클라우드 기반 스마트 그리드 환경에서의 보안 이슈

이협건*, 이경화, 박민수, 신용태
*숭실대학교 컴퓨터학과
{hglee*, khlee, mspark}@cherry.ssu.ac.kr, shin*@ssu.ac.kr

Security Issues on Cloud Based Smart Grid

Hyeop-Geon Lee*, Kyoung-Hwa Lee, Min-Su Park, Yong-Tae Shin
*Dept. of Computer, SoongSil University

요 약

최근 큰 관심을 모으고 있는 스마트 그리드는 그린 에너지 환경 구현을 위한 기반 기술로 에너지 효율을 최적화하고자 하는 차세대 전략망이다. 스마트 그리드의 다양한 활용 가능성에도 불구하고 구조적 특징과 상호 운용성 표준의 부재로 인해 신뢰적인 인증을 보장하지 못한다. 이로 인해 네트워크의 신뢰성을 약화시키는 요인으로 작용하며, 많은 보안상의 문제를 야기한다. 따라서, 신뢰적인 클라우드 기반 스마트 그리드 환경을 구현하기 위하여 표준 및 정책 제정과 안전한 데이터 통신을 위한 보안 메커니즘 개발 및 인증 기술 개발이 필요하다. 본 논문에서는 클라우드 기반 스마트 그리드와 표준화 동향 및 클라우드 기반 스마트 그리드 환경에서의 보안기술을 살펴보고 이를 해결하기 위한 대안을 제시함을 목표로 한다.

1. 서론

스마트 그리드는 그린 에너지 환경 구현을 위한 기반 분야로서 국내외 다양한 표준기구 및 연구단체의 주도로 많은 연구개발이 진행 중이다. 또한 스마트 그리드는 에너지 효율성 향상을 목적으로 기존 전력망에 IT 기술을 도입・융합하여 전력공급자와 사용자 간의 양방향 통신을 제공한다. 이로 인해 실시간 데이터를 교환함으로써 지능화된 전력 에너지의 송・배전이 가능하다[1].

그러나 스마트 그리드의 구조적 특징과 상호 운용성 표준의 부재는 데이터의 보호 및 인증 관점에서 네트워크 신뢰성을 저하시키는 요인으로 작용한다. 따라서 스마트 그리드의 안전한 서비스 제공 및 보안 응용 서비스의 출현을 위하여 상호 운용성 표준 및 정책 제정과 안전한 데이터 통신을 위한 보안 메커니즘 개발 및 인증 기술 개발이 필요하다.

본 논문에서는 클라우드 기반 스마트 그리드와 표준화 동향 및 클라우드 기반 스마트 그리드 환경에서의 보안기술을 살펴보고, 클라우드 기반 스마트 그리드 환경에서의 인프라, 시장과 정책 보안 이슈를 제시한다.

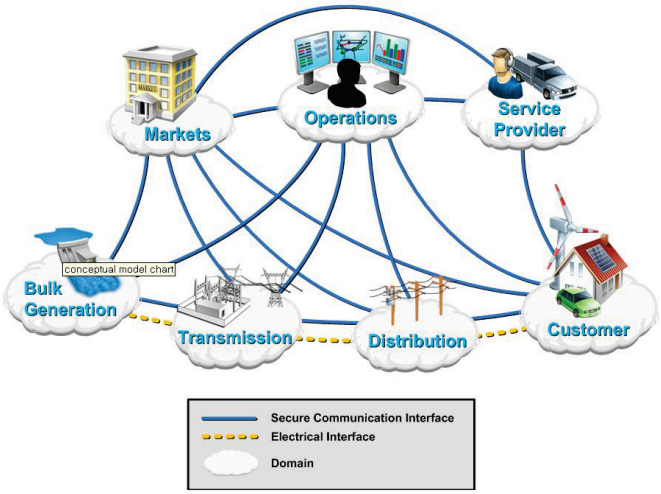
본 논문의 구성은 다음과 같다. 2 장에서는 클라우드 기반 스마트 그리드 및 표준화 동향을 살펴본다. 3 장에서는 클라우드 기반 스마트 그리드 환경에서 적용 가능한 보안기술을 살펴본다. 4 장에서는 클라우드 기반 스마트 그리드 환경에서의 보안 이슈를 제시한다. 마지막 5 장에서는 결론을 맺는다.

2. 클라우드 기반 스마트 그리드 및 표준화 동향

2,1. 클라우드 기반 스마트 그리드

클라우드 기반 스마트 그리드는 스마트 그리드와 클라우드 컴퓨팅 기술을 융합한 새로운 기술이다.

