Journal of KIIT. Vol. 22, No. 7, pp. 169-177, Jul. 31, 2024. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2024.22.7.169

블록체인 기반 스마트그리드 비식별화 메타데이터 전송 메커니즘

김진수*, 박남제**

Blockchain-based Smart Grid De-Identification Metadata Transmission Mechanism

Jinsu Kim*, Namje Park**

이 논문은 2024학년도 제주대학교 교육·연구 및 학생지도비 지원에 의해서 연구되었음

요 약

기후 위기에 대한 대응이 중요해짐에 따라 탄소 중립과 같은 친환경 에너지 정책의 적극적인 도입이 요구되고 있다. 이에 따라 전력을 효율적으로 분배하기 위해 스마트그리드를 접목하여 전기 공급자와 소비자의 실시간 정보교환을 제공하는 지능형 전력인프라가 도입되고 있다. 스마트그리드에서 전기 공급자와 소비자간의 정보교환은 효율적인 전력 활용에 이바지하고 있으나, 동시에 정보교환 과정에서 발생하는 다양한 문제점이 존재한다. 특히 소비자가 특정되는 경우에는 특정 가구의 계량 정보를 기반으로 소비자의 생활 패턴을 분석함으로써 개인정보침해로 이어질 수 있다. 따라서 본 논문에서는 정보교환 과정을 비식별화된 메타데이터를 블록체인을 활용하여 전달하는 블록체인 기반의 비식별화 메타데이터 전송 메커니즘을 제안한다.

Abstract

As the response to the climate crisis becomes important, the active introduction of eco-friendly energy policies such as carbon neutrality is required. Accordingly, an intelligent power infrastructure that provides real-time information exchange between electricity providers and consumers by grafting a smart grid is being introduced in order to efficiently distribute power. Information exchange between electricity providers and consumers in a smart grid contributes to efficient use of power, but at the same time, there are various problems that arise in the process of information exchange. In particular, when a consumer is specified, it can lead to personal information infringement by analyzing the consumer's life pattern based on the measured information of a specific household. Therefore, this paper proposes a blockchain-based de-identified metadata transmission mechanism that transmits de-identified metadata in the information exchange process using a blockchain.

Keywords
blockchain, de-identification, metadata, smart grids, data transfer

* 제주대학교 융합정보보안학 협동과정 박사과정
- ORCID: https://orcid.org/0000-0003-1009-3928
** 제주대학교 초등컴퓨터교육학과 교수(교신저자)
- ORCID: https://orcid.org/0000-0003-4434-8933

· Received: Mar. 29, 2024, Revised: Jul. 01, 2024, Accepted: Jul. 04, 2024
· Corresponding Author: Namje Park
Dept. of Computer Education, Teachers College, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
Tel.: +82-64-754-4914, Email: namjepark@jejunu.ac.kr

Ⅰ. 서 론

기후 변화가 현실에 큰 영향을 끼침에 따라 6대 온실 가스의 배출량과 흡수량을 같도록 하는 Net-Zero가 국제적인 이슈가 되고 있으며, 국내에서는 탄소중립기본법에서 탄소 중립을 6대 온실가스에 대한 상쇄로 정의함에 따라 탄소 중립이라는 단어로도 표현하고 있다[1][2]. 각 국에서는 Net-Zero를 실현하기 위한 많은 시도를 진행하고 있으며, 온실가스의 배출을 최소화하기 위해 기존의 전력 발전 방식을 대체하는 재생 에너지 발전 비중을 높이고 있다[3][4]. 하지만 재생 에너지는 언제나 일정할 수 없으며, 환경의 변화에 따라 불규칙적일 수 밖에 없다. 따라서 효과적인 전력 분배가 요구되며, 이에 따라 화두가 되는 것이 스마트그리드(Smartgrid)이다[5][6].

스마트그리드는 정보통신기술을 활용하여 전기 공급자와 소비자 사이의 실시간 정보교환을 수행함으로써 효과적으로 전기를 공급할 수 있도록 하는 차세대 전력 공급 인프라이다[7][8]. 전력 공급자와 에너지 관리 시스템, 전력 소비자 및 소비 시설 등 전반적인 에너지 설비를 포함한다[9][10]. 스마트그리드에서는 실시간으로 정보를 교환함으로써 소비자에게 요구되는 전력을 공급하기 때문에 과잉 생산을 방지할 수 있으며, 재생 에너지를 생산하는 가구에서는 전력을 판매까지 할 수 있는 환경을 구축할 수 있다[11][12].

