 해결하기 위한 후속 연구가 필요하다. 특히, BVPP 모델의 실증 테스트를 진행하여, 실제 군사 기지 및 원격 지역에서 분산형 에너지 자원을 최적화할 수 있는 방안을 구체적으로 연구해야 한다. 또한, 블록체인 기반 전력 시장 모델을 적용하여 군사 목적뿐만 아니라, 민간 부문에서도 신재생 에너지 관리 및 스마트 그리드 확산에 기여할 수 있는 방안을 마련할 필요가 있다. 이를 통해 한국군의 전술적 마이크로그리드가 안정적으로 운영될 수 있도록 기술의 신뢰성을 높이고,

군사 및 민간 분야에서의 응용 가능성을 확대해 나갈 수 있을 것이다. 본 연구는 이러한 향후 연구를 위한 기초 자료를 제공하며, 자율적이고 안전한 에너지 관리가 필요한 다양한 환경에서 마이크로그리드 보안 강화 방안을 제시하는 데 중요한 의의를 지닌다. BVPP와 프라이빗 블록체인의 결합을 통한 에너지 네트워크의 보안성 향상은 군사 작전뿐만 아니라, 재난 대응, 원격 지역 전력 공급, 스마트 시티 구축 등 다양한 분야에서 활용될 수 있는 중요한 전략적 기술로 자리 잡을 것으로 기대된다.

참고문헌

[1] Y. Song, M. Jeong, and G. Lee, “Army’s Long-Term Strategy Beyond the 4th Industrial Revolution -Army Vision 2050-,” *Defense & Technology*, Vol. 496, pp. 46-57, June 2020.

[2] M. Jeong, “8 Game Changers That Will Shake Up Future Battlefields: 2050 Army Vision,” *The Republic of Korea Army Magazine*, No. 421, pp. 22-23, December 2020.

[3] I. Lee, S. Park, and D. Lee, “A Study on the Application of Microgrid for Stable Wartime/Peacetime Energy Source in Republic of Korea Army,” *Korean Journal of Military Art and Science*, Vol. 78, No. 3, pp. 387-418, October 2022.

[4] S.-H. Park, I.-H. Shin, and J.-W. Yang, “Application Cases and Implications of Blockchain Technology in Defense Sectors,” *Defense & Technology*, Vol. 541, pp. 104-111, March 2024.

[5] J. Kim, M. Jo, J. Kim, J. Park, and D. Moon, “A Study on Microgrid Security Modeling and Field Demonstration,” in *Proceedings of Symposium of the Korean Institute of Communications and Information Sciences*, Jeju, pp. 1118-1119, June 2018.

[6] M.-J. Lee and Y.-T. Jin, “Software Development Based on Blockchain Using Hyperledger Fabric,” *Journal of Knowledge Information Technology and Systems*, Vol. 17, No. 2, pp. 211-220, April 2022. http://doi.org/10.34163/jkits.2022.17.2.004

[7] DoD (United States Department of Defense), Tactical Microgrid Communications and Control, Author, Arlington: VA, Department of Defense Interface Standard MIL-STD-3071, January 2023.

[8] Y. Lee, Current Status of Domestic and International Promotion of Microgrid and Policy Trends, KEPCO Economy & Management Research Institute, Naju, KEMRI Power Economics Review No. 2015-12, pp. 7-10, December 2015.

[9] J. Lee, “KEPCO Transforms Lizard Butterfly Farm into Drawer ‘Intelligent Power Grid’,” *Electric Power72*, Vol. 2016, No. 3, pp. 72-73, March 2016.

[10] Kitakyushu City. Kitakyushu Eco-town Business Transaction [Internet]. Available: https://www.kitaqecotown.com/docs/20191030/ecotown-pamphlet-kr.pdfiPamphlet-KR.

[11] G. Prettico, A. De Paola, D. Thomas, N. Andreadou, I. Papaioannou, and E. Kotsakis, Clean Energy Technology Observatory: Smart Grids in the European Union - 2022 Status Report on Technology Development, Trends, Value Chains and Markets, Publications Office of the European Union, Luxembourg, EUR 31237 EN, November 2022. https://dx.doi.org/10.2760/276606

[12] National Renewable Energy Laboratory. Summary of Microgrid Activities in the USA [Internet]. Available: https://microgrid-symposiums.org/wp-content/uploads/2022/01/Summary-of-Microgrid-Activities-in-the-United-States.pdf.

[13] P. Asmus, A. Forni, and L. Vogel, Microgrid Analysis and Case Studies Report: California, North America, and Global Case Studies, California Energy Commission, Sacramento: CA, Energy Research and Development Division FINAL PROJECT REPORT CEC-500-2018-022, August 2018.

[14] S. Booth, J. Reilly, R. Butt, M. Wasco, and R. Monohan, Microgrids for Energy Resilience: A Guide to Conceptual Design and Lessons from Defense Projects, National Renewable Energy Laboratory, Golden: CO, Technical Report NREL/TP-7A40-72586, January 2020. https://doi.org/10.2172/1598145

[15] United States Department of Energy, Microgrid and Integrated Systems Program, Author, Washington, DC, January 2022.

