안전한 스마트그리드 환경을 위한 정보보호 기법 연구

A Study on Information Protection Technique for Secure Smart Grid Environment

조 도 은*, 김 시 정**
목원대학교*, 한남대학교**

Do-Eun Cho*, Si-Jung Kim**
Mokwon Univ.*, Hannam Univ.**

요약

스마트 그리드의 현대화에 따라 가용한 개인 정보의 상세 수준뿐만 아니라 개인정보의 수립 사례, 사용 및 유출의 수준이 점차 높아지고 있다. 본 논문에서는 안전한 스마트 그리드 환경을 위하여 사용자와 정보 관리자, 정보공유자 사이의 개인정보 공유와 보호를 위한 기법을 제안한다. 본 논문에서 제안된 기법은 안전한 스마트 그리드의 서비스 제공과 함께 스마트 그리드 추진의 활성화에 도움이 될 것으로 기대한다.

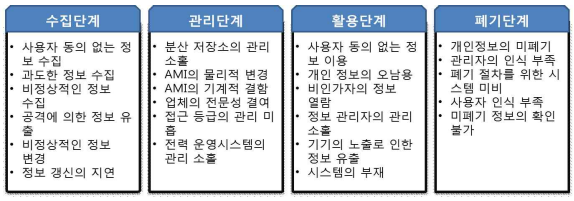
Ⅰ. 서론

최근 그린 IT에 대한 관심이 고조되면서 이를 실현하기 위한 주요 기술의 하나로 스마트 그리드가 주목을 받고 있다. 하지만 스마트 그리드는 에너지 효율을 크게 높이고, 여러 가지 부가서비스를 제공하지만 동시에 사생활 침해의 우려도 있다[1]-[2]. 소비자들의 상세한 전력 사용 내역이 스마트그리드의 기반기술인 AMI(Advanced Metering Infrastructure)를 통하여 자동 전송됨에 따라 개인 정보의 유출 가능성이 발생될 수 있다. 또한 점점 자동화 되어가는 스마트 그리드 환경에서 가용한 개인정보의 상세 수준뿐만 아니라 개인정보의 수집사례, 사용 및 유출의 수준이 더욱 높아지고 있다[3]. 본 논문에서는 안전한 스마트 그리드 환경을 위하여 사용자와 정보관리자, 정보공유자 사이의 개인정보 공유와 보호를 위한 기법을 제안하였다.

논문의 구성은 다음과 같다. 먼저 2장에서는 관련연구로 스마트 그리드 환경과 개인정보의 보안 취약점을 살펴보고, 3장에서는 개인정보보호 기법을 제안한다. 4장에서는 제안 기법의 안전성을 분석하고, 끝으로 5장에서 결론을 맺는다.

Ⅱ. 관련연구

스마트 그리드를 통해 고객은 기존 서비스와 융합된 새로운 서비스를 제공받을 수 있게 된다. 하지만 이러한 서비스를 제공받기 위해서 고객은 자신의 정보를 서비스 업체에 공개해야 하며, 이 경우 자신이 원하지 않는 정보까지 노출될 수 있는 위험이 있다. 또한 제공받은 정보를 서비스 업체가 제대로 관리하지 않을 경우 사용자의 정보가 악용될 소지가 있다. 따라서 스마트 그리드는 개인정보 수집 단계, 저장 및 관리 단계 그리고 이용 단계와 정보의 폐기 단계에서 개인 정보 보안에 많은 취약점을 가지고 있다[4]-[5]. 그림 1은 스마트 그리드 환경에서 개인정보 유출에 대한 보안 위협을 나타낸 것이다.

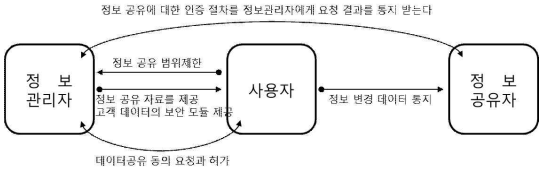


▶▶ 그림 1. 개인정보 유출에 대한 보안 위협

Ⅲ. 제안하는 안전한 정보 보호 기법

3.1 개인 정보 수집 단계

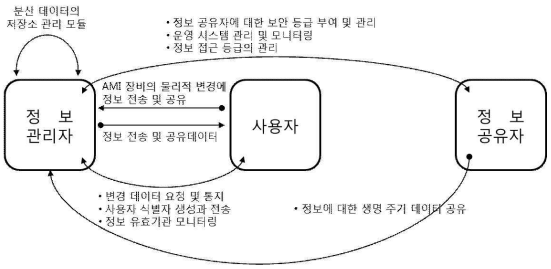
스마트 그리드 환경에서 사용자는 스마트 기기를 통하여 전력 사용량, 스마트 미터 정보, 동적 요금제에 대한 고객의 서비스 이용 정보 그리고 홈 기기의 사용 및 상태 정보 등과 같은 다양한 개인 정보를 생성하게 되고, 이를 전력 회사와 부가 서비스 업체와 공유 하게 된다. 따라서 사용자는 사용 등록 시 개인정보 공개 범위와 이용 범위 그리고 기기들의 접근 여부를 선택 하도록 하여 비인가된 사용자의 접근과 정보 공유에 대한 제한을 설정해야 한다. 그림 2는 사용자 등록 시 개인정보 보안 설정과 개인정보 수집 단계에 대한 흐름도이다.