하지만 현재의 전력 공급 방식에서 공급된 전력의 측정 방식이 현장의 계량기 확인을 통한 일정 주기 단위의 소비 전력 측정이 아닌, 실시간으로 소비 전력을 측정하고 해당 내용이 네트워크를 통해 전달될 수 있다는 점에서 소비자의 전력 사용 패턴을 분석하여 생활 패턴을 파악할 수 있다는 개인정보 침해 문제, 임의적인 계량기 접근을 통한 조작으로 인해 실제 소비 전력과는 다르게 위•변조를 수행할 수 있다는 문제 등이 발생할 수 있다[13][14].

따라서 본 논문에서는 비식별화 메타데이터와 블록체인을 기반으로 전력 공급자와 소비자간의 정보 교환 데이터의 무결성을 강화하고, 참여자간에 데이터가 공유되는 블록체인의 특성 상 발생할 수 있는 전력 사용 유출 방지를 위해 비식별화하여 특정 사용자를 식별할 수 없도록 하는 메커니즘을 제안한다.

Ⅱ. 스마트그리드 메타데이터 유형 분석

2.1 스마트그리드 구성요소

2019년 한국인터넷진흥원에서 발간한 「스마트에너지 사이버보안 가이드」에 따르면 스마트 에너지의 구성요소는 정보통신기술의 양방향 통신을 기반으로 디지털 계량방식을 탑재하여 전력 공급자와 실시간으로 정보를 주고받을 수 있는 첨단계량인프라(AMI, Advanced Metering Infrastructure), 생산된 전기를 저장장치에 보관하여 필요한 경우 전기를 제공할 수 있도록 하는 에너지저장장치(ESS, Energy Storage System), 정보통신기술 및 제어기술을 기반으로 상업용 건물, 공장, 주택등을 대상으로 소비 에너지 시각화 및 최적화를 위한 에너지관리시스템(EMS, Energy Management System), 전기차 충전 기반시설인 EV(Electric Vehicle)충전시스템, 주유를 위한 장치로 POS(Point Of Sale System)를 포함하는 셀프주유기, 가정 내의 스마트에너지용 기기 및 스마트 기기와 외부에서 가정 내의 기기와 연결되는 모든 기기를 의미하는 댁내 에너지 기기로 구성된다[15][16].

2.2 스마트그리드 메타데이터 분석

스마트그리드 환경에서 메타데이터는 크게 계량정보, 요금정보, 고객정보, 결제정보, 제어정보, 부가정보의 6가지로 구성된다. 계량정보는 고객과 계량기의 번호, 계측값, 시간 등 에너지 계량과 관련된 정보를 포함한다. 요금정보는 요금의 산정기간, 합계, 계산일, 고객 번호와 같이 과금에 연관된 정보를 의미한다. 고객 정보는 고객번호와 이름, 주소와 같이 에너지를 사용하는 사용자의 개인정보가 포함된다. 결제정보는 신용카드의 번호나 유효기간과 같이 신용카드 결제와 관련된 정보를 의미한다. 제어정보는 개폐 명령이나 개폐 상태와 같이 기기에 대한 제어 정보를 포함한다.

부가정보는 계량기의 번호와 발생한 이벤트의 구분, 시간, 내용 등의 부가적인 내용을 포함한다. 따라서 스마트그리드 메타데이터에는 개인정보, 에너지 사용량, 결제 정보와 같이 보안이 필요한 다양한 데이터가 포함된다[17][18].

2.3 스마트그리드 데이터 보안 동향 분석

환경 오염의 대응을 위한 Net-Zero 정책이 주요한 화두로 떠오름에 따라 에너지 최적화를 위한 스마트그리드의 중요성은 점차 확대되고 있다. 하지만, 계량기 중심의 전력 공급을 수행하던 기존의 방식과 달리, 계량 정보가 네트워크상을 통해 공유된다는 점에서 데이터의 훼손을 방지하고, 안전한 에너지 거래 수행을 위한 방안이 요구되고 있다. 특히, 에너지 거래의 투명성을 보장함과 동시에 거래 기록의 무결성를 강화할 수 있다는 점에서 블록체인을 기반으로 한 에너지 거래 기법에 대한 연구가 수행되고 있다.

Y.-N. Cao et al.의 연구[19]에서는 스마트그리드에서 발생하는 데이터의 수집과 에너지 거래 프로세스의 프라이버시, 신원 인증과 데이터 활용성 측면에서 블록체인을 접목하였을 때 발생할 수 있는 이점을 분석하기 위해 다양한 연구의 동향을 분석하였다. 분석 과정에서 현재까지의 블록체인 기반 스마트그리드 전력거래 플랫폼에서 발생할 수 있는 단점으로 무조건적인 익명성에 따른 블록체인 추적성 감소, 스마트 계량기의 물리적 보안 취약점과 같은 문제를 제시하였다.