스마트 그리드[1]는 기존 전력망에 IT 기술을 접목하여 전력 공급자와 소비자가 양방향으로 실시간 정보를 교환함으로써 에너지 효율을 최적화하고자 하는 차세대 전략망이다. (그림 1)은 스마트 그리드 구조를 나타낸다.

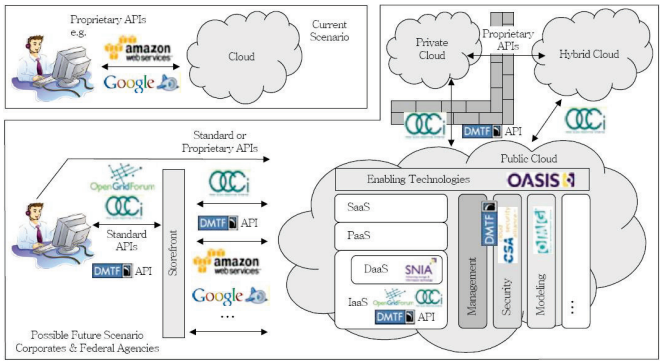


(그림 1) 스마트 그리드 구조

스마트 그리드[2]는 전력망 전체의 혁신을 통해 새로운 전력 공급 시스템 체계를 갖추는 것이 목적이다.

그리고 스마트 그리드는 전력 시스템과 IT 기술이 융합된 전력망의 진화된 형태이다. 전력망은 발전, 송전, 배전, 소비에 이르기까지 전력을 실어 나르는 모든 설비 및 기기를 의미한다.

클라우드 컴퓨팅[3]은 대용량의 확장 가능(Scalable)하고 가상화된(Virtualized) 자원들이 인터넷 상에서 서비스의 형태로 제공되는 컴퓨팅의 형태이다. (그림 2)는 클라우드 컴퓨팅의 개념적 구조를 나타낸다.



(그림 2) 클라우드 컴퓨팅의 개념적 구조

클라우드 컴퓨팅은 성능 향상, IT 개발 비용 절감, 스토리지 용량 확대, 유지 보수 비용 절감, 데이터 호환성 증가와 같은 많은 이점을 가진다. 그러나 민감한 데이터에 대한 직접 제어권은 얻기 힘들다. 또한 보안 문제가 발생시 피해의 파급효과가 크기 때문에 기업 비밀 관리나 개인의 프라이버시 측면에서 많은 문제점이 있다[4].

2.2. 클라우드 기반 스마트 그리드 표준화 동향

스마트 그리드의 표준화는 아직 초기 진행 상태이다. 각 국에서는 스마트 그리드에 대한 상호 운용성 표준을 추진하고 있다. 미국은 EPRI(European Parliaments Research Initiative)와 NIST(National Institute of Standards and Technology)를 중심으로 스마트 그리드의 상호 운용성 표준화를 주도하고 있으며, 유럽은 ETP(European Technology Platform, Smart Grids)를 중심으로 표준화를 진행하고 있다.

<표 1>은 각 국에서의 기술분야별 표준화 추진 동향을 나타낸다.

<표 1> 기술분야별 표준화 추진 동향

기술분야	표준내용	표준화 단체
지능형 전력관리 기술	스마트 그리드 인프라를 위한 Wibro 기술	IEEE 802.16
	스마트 그리드와 마이크로 그리드 연동	ISO/IEC
	지능형 에너지 관리 시스템과 전력 소비량수집 네트워크 간 인터페이스	OpenAMI, IEEE
	스마트 그리드 기기/시스템의 상호 호환	IEC TC57
지능형 전력망 보안기술	스마트 그리드 기기/시스템 보안	IEEE 1686-2007, UCAlug AMI-SEC SSR
	스마트 그리드/인프라 보안	NERC CIP 002-009
	스마트 그리드에서의 데이터 통신 보안	IEC 62351
	스마트 그리드 개인 정보 보안	NIST SP, NERC CIP
정책	전력 IT 시스템 자율 관리 정책	TTA, 기술표준원
	전력에너지 사용량 기반 전력절감 관리 정책	

3. 클라우드 기반 스마트 그리드 환경에서의 보안기술

현재까지의 전력망은 폐쇄형, 단독망 운영관리로 보안이 크게 문제 되지 않는 구조이다. 그러나 클라우드 기반 스마트 그리드는 정보통신 네트워크 기기에서 발생하고 있는 보안 문제가 나타난다. 이 절에서는 클라우드 기반 스마트 그리드 환경에서의 대표적인 보안 기술 중 사용자 인증과 접근 제어, 데이터 암호화, 네트워크 보안 기술, 가용성 및 복구에 대해 살펴본다[5].

