정 보 보 호 학 회 지
제26권 제1호, 2016. 2

스마트그리드 개인정보보호를 위한 정책적 고려사항

이 동 혁*, 박 남 제*,**

요 약

지난 수년간 주요 선진국들은 스마트그리드의 도입을 적극적으로 추진하여 왔으며, 이에 대한 연구도 많이 진행된 상황이다. 스마트그리드의 활성화를 위해서는 개인정보보호에 대한 대책이 필수이며 이를 기반으로 사용자에게 신뢰성 있는 서비스가 제공되어져야 한다. 이러한 서비스 제공을 위해서는 개인정보보호에 대한 기술적인 부분만이 아니라 정책적인 부분도 동시에 고려되어야 한다. 본 고에서는 스마트그리드에서의 안전한 개인정보보호 정책 수립을 위한 고려사항에 대하여 살펴본다.

Ⅰ. 서 론

스마트그리드는 새롭게 진화하는 차세대 지능형 전력망이다. 지난 수년간 여러 국가에서 스마트그리드의 보급을 적극적으로 주도하여 왔으며, 기술적 및 제도적으로 많은 연구가 진행되어 왔다.

스마트그리드의 보급에 있어 우선적으로 고려시되어야 할 부분은 개인정보보호이다. 이는 전통적인 보안의 관점과는 다르며, 서비스 제공자의 측면이 아닌 사용자의 측면에서 프라이버시를 보호할 기본 권리를 갖출 수 있도록 해야 한다는 관점에서 이해해야 한다.

스마트그리드 환경은 기존의 환경보다 더욱 많은 정보들이 노출될 수 있다. 특히, 에너지 소비량 뿐만 아니라, 스마트 기기 등으로 다양하고 구체적인 정보가 노출될 수 있다. 이러한 점은 정보가 결합되면 더욱 많은 정보에 대한 노출이 가능해진다는 측면에서 매우 위험할 수 있다.

그동안 스마트그리드의 개인정보보호 분야에 있어서도 많은 연구가 진행되어 왔으며, 제도적인 부분에 있어서도 확립이 되고 있는 단계이다. 개인정보는 서비스 제공자 및 제3자가 취급하게 되며, 각 서비스 제공자 및 제3자는 이러한 부분을 충분히 고려하여 개인정보보호 정책을 수립할 필요가 있다.

본 고에서는 NIST의 연구내용[1]을 중심으로 스마트그리드 환경에서 사용자의 프라이버시를 보호하기 위한 정책적 고려사항을 설명하고자 한다.

Ⅱ. 스마트그리드 프라이버시

2.1. 개요

‘프라이버시(privacy)’라는 용어는 보편적이고 국제적으로 통용되는 정의를 가지지 않으며, 개인마다 다양한 의미를 가질 수 있다. 가장 기초적으로 정의하자면 프라이버시는 혼자 남을 권리로 볼 수 있다. 프라이버시는 평이하게 묘사되는 개념이 아니며, 법률이나 규정으로 제공되는 사양에 국한되는 것도 아니다. 또한, 프라이버시는 기밀성과 같은 관점에서 볼 수 없다.

개인정보(personal information)는 기밀정보(confidential information)와 동일한 것이 아니다. 기밀정보는 사업상 알 필요성이 있거나 조회의 권한을 가지고 있는 자에 한해서만 액세스가 제한되고 부적절하게 공유될 경우에 시스템, 데이터, 애플리케이션 또는 다른 사업적 기능을 침해할 수 있는 정보이다.

프라이버시는 보안(security)과 자주 혼동되기도 한다. 두 용어의 정의는 많은 부분 중복되지만, 서로 구분

이 연구는 2013년도 정부(교육부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호:2013R1A1 A4A010 13587).

* 제주대학교 일반대학원 컴퓨터교육전공 박사과정 (bonfard@jejunu.ac.kr)
** 제주대학교 교육대학 초등컴퓨터교육전공 교수 (namjepark@jejunu.ac.kr, 교신저자)

되는 개념들이다. 프라이버시가 없는 보안은 있을 수 있으나, 보안이 없는 프라이버시는 있을 수 없다. 보안은 프라이버시를 구성하는 요소 중 하나이다. 보안은 기밀성, 무결성, 데이터 가용성을 보장한다. 그러나, 프라이버시는 적절한 인증 및 유사한 보호조치를 갖춘다는 수준을 넘어선다. 수집된 목적에 따라서만 데이터를 사용하고 그 목적이 충족되어 더 이상 필요하지 않게 된 데이터는 적절히 처분해야 한다.