W. Zhao et al.의 연구[20]에서는 스마트그리드 환경에 블록체인을 적용하기 위한 요구사항을 연구하였다. 해당 연구에서는 블록체인 기술이 스마트그리드에서 수행해야 할 역할을 데이터 불변성, 투명성, 스마트 계약, 보안을 기반으로 4가지 측면으로 정리하였다. 블록체인의 역할에는 친환경 에너지의 생성부터 관리 및 거래 과정에서 데이터가 변하지 않도록 하는 데이터 불변성, 모든 데이터가 제 3자에 의해 검증될 수 있도록 하는 투명성, 작성된 계약에 의해서만 거래를 수행하며 계약 내용이 제 3자에 의해 임의로 수정될 수 없는 스마트 계약, 공개키 기반의 사용자 인증을 수행하는 보안이 포함된다.

J. Gao et al.의 연구[21]에서는 마이크로그리드 환경에서 예측 불가능한 분산 전력 생산 문제를 해결하기 위해 블록체인 기반의 P2P 에너지 거래 시스템을 제안하였다. 해당 연구에서는 무인증 암호화(Certificateless signcryption) 기술과 프라이빗 블록체인을 기반으로 사전에 선택된 노드에서 블록 생성을 위한 합의 과정을 수행함으로써 요구되는 비용을 최소화하는 P2P 기반의 에너지 거래를 수행할 수 있도록 하였다.

III. 블록체인 기반 스마트그리드 비식별화 메타데이터 전송 메커니즘

본 논문에서는 스마트그리드 환경에서 전력 공급자와 사용자간의 정보교환 과정을 블록체인을 적용하여 수행하며, 수행 과정에서 메타데이터에 대한 비식별화를 수행함으로써 제 3자에 의한 데이터 유출을 방지하고, 데이터의 무결성을 강화할 수 있는 메커니즘을 제안한다. 제안하는 메커니즘은 크게 클라이언트와 블록 네트워크, 서버의 3가지 구성요소로 나뉘며, 클라이언트는 전력 공급자와 소비자로 구분한다. 제안하는 메커니즘의 주요 모듈은 클라이언트를 블록 네트워크에 등록하는 DID 등록 모듈, 전력 거래 수행 모듈의 2가지로 구성된다.

DID 등록 모듈에서는 서버에서 소비자와 전력 공급자를 포함하는 클라이언트에 1차적으로 식별정보를 제공하고, 해당 식별정보를 포함하여 DID를 생성함으로써 인증된 사용자 리스트를 서버에서 보관한다. 전력 거래 수행 모듈에서는 소비자와 전력 공급자간의 전력 거래 수행 과정을 블록체인을 기반으로 수행함으로써 데이터의 무결성을 강화한다.

그림 1은 제안 메커니즘의 전반적인 전력 거래 과정을 보이는 것이다. 전력 공급자는 전력 현황에 대한 갱신값을 지속적으로 블록 네트워크상에 기록하며, 소비자에 의한 전력 요청이 발생할 경우에 전력 요청 트랜젝션을 생성한다. 소비자는 전력 요청 트랜젝션에 자신의 검증정보를 포함하여 트랜젝션을 생성한다.