3.1. 사용자 인증과 접근 제어

클라우드 기반 스마트 그리드는 다수의 사용자의 데이터가 혼재되어 있다. 그러므로 사용자 인증과 접근 제어기술이 필요하다. 사용자 인증과 접근 제어 기술은 OASIS 의 SAML(Security Assertion Markup Language)과 SSO(Single-Sign ON)이 있다.

3.2. 데이터 암호화

개인 및 기업 데이터에 대한 기밀성(Privacy) 보호를 위해서는 기본적으로 암호화(Encryption) 기술이 제공되어야 한다. 데이터 암호화 기술은 RSA(Rivest-Shamir-Adleman), AES(Advanced Encryption Standard)과 DES(Data Encryption Standard) 등이 있다.

3.3. 네크워크 보안

클라우드 기반 스마트 그리드 환경은 네트워크 기반이다. 네트워크 보안 기술은 IDS(Intrusion Detection System), IPS(Intrusion Prevention System), Firewall, IPsec(Internet Protocol Security protocol)과 VPN(Virtual Private Network) 등이 있다.

3.4. 가용성 및 복구

서비스의 중단이나 데이터의 손실을 막기 위해서는 서비스를 지속할 수 있는 고장 감내성(Fault Tolerance) 및 데이터 복구(Recovery) 기술이 필요하다.

<표 2>는 앞서 설명한 클라우드 기반 스마트 그리드 환경에서의 보안기술을 정리한 내용을 나타낸다.

<표 2> 클라우드 기반 스마트 그리드 환경에서의 보안 기술

구분	보안기술	특징
사용자 인증, 접근 제어	SAML	보안 표준 언어
	SSO	단일 사용 승인
데이터 암호화	RSA	비대칭키 암호화 알고리즘
	AES	대칭키 암호화 알고리즘
	DES	대칭키 암호화 알고리즘
네트워크 보안	IDS	침입탐지시스템
	IPS	침입방지시스템
	Firewall	외부와 신뢰적 통신
	IPsec	인터넷 보안 프로토콜
	VPN	가상 사설망
가용성, 복구		고장 감내성, 데이터 복구

4. 클라우드 기반 스마트 그리드 환경에서의 보안 이슈

클라우드 기반 스마트 그리드 환경에서의 보안 이슈는 크게 인프라, 시장, 정책으로 구분할 수 있다.

4.1. 인프라 측면에서의 보안이슈

4.1.1. AMI(Advanced Metering Infrastructure) 영역

AMI 는 최종 소비자와 전력회사 사이의 전력서비스 정보화를 위한 인프라이다. AMI 는 스마트 그리드 구현에 필요한 핵심적인 인프라으로서, 공급자・수요자 상호 인지 기반의 수요반응(DR) 실현을 위한 핵심 수단이다. 또한 AMI 는 스마트 미터 시스템을 통하여 일정시간마다 디지털 방식으로 정보를 기록하며, 스마트 그리드 기반 통신망을 통해 유틸리티 등의 사업자와 통신을 한다. 스마트 미터기는 수요반응 프로그램의 핵심기술로서 스마트 그리드에서 매우 중요한 역할을 한다. AMI 영역에서의 보안 이슈는 스마트 미터기의 보안 취약성(vulnerability of smart meter), 스마트 미터기에서의 프라이버시(privacy in smart meter)와 스마트 미터기에 대한 접근통제(access control of smart meter)가 있다.

4.1.2. 데이터 통신망 영역

클라우드 기반 스마트 그리드는 고속 양방향 통신이 가능한 광통신, 광대역 전력선 통신(Broadband over Powerline Communcations, BPL), 이동통신 및 위성 통신 등 광범위한 통신이 적용된다. 따라서 클라우드 기반 스마트 그리드에서의 다양한 통신 기술의 사용은 보다 신속하고 안정적인 통신을 제공함으로써 다른 IT 기술과 융합할 수 있다. 데이터 통신망 영역에서의 보안 이슈는 유・무선 통신 네트워크에서의 취약성과 전력선 기반 통신에서의 셀 보안 취약성이 있다.