▶▶ 그림 2. 개인정보 수집 단계 흐름도

3.2 개인 정보 관리 단계

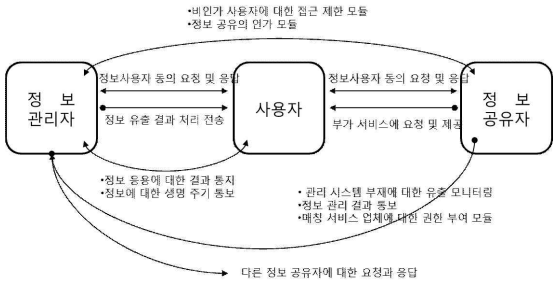
정보 관리자는 분산된 DB에 정보를 저장하고, DB에 저장된 정보에 유효기간을 설정한다. 또한 유효기간 관리에 대한 정책을 수립하고, 정보에 대한 접근 절차와 접근과 인가에 대한 과정을 통하여 접근에 대한 유효성을 확인한다. 또한 침해 요소 분석을 통하여 정기적으로 시스템 유효성 검사와 AMI에 대한 유효성 검사를 실시한다. 그림 3은 개인 정보 관리 단계의 흐름을 나타낸 것이다.



▶▶ 그림 3. 개인정보 관리 단계 흐름도

3.3 개인 정보 활용 단계

개인 정보 활용 단계에서는 지속적인 정보 조회와 관리가 이루어지므로 개인정보에 대한 가장 많은 침해 요인이 존재 한다. 정보 활용에 있어서 정보 관리자는 반드시 사용자의 동의를 요청하고 정보를 제공하도록 한다. 이는 개인정보의 오남용을 막기 위한 절차이다. 개인 정보는 정당한 사용 목적이 아닌 각 기관의 필요에 의해 여러 형태로 가공되고 침해 될 수 있다. 사용자의 사용 동의 요청에 대한 정보의 범위는 사용자가 생성한 보안 모듈의 절차에 따른다. 그림 4는 개인정보의 활용의 단계를 나타낸 것이다.



▶▶ 그림 4. 개인정보 활용 단계 흐름도

3.4 개인 정보 폐기 단계

수집된 개인 정보는 지정된 유효기간에 따라 폐기 과정을 수행해야 한다. 하지만 폐기해야 하는 개인정보들이 기관의 목적이나 공공의 활용을 위하여 폐기되지 않고 계속적인 보관이 유지 될 수 있다. 이는 관리자의 인식 부족이나 관리 소홀에 의해 이루어질 수 있다. 따라서 개인정보에 대한 목적 달성이 이루어진 후 반드시 폐기 과정을 수행해야 한다.

Ⅳ. 안전성 분석

스마트 그리드 환경에서 개인정보에 대한 흐름은 사용자에서 정보 관리자와 정보 공유자로 이루어지고 있다. 따라서 각 단계에서 수행되는 관리 기법에 대한 안전성은 먼저 사용자 측면에서 사용자가 자신의 개인정보에 대한 열람과 접근에 대한 제한을 설정하므로 비 인가된 사용자의 접근을 차단하게 된다. 또한 정보에 대한 갱신과 활용 그리고 폐기에 대한 정보를 정보 관리자에게 제공 받아 개인정보의 생명주기에 대한 명확한 정보 제공을 기대 할 수 있다. 정보 관리자는 소비자가 또 다른 소비자에 대한 정보 열람과 같은 취약점을 사용자의 동의 절차를 통해 정보 공유와 접근을 제한 한다. 이를 통하여 개인 정보에 대한 오남용을 줄이고 내부 사용자에 대한 접근 통제 장치의 대한 부재에 대한 대안을 제시한다. 또한 제3자의 정보 접근에 대하여 정보 제공에 대한 자료를 보관하고, 이를 사용자와 공유 하므로 개인 정보의 사용과 보유, 폐기여부에 대한 정보를 관리 할 수 있도록 한다. 이는 미폐기 보유를 통한 정보 유출 그리고 정보 보유 여부의 확인과 접근 불가의 정보에 대한 관리 문제를 해결 한다.

Ⅴ. 결론

본 논문에서는 스마트 그리드 환경에서 개인정보 보호 기법을 제안하였다. 스마트 그리드에서의 개인정보 보안 취약점은 무엇인지 살펴보고, 사용자에서 정보 관리자와 정보 공유자로 개인정보의 흐름을 분석하여 개인정보의 공유와 보호기법을 제안하였다. 제안된 기법은 안전한 스마트 그리드의 서비스 제공과 함께 스마트 그리드 추진의 활성화에 도움이 될 것으로 기대한다. 향후 안전한 스마트 그리드를 위해서 사용자의 접근 통제에 관한 경량 보안 시스템에 대한 지속적인 연구가 필요할 것이다.

■ 참 고 문 헌 ■

[1] Patrick McDaniel and Stephen McLaughlin, “Security and Privacy Challenges in the Smart Grid,” IEEE Security and Privacy, Vol. 7, No. 3, pp. 75-77, 2009.

[2] Do-Eun Cho, Si-Jung Kim, “Study on Safe Remote Control Method of Home Device under Environment of Smart Grid”, Lecture Notes in Electrical Engineering, Vol. 179, No. 2, pp. 281-286, 2012.

[3] Geun-Young Kim, Young-Myoung Kim, “Implementation of Telco Home Network-based AMI,” Journal of the Korean Institute of Information Scientists and Engineers, Vol.27, No.11, pp. 93-97, 2009.

[4] Rosslin John Robles and Tai-hoon Kim, “A Review on Security in Smart Home Development,” International Journal of Advanced Science and Technology(IJAST), Vol.15, pp. 13-22, 2010.

[5] NIST, “Smart Grid Cyber Security Strategy and Requirements,” DRAFT NISTIR 7628, 2010.