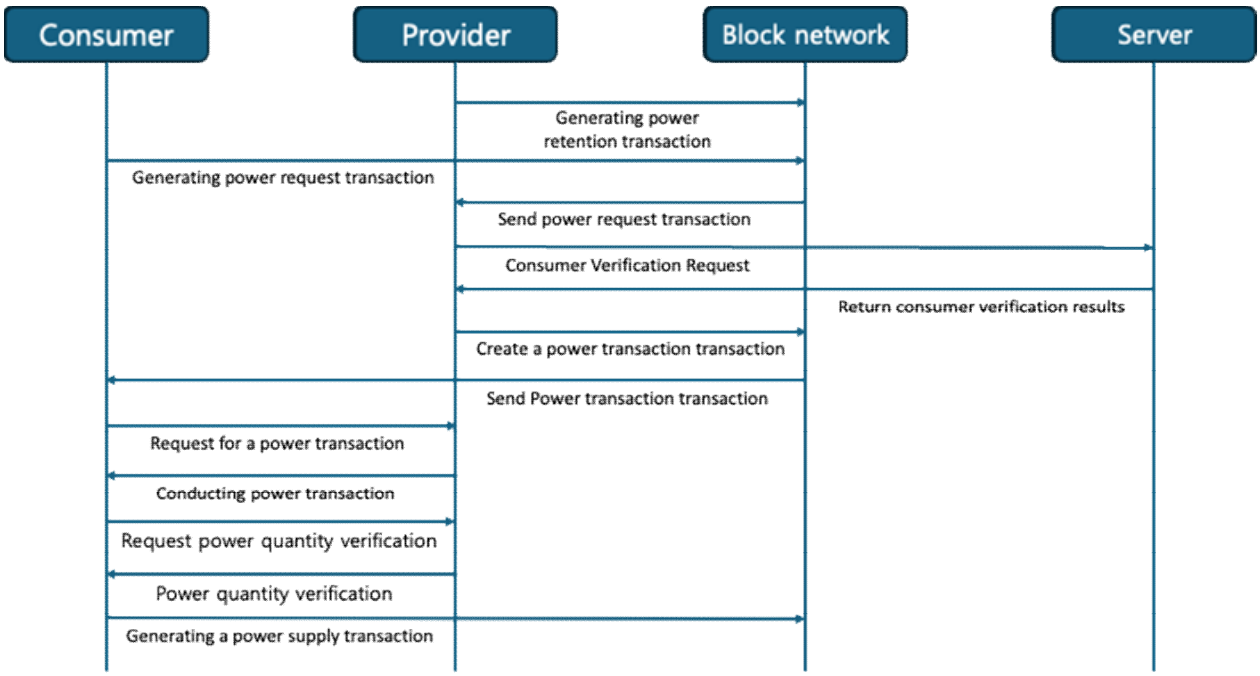

그림 1. 제안 메커니즘 흐름도
Fig. 1. Flowchart of proposed mechanism

전력 공급자는 전력 요청 트랜젝션 내의 사용자 검증정보를 서버측에 전송하여 검증을 요청한다. 이때, 사용자 검증정보는 서버에 의해 생성되며 식별번호, 사용자 정보 등을 포함한다. 서버는 사용자 검증정보를 활용하여 수행한 검증 결과를 전력 공급자에 제공하며, 전력 공급자는 서버에 의해 소비자가 정상적인 소비자임이 확인될 경우 전력 거래 트랜젝션을 생성한다. 전력 거래 트랜젝션은 전력 공급자에게 전달되며, 트랜젝션을 받는 전력 공급자가 둘 이상인 경우, 중복으로 둘 이상의 전력 공급자의 전력 거래 트랜젝션이 처리될 수 있으므로, 소비자가 트렌젝션에 의해 전력 공급자에게 전력 거래 요청을 수행할 경우 전력 거래를 진행한다. 거래가 성사된 경우 전력 공급 트랜젝션을 작성하여 블록 네트워크에 전송한다.

3.1 DID 클라이언트 등록 모듈

클라이언트는 전력 공급을 희망하는 소비자와 전력 공급을 수행하는 전력 공급자로 구분할 수 있다. 하지만, 지속적인 정보교환은 실시간으로 사용자의 전력량을 확인할 수 있기에 사용자의 식별정보는 사용자의 전력량 변화를 확인할 수 있는 지표가 될 수 있다. 따라서 전력 거래 과정에서 사용자를 유추할 수 있는 정보의 비식별화가 요구된다.

DID 클라이언트 등록 모듈에서는 1차적으로 서버에 의해 사용자의 식별번호(IDU), 등록 일자(DR), 계량기 식별 정보(IDEM) 등 사용자를 식별할 수 있는 정보를 포함하는 사용자 식별 정보를 생성하여 클라이언트에 전송한다.

그림 2는 서버에서 생성한 DID 식별정보를 클라이언트에 전달하는 과정을 보이는 것이다.

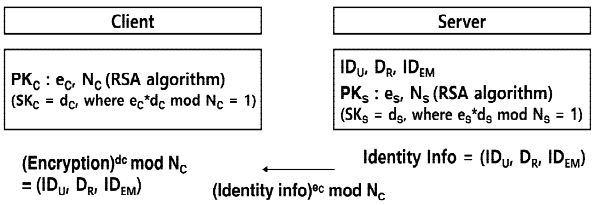

그림 2. DID 식별정보 전달 과정
Fig. 2. Delivery process of DID identification information

그림 3은 클라이언트에서 블록 네트워크에 DID를 등록하는 과정을 보이는 것이다. 클라이언트는 클라이언트의 공개키와 식별정보의 해시값을 포함하는 DID 식별자를 생성하여 블록 네트워크에 DID 등록을 요청한다.

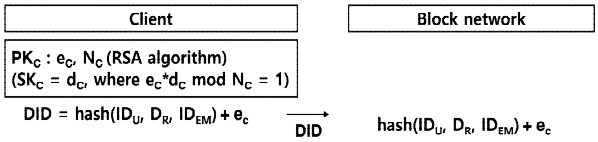

그림 3. 클라이언트-블록네트워크 DID 등록 과정
Fig. 3. Registration process of client-block network DID

그림 4는 DID 등록 과정을 보이는 것이다. 클라이언트에 의해 블록 네트워크에 등록된 DID 정보는 서버에서 검증을 수행한다. 검증된 DID 정보는 서버의 비밀키에 의해 암호화되어 블록 네트워크에 기록함으로써 다른 클라이언트에 대해 해당 DID가 서버에 의해 검증되었음을 증명한다.