[16] E. O’Shaughnessy, J. Heeter, J. Gattaciecca, J. Sauer, K. Trumbull, and E. Chen, Community Choice Aggregation: Challenges, Opportunities, and Impacts on Renewable Energy Markets, National Renewable Energy Laboratory (NREL), Golden: CO, Tech. Rep. NREL/TP-6A20-72195, February 2019.

[17] G. B. Gaggero, P. Girdinio, and M. Marchese, “Advancements and Research Trends in Microgrids Cybersecurity,” *Applied Sciences*, Vol. 11, No. 16, 7363, August 2021. https://doi.org/10.3390/app11167363

[18] N. Jamil, Q. S. Qassim, F. A. Bohani, M. Mansor, and V. K. Ramachandaramurthy, “Cybersecurity of Microgrid: State-of-the-Art Review and Possible Directions of Future Research,” *Applied Sciences*, Vol. 11, No. 21, 9812, October 2021. https://doi.org/10.3390/app11219812

[19] S.-Y. Kim and J. A. Mathews, “Korea’s Greening Strategy: The Role of Smart Microgrids,” *Asia-Pacific Journal*, Vol. 14, No. 24, e1, December 2016. https://doi.org/10.1017/S1557466016013140

[20] TTA (Telecommunications Technology Association), Security Requirements for Smart Grid, Author, Seongnam, TTAK.KO-12.0182, December 2011.

[21] TTA (Telecommunications Technology Association), Security Functional Requirements for Smart Grid System, Author, Seongnam, TTAK.KO-12.0209, December 2012.

[22] KETEP (Korea Institute of Energy Technology Evaluation and Planning), Construction of K-MEG Open-Type Onboard Test for DC Distribution Application, Author, Seoul, Final Report 2011T100100025, October 2014.

[23] T. Basso and R. DeBlasio, IEEE Smart Grid Series of Standards IEEE 2030 (Interoperability) and IEEE 1547 (Interconnection) Status, National Renewable Energy Laboratory, Golden: CO, NREL/CP-5500-53028, April 2012.

[24] NIST (National Institute of Standards and Technology), The NIST Cybersecurity Framework (CSF) 2.0, Author, Gaithersburg: MD, NIST CSWP 29, February 2024. https://doi.org/10.6028/NIST.CSWP.29

[25] ITTP (Institute of Information & Communications Technology Planning & Evaluation), Development of Blockchain-Based Embedded Devices and Platform for MG Security and Operational Efficiency, Ministry of Science and ICT, Sejong, February 2021.

[26] S. Kim and K. Lee, “Analysis of Cyber Attack Threats and Response Measures for Microgrid Control Systems,” *Journal of Information Security*, Vol. 27, No. 2, pp. 45-53, 2017.

[27] S. Booth, J. Reilly, R. Butt, M. Wasco, and R. Monohan, Microgrids for Energy Resilience: A Guide to Conceptual Design and Lessons from Defense Projects. National Renewable Energy Laboratory. Golden: CO, Technical Report NREL/TP-7A40-72586, January 2020. https://doi.org/10.2172/1598145

[28] S. Booth, J. Reilly, R. Butt, M. Wasco, and R. Monohan. Private Blockchain Networks: A Solution for Data Privacy [Internet]. IEEE. https://ieeexplore.ieee.org/document/9334132.

[29] P. Krishnamoorthi, S. Shahid, and O. Boydell, Preserving Privacy in Private Blockchain Networks, in K. Lee and L. J. Zhang (Eds.), *Blockchain −ICBC 2021*, Lecture Notes in Computer Science, Vol. 12991, Cham: Springer, 2022. https://doi.org/10.1007/978-3-030-96527-3_8

[30] D. Drescher, Blockchain Technology in the Department of Defense, Naval Postgraduate School, 2017.

[31] Z. Li and B. Yang, “Research on Intelligent Security Management Architecture of Military Blockchain,” In *Proceedings of IEEE Conference*, 2020.

[32] F. Luo, A. Dorri, G. Ranzi, and R. Jurdak, “Aggregating Buildings as Virtual Power Plant: Architecture, Implementation Technologies, and Case Studies,” arXiv:2004.05807, 2020. https://doi.org/10.48550/arXiv.2004.05807

[33] M. M. Hussain, M. Rahman, and M. S. Hossain, “Blockchain-Based Microgrid Energy Trading System: A Review of the State-of-the-Art and Future Research,” *Energies*, Vol. 14, No. 24, 8050, December 2021.

최연호(Yeon-ho Choi)

2018년～2022년: 동의대학교 전기공학과
2022년～현 재: 아주대 정보통신대학원 사이버보안과
2022년～현 재: 대한민국 육군 정보통신 장교
※관심분야 : 디지털 포렌식(Digital Forensics), 블록체인(Blockchain), 에너지 저장 시스템(ESS System), 스마트/마이크로 그리드(Smart/Microgrid) 등

손태식(Taeshik Shon)

2000년 : 아주대학교 정보및컴퓨터공학부 졸업(학사)
2002년 : 아주대학교 정보통신전문대학원 졸업(석사)
2005년 : 고려대학교 정보보호대학원 졸업(박사)
2004년～2005년: University of Minnesota 방문연구원
2005년～2011년: 삼성전자 통신·DMC 연구소 책임연구원
2017년～2018년: Illinois Institute of Technology 방문교수
2011년～현 재: 아주대학교 정보통신대학 사이버보안학과 교수
※관심분야 : Digital Forensics, ICS/Automotive Security