4.1.3. 서비스 제공 사업자 영역

서비스 제공 사업자 영역은 클라우드 기반 스마트 그리드에서 서비스를 제공하는 사업자의 영역이다. 이 영역에서는 전송받은 사용자의 데이터를 저장・처리・이용함으로써 서비스 제공사업자가 사용자에게 여러 가지 서비스를 제공한다. 서비스 제공 사업자 영역에서의 보안 이슈는 사용자 데이터의 소유권(ownership of user data), 사용자 데이터에서의 프라이버시(privacy in user data), 사용자의 전력사용에 대한 통제(control over power usage), 저장된 사용자 데이터에 대한 접근통제, 사용자 데이터의 파기의 보장, 사용자 데이터 처리 및 제 3 자 제공 등의 이용에 대한 고지 및 동의가 있다.

4.2. 시장 측면에서의 보안이슈

국내 기업의 기술 및 자금력은 글로벌 외국 기업에 비해 부족하다. 보안 신기술을 보유한 외국의 선두업체들로부터 국내 시장 잠식 위협을 가지고 있다. 시장 측면에서의 보안 이슈는 클라우드 기반 스마트 그리드의 보안 신기술 솔루션 개발 능력이 취약한 국내 사업자들을 지속적인 지원을 통한 선진국과의 기술격차 해소가 있다.

4.3. 정책 측면에서의 보안 이슈

사용자는 개인 프라이버시 정보 및 기업 내 중요한 자산(정보, 문서, 금전 등)들을 악의적인 목적을 가진 제 3 자로부터 안전하게 보호하고 관리하는 정보보호 기술의 필요성에 대한 인식이 크게 증가하고 있다. 이로 인해 현대사회에서는 원천기술 및 산업체에서 활용되고 있는 상용기술 개발과 더불어 해당 기술에 대한 지적재산권(IPR) 확보를 위한 국내 및 국제 표준 개발이 중요하다. 정책 측면에서의 보안 이슈는 개인정보보호 및 고객정보보호 등을 위한 법제 정비와 클라우드 기반 스마트 그리드 보안을 위한 표준 제정이 있다.

<표 3>은 앞서 설명한 클라우드 기반 스마트 그리드 환경에서의 보안 이슈를 정리한 내용을 나타낸다.

<표 3> 클라우드 기반 스마트 그리드 환경에서의 보안 이슈

구분		보안 이슈
인프라	AMI	・스마트 미터기의 보안 취약성 ・스마트 미터기에서의 프라이버시 ・스마트 미터기에 대한 접근통제
	데이터 통신망	・유・무선 통신 네트워크에서의 취약성 ・전력선 기반 통신에서의 셀 보안 취약성
	서비스 제공 사업자	・사용자 데이터의 소유권 ・사용자 데이터에서의 프라이버시 ・사용자의 전력사용에 대한 통제 ・저장된 사용자 데이터에 대한 접근통제 ・사용자 데이터의 파기의 보장

		· 사용자 데이터 처리 및 제 3 자 제공 등의 이용에 대한 고지 및 동의
시장		· 선진국과의 기술격차 해소
정책		· 개인정보보호 및 고객정보보호 등을 위한 법제 정비 · 클라우드 기반 스마트 그리드 보안을 위한 표준 제정

5. 결론

본 논문에서는 클라우드 기반 스마트 그리드의 표준화 동향 및 보안기술을 살펴보고, 클라우드 기반 스마트 그리드 환경에서의 인프라, 시장과 정책 측면에서의 보안 이슈를 제시하였다. 스마트 그리드의 다양한 활용 가능성에도 불구하고 구조적 특징과 상호운용성 표준의 부재로 인해 신뢰적인 인증을 보장하지 못한다. 이로 인해 네트워크의 신뢰성을 약화시키는 요인으로 작용하며, 많은 보안상의 문제를 야기한다

따라서 향 후, 클라우드 기반 스마트 그리드 환경에서의 상호 운용성 표준 및 정책 제정과 안전한 데이터 통신을 위한 보안 메커니즘 개발 및 인증 기술 개발이 필요하다.

참고문헌

[1] Report to NIST on the Smart Grid Interoperability Standards Roadmap, D.V. Dollen, Electric Power Research Institute (EPRI), 2009.

[2] Standards Identified for Inclusion in the Smart Grid Interoperability Standards Framework, Release 1.0. National Institute of Standards and Technology, http://www.nist.gov/smartgrid/standards.html.

[3] Gartner says cloud computing will be as influential as E-business, http://www.gartner.com/it/page.jsp?id=707508.

[4] Armbrust, M., A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, Above the clouds: A Berkeley view of cloud computing. University of California, Berkeley, Tech. Rep, 2009.

[5] NIST. Smart Grid Cyber Security Strategy and Requirements, 2 Feb 2010. http://www.itl.nist.gov/div893/csrc/publications/drafts/nistir-7628/draft-nistir-7628_2nd-public-draft.pdf.