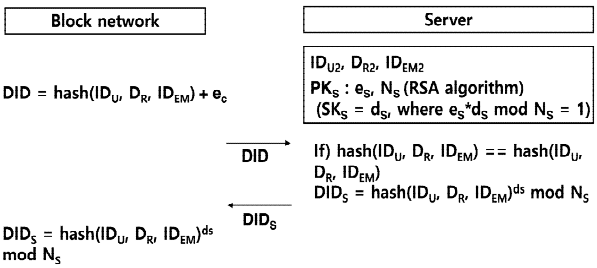

그림 4. 블록네트워크-서버 DID 등록 과정
Fig. 4. Registration process of block network-server DID

3.2 전력 거래 수행 모듈

전력 거래 수행 모듈은 소비자와 전력 공급자 사이에서 전력을 거래하는 과정에서 소비자의 메타데이터를 비식별화하여 외부 노출을 최소화한다.

전력 거래는 소비자가 블록 네트워크에 전력 요청 트랜잭션을 생성함으로써 시작한다. 전력 요청 트랜잭션에는 식 (1)과 같이 전력 요청 정보(Request energy)와 요청 시간, 사용자 식별 번호, 등록일자, 계량기 식별정보, 요청 시간(TR)에 대한 해시가 포함된다. 식 (2)는 소비자의 식별정보 구조를 보이는 것이다.

$$Requestdata = requestenergy + T_R + Hash(ID_U + D_R + ID_{ER} + T_R) \quad (1)$$

$$U_{ID} = ID_U + D_R + ID_{ER} + T_R \quad (2)$$

전력 공급자는 블록 네트워크상의 전력 요청 트랜잭션을 획득하여 정당한 소비자임을 확인하기 위해 서버로 소비자 식별정보 해시와 요청 시간을 전력 공급자의 비밀키로 암호화한 뒤, 2차적으로 서버의 공개키로 암호화를 수행하여 서버로 전송한다. 외부로 노출되는 소비자의 식별정보는 요청 시간과 식별정보에 요청시간을 추가한 해시값으로 구성된다. 식 (3)는 소비자의 검증을 위해 전력 공급자로부터 서버로 전송하는 데이터 구조를 보이는 것이다.

$$data = T_R + Hash(ID_U + D_R + ID_{ER} + T_R) \quad (3)$$

서버는 가지고 있는 클라이언트의 식별정보와 전력 공급자로부터 받은 요청 시간을 결합하여 소비자를 검증하고, 소비자의 검증 수행 결과와 전력 공급자의 요청 순위를 전력 공급자에게 전송한다. 이때, 요청 순위는 소비자의 전력 공급 요청에 따라 서버로 소비자의 검증 요청을 수행한 전력 공급자의 우선 순위를 의미한다. 검증된 소비자임이 증명된 경우, 전력 공급자는 서버로부터 받은 우선 순위(RP)와 소비자 식별 정보 해시, 전력 공급 정보(IPS), 전력 공급자의 식별정보(IDEM) 해시를 포함하여 전력 거래 트랜잭션을 작성한다. 식 (4)은 전력 거래 트랜잭션의 구조를 보이는 것이다.

$$Transaction = hash(ID_{EM}) + R_P + I_{PS} + hash(ID_U + D_R + ID_{ER} + T_R) \quad (4)$$

소비자는 전력 거래 트랜잭션을 통해 우선 순위의 전력 공급자에 전력와 거래를 수행하고, 전력 공급 트랜잭션을 작성한다. 전력 공급 트랜잭션의 작성을 위한 1차적 데이터는 소비자에 의해 전력 거래 정보(IDT)를 포함하여 전력 공급자에 검증을 요청한다. 식 (5)는 소비자가 전력 공급자에게 전송하는 1차 전력 공급 검증 데이터의 구조를 보이는 것이다.

$$^{1st}Transaction_d = hash(U_{ID}) + ID_T + T_R + hash(ID_{EM}) \quad (5)$$

전력 공급자는 소비자로부터 받은 1차 데이터에 대한 검증을 수행한 후, 데이터가 정상적인 데이터인 경우에는 1차 데이터의 해시를 생성하여 전력 공급자의 비밀키(dp, Np)로 암호화하여 2차 데이터를 작성하여 소비자에게 전송한다. 식 (6)은 전력 공급자에 의해 검증이 수행되었음을 증명하는 해시를 포함하여 소비자에게 전달되는 2차 검증 데이터의 구조를 보이는 것이다.

$$^{2nd}Transaction_d = {}^{1st}Transaction_d + (hash({}^{1st}Transaction_d))^{dp} \bmod N_p \quad (6)$$

소비자는 전력 공급자로부터 받은 2차 데이터에 포함되어있는 전력 공급자의 해시와 1차 데이터를 사용하여 검증을 수행하고, 전력 공급 트랜잭션을 작성한다.

Ⅳ. 제안 메커니즘 분석

스마트그리드에서 에너지 거래의 신뢰성을 강화하기 블록체인을 적용하는 것은 거래의 투명성을 강화하고, 트랜잭션의 무결성을 증명할 수 있는 방안이 될 수 있다. 블록체인을 스마트그리드에 적용하기 위해 다양한 방면에서의 검토가 요구되며, 본 절에서는 효과성 검증을 수행하기 위해 Ya-Nan Cao의 연구에서 제시하고 있는 문제점인 데이터 익명성과 Wenbing Zhao의 연구에서 제시하고 있는 블록체인 기반 스마트그리드 환경에서 요구되는 트랜잭션 투명성과 데이터 불변성을 포함하여, 총 3가지 관점에서 제안 메커니즘의 효과성 분석을 수행한다.

데이터 익명성은 공개되어있는 블록체인의 특성상 노출되는 데이터에 의해 제 3자에 의해 특정 사용자임을 인지할 수 없도록 하는 것이다. 일반적으로 에너지 거래 과정에서 사용자의 정보를 숨기는 익명성은 에너지 활용 패턴을 포함한 메타데이터를 익명화함으로써 특정 사용자의 에너지 사용 패턴을 숨김으로서 프라이버시를 보호하는데 중요한 요소이다. 하지만, 익명성의 강화는 공개성을 요구하는 블록체인에서 추적성을 감소시킨다는 문제를 야기할 수 있다. 제안 메커니즘에서는 소비자의 식별 정보를 서버와 소비자만이 공유하는 방식을 적용하여 식별 정보와 전력 요청 정보의 해시를 트랜잭션의 식별 정보로 활용함으로써 익명성을 보장하되, 소비자 혹은 서버는 식별 정보를 기반으로 전력 거래의 무결성을 검증할 수 있도록 하여 제 3자에 의한 추적은 불가하도록 하였다.

트랜잭션 투명성은 거래 과정에서 발생하는 트랜잭션이 제 3자에 의해 변동되지 않으며, 모든 데이터가 제 3자에 의해 검증될 수 있어야 함을 의미한다. 제안 메커니즘에서는 전력 거래 요청 과정에서 사용자의 정보를 익명화함에 따라 제 3자는 거래를 수행하는 당사자를 유추할 수 없다. 하지만 전력 공급자에 의한 전력 거래 트랜잭션에서 요청 일자와 결합되어 유동성을 가지는 소비자 식별 정보 해시와 전력 공급 우선순위, 전력 공급자의 식별 정보를 통해 전력 요청을 검증할 수 있으며, 거래 과정에서 발생하는 전력 거래 트랜잭션의 전력 거래 정보와 거래 일시를 통해 전력 거래 과정을 검증할 수 있다.

데이터 불변성은 에너지 생성에서부터 거래에 의한 소비까지 전주기에 대한 트랜잭션이 제 3자에 의한 변동 없이 무결성을 유지하여야 함을 의미한다. 제안 메커니즘에서는 전력 공급자의 전력 정보에 대해 블록 네트워크상에 지속적으로 갱신하도록 하여 전력 생산에 대한 정보를 기록하며, 생산된 전력에 대한 거래가 수행된 경우, 요청 프로세스와 거래 프로세스의 트랜잭션을 생성하여 기록하도록 하여 전력 공급 전주기에 대한 데이터를 블록 네트워크에 기록하도록 하였다.

따라서 제안 메커니즘은 사용자 식별정보를 유동적으로 변경하여 제 3자에 의한 추적은 불가하되, 사용자 식별정보를 가진 사용자와 서버에서는 식별할 수 있도록 하여 추적성을 제공함으로써 데이터 익명성을 제공한다. 또한 유동적인 사용자 식별 정보 해시를 식별키로 사용하는 전력 거래 트랜잭션을 작성함으로써 비식별화된 사용자 정보와 평문 전력 거래 정보를 제공함으로써 제 3자에 의한 검증을 수행할 수 있도록 트랜잭션 투명성을 제공한다. 마지막으로 전력 공급 전주기에 대한 트랜잭션 관리를 통해 전력의 공급부터 소비까지의 과정을 블록 네트워크를 통해 기록함으로써 데이터 불변성을 강화하였다.

제안 메커니즘은 에너지 거래를 수행하는 과정에서 소비자의 식별정보를 에너지 거래 데이터와 결합한 해시로 변환하여 비식별화하는 메커니즘이다. 따라서 사용자 식별정보와 에너지 거래 데이터를 기반으로 블록에 포함되는 데이터의 작성에 시간이 요구된다. 700Byte 크기의 사용자 식별정보를 에너지 거래 데이터와 결합하여 해시값을 생성하고, 최종적으로 블록에 기록하기 위해 암호화를 수행하는 과정에서 평균적으로 8ms 가량이 소요되었다.

제안 메커니즘은 거래 과정을 블록체인을 기반으로 수행하기에 블록의 생성속도가 중요한데, 일반적으로 알려진 PoW 방식의 비트코인은 평균적으로 10분에 걸쳐 하나의 블록이 생성되며, PoS 방식으로 전환을 수행한 이더리움은 약 13~15초 간격으로 블록의 생성을 수행한다. 따라서 이더리움에 적용할 경우, 제안 메커니즘에서는 전력 요청, 거래 계약, 공급 시작 시점, 공급 종료 시점 4단계 과정을 거쳐 수행되므로 하나의 거래가 온전히 수행되기 위해서는 1분 이상의 시간이 소요될 것으로 분석된다.

Ⅴ. 결 론

온실 가스에 의한 환경 오염 문제가 부상함에 따라 각 국에서는 온실 가스의 배출량을 줄이는 Net-Zero 정책을 진행하고 있다. 이에 따라 재생 에너지를 적극적으로 도입하고, 불규칙한 재생 에너지의 안정적 공급을 위해 스마트그리드를 통한 전략적인 에너지 공급 수행이 요구되고 있다.

하지만 전력 공급을 소비자의 수요에 따라 진행해야하는 스마트그리드에서는 효과적인 공급을 위해 소비자와 지속적인 정보교환이 요구되며, 이에 따라 정보교환 과정에서 발생하는 데이터의 유출로 인한 소비자의 에너지 사용 패턴 분석 문제, 사용자의 개인 사생활을 위협할 수 있는 프라이버시 문제, 계량 정보의 임의적 위·변조 수행을 통한 데이터 무결성 훼손과 같은 다양한 문제가 야기되고 있다.

따라서 본 논문에서는 블록체인을 기반으로 전력 공급자와 소비자의 정보교환을 수행함으로써 데이터의 무결성을 강화한다. 또한, 소비자의 식별 정보를 서버에서 생성한 식별 정보와 전력 요청 시간을 결합한 해시값을 사용함으로써 서버에서는 소비자를 검증할 수 있도록 하며, 전력 공급자에게는 소비자를 식별할 수 없도록 하였다. 또한, 전력 공급 전 주기에 대한 트랜젝션을 작성함으로써 데이터가 제 3자에 의해 임의로 변경되어 전력 공급에 대한 데이터가 위·변조 되는 것을 방지하였다. 하지만 제안 메커니즘은 사용자 식별정보를 서버와 사용자가 공유하도록 하여 데이터 검증이 요구되는 경우에 사용자 식별 정보를 요구한다는 점에서 다른 문제를 야기할 수 있다. 사용자 식별정보와 전력 거래 과정에서 발생하는 유동적 데이터를 결합한 해시에 기반하기에 사용자 식별 정보가 탈취되는 경우에는 제 3자에 의해 탈취된 사용자의 전력 공급 정보를 획득할 수 있다는 문제를 가질 수 있다. 향후, 사용자 식별 정보 탈취에 따른 제 3자의 데이터 획득을 방지하기 위해 사용자 식별 정보를 분산 기록하는 방안의 연구 수행이 요구된다.

References

[1] Korean Law Information Center, "Framework Act on Carbon Neutrality and Green Growth for For Coping with Climate Crisis", Act No. 18469, Sep. 2021.

[2] J. Kim, N. Park, G. Kim, and S. Jin, "CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia", Electronics., Vol. 8, No. 4, pp. 412, Mar. 2019. https://doi.org/10.3390/electronics8040412.

[3] H. Li, Z. Ren, A. Trivedi, D. Srinivasan, and P. Liu, "Optimal Planning of Dual-Zero Microgrid on an Island Toward Net-Zero Carbon Emission", IEEE Transactions on Smart Grid, Vol. 15, No. 2, pp. 1243-1257, Mar. 2024. https://doi.org/10.1109/TSG.2023.3299639

[4] S. M. Rue, "Study on Smart Grid Trend and Policy Enforcement Way", Journal of Korean Institute of Information Technology, Vol. 12, No. 7, pp. 163-177, Jul. 2014. https://doi.org/10.14801/kiitr.2014.12.7.163.

[5] M. B. Mollah, et al., "Blockchain for Future Smart Grid: A Comprehensive Survey", IEEE Internet of Things Journal, Vol. 8, No. 1, pp. 18-43, Jan. 2021. https://doi.org/10.1109/JIOT.2020.2993601.

[6] J. Kim and N. Park, "Role-based Access Control Video Surveillance Mechanism Modeling in Smart Contract Environment", Transactions on Emerging Telecommunications Technologies, Vol. 33, No. 4, pp. e4227, Apr. 2022. https://doi.org/10.1002/ett.4227.

[7] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions", Computer Networks, Vol. 169, pp. 107094, Mar. 2020. https://doi.org/10.1016/j.comnet.2019.107094.

[8] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for Cybersecurity in Smart Grid: A Comprehensive Survey", IEEE Transactions on Industrial Informatics, Vol. 17, No. 1, pp. 3-19, Jan. 2020. https://doi.org/10.1109/TII.2020.2998479.

[9] I. Colak, R. Bayindir, and S. Sagiroglu, "The Effects of the Smart Grid System on the National Grids", 2020 8th International Conference on Smart Grid (icSmartGrid), Paris, France, Jun. 2020. https://doi.org/10.1109/icSmartGrid49881.2020.9144891.

[10] S. Shin and C. K. Suh, "The Influence of Quality and Satisfaction on the Quality Data Sharing of Mobile Telecommunication Service", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 18, No. 4, pp. 61-72, Aug. 2018. https://doi.org/10.7236/JIIBC.2018.18.4.61.

[11] J. Kim and N. Park, "De-Identification Mechanism of User Data in Video Systems According to Risk Level for Preventing Leakage of Personal Healthcare Information", Sensors, Vol. 22, No. 7, Mar. 2022. https://doi.org/10.3390/s22072589.

[12] Q. N. Minh, V. H. Nguyen, V. K. Quy, L. A. Ngoc, A. Chehri, and G. Jeon, "Edge Computing for IoT-Enabled Smart Grid: The Future of Energy", Energies, Vol. 15, No. 17, pp. 6140, Aug. 2022. https://doi.org/10.3390/en15176140.

[13] J. Kim, M. Kim, and Y. Park, "Blockchain-based Smart Meter Authentication Protocol in Smart Grid Environment", Journal of Korea Society of Industrial Information System, Vol. 28, No. 5, pp. 41-54, Oct. 2023. https://doi.org/10.9723/jksiis.2023.28.5.041.

[14] S. Yoo, "A Study on Consensus Algorithm based on Blockchain", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 19, No. 3, pp. 25-32, Jun. 2019. https://doi.org/10.7236/JIIBC.2019.19.3.25.

[15] J. Kim and N. Park, "A face image virtualization mechanism for privacy intrusion prevention in healthcare video surveillance systems", Symmetry, Vol. 12, No. 6, pp. 891, Jun. 2020. https://doi.org/10.3390/sym12060891.

[16] Korea Internet and Security Agency, "Smart Energy Cybersecurity Guide", 2019.

[17] D. Lee and N. Park, "Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance", Supercomputing, Vol. 73, No. 3, pp. 1103-1118, Aug. 2016. https://doi.org/10.1007/s11227-016-1841-5.

[18] J. Kim and N. Park, "Blockchain-Based Data-Preserving AI Learning Environment Model for AI Cybersecurity Systems in IoT Service Environments", Applied Sciences, Vol. 10, No.14, pp. 4718, Jul. 2020. https://doi.org/10.3390/app10144718.

[19] Y. N. Cao, Y. Wang, Y. Ding, Z. Guo, Q. Wu, and H. Liang, "Blockchain-empowered security and privacy protection technologies for smart grid", Computer Standards & Interfaces, Vol. 85, pp. 103708, Apr. 2023. https://doi.org/10.1016/j.csi.2022.103708

[20] W. Zhao, Q. Qi, J. Zhou, and X. Luo, "Blockchain-Based Applications for Smart Grids: An Umbrella Review", Energies, Vol. 16, No. 17, pp. 6147, Aug. 2023. https://doi.org/10.3390/en16176147

[21] J. Gao, K. O. Asamoah, Q. Xia, E. B. Sifah, O. I. Amankona, and H. Xia, "A Blockchain Peer-to-Peer Energy Trading System for Microgrids", IEEE Transactions on Smart Grid, Vol. 14, No. 5, pp. 3944-3960, Jan. 2023. https://doi.org/10.1109/TSG.2023.3237624.

저자소개

김 진 수 (Jinsu Kim)

2019년 9월 ~ 현재 : 제주대학교 융합정보보안학협동과정 박사과정
2018년 9월 ~ 현재 : 제주대학교 사이버보안인재교육원 연구원
관심분야 : 클라우드, 지능형 영상감시 시스템, IoT

박 남 제 (Namje Park)

2008년 2월 : 성균관대학교 컴퓨터공학과(공학박사)
2003년 4월 ~ 2008년 12월 : ETRI 정보보호연구단 선임연구원
2009년 1월~ 2010년 8월 : UCLA Post-Doc., ASU Research Scientist
2010년 9월 ~ 현재 : 제주대학교 교육대학 초등컴퓨터교육전공 교수, 대학원 융합정보보안협동과정 교수
관심분야 : 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드