스마트그리드의 프라이버시에 관한 고려사항에 개인(individual)의 권리, 가치, 이익을 검토하는 과정을 포함시키는 것은 중요하다. 여기에는 관련 특징, 활동, 개인의 의견이 개입되어 있다. 데이터 프라이버시는 개인 데이터를 공급하는 소비자와 이 데이터를 수집 또는 취급하는 모든 주체의 관행으로부터 영향을 받는다.

2.2. 스마트그리드에서의 개인정보보호

스마트그리드 기술의 배포에 관련된 주된 개인정보보호 문제는 최신 전기 계기와 이에 관련된 장치 및 기술의 설치가 개인의 에너지 소비 및 생산의 성격과 빈도에 관해 보다 세부적인 개인 식별 데이터를 수집, 전송 및 유지를 초래한다는 점이다. 이러한 우려는 이러한 유형의 데이터가 개인 소비자 또는 위치에 관련될 때에 제기된다. 공공시설은 수십 년 동안 에너지 소비 및 개인 청구 데이터를 통상적으로 수집해 왔다. 최신 계측 인프라에 관해 새롭게 제기되고 있는 개인정보보호 문제는 계측기에서 빈번하고 상세하게 수집되는 에너지 사용 데이터로부터 행동적 추론이 가능하다는 점이다. 또한, 스마트미터는 데이터는 수동 계측기 판독 및 수집이 아닌 전자적으로 수집 및 전송함으로써 방법론상의 감시 문제를 제기한다.

특정 가전기기 또는 소비자 패턴을 파악할 수 있는 능력은 계측기가 정보를 수집하는 빈도와 계측기가 수집하는 데이터가 무엇인지에 따라 달라진다. 에너지 사용 데이터를 자주 수집하게 되는 경우에는 주거지 또는 기타 부지에서 일어나는 활동에 관한 정보를 추론하기가 과거보다 쉬워질 수 있다.

Ⅲ. 개인정보보호 취약요소

스마트그리드의 특성상 개인정보는 더욱 다양하게 노출될 수 있다. 원활한 서비스 제공을 위해서는 최소한의 개인정보의 취급은 필수불가결하나, 이를 안전하게 관리한다는 전제가 반드시 필요하다. 본 장에서는 스마트그리드 개인정보보호의 취약요소를 분석한다.

3.1. 개인정보 노출 범위

스마트그리드에서 다루어야 할 개인정보보호우려는 방대하게 존재한다. 이는 스마트그리드 시스템의 구현이나 효용성에 영향을 미칠 수 있다. 예컨대, 에너지 소비 데이터의 보안 및 개인정보보호에 관한 소비자 신뢰의 결여는 전면적인 소송전은 아닐지라도 소비자 수용성 및 참여의 결여를 초래할 수 있다.

일반적으로, 스마트그리드에 관한 개인정보 노출은 다음의 두 가지 범위 중 하나에 속한다.

⊙ 기존에는 쉽게 수집할 수 없었던 개인정보의 획득
⊙ 기존에도 개인정보 수집이 가능했던 정보에 대한 새로운 정보 획득

첫 번째 범위의 예시로는 해당 위치의 합법적 및 불법적 작동 시기와 개인적 패턴을 나타내는 특정 의료기기 및 전자기기의 사용에 관한 정보, 각 가전기기와 측정 위치에서의 전력 소비에 관한 세분화된 시계열 데이터를 비롯하여 주어진 위치에서 사용 중인 가전기기 및 장비에 관한 상세 정보를 들 수 있다.

두 번째 범위는 개인정보가 다른 출처에서 제공되고 스마트그리드가 이 정보의 새로운 출처가 되는 경우가 속한다. 예컨대, 개인의 물리적 위치는 오늘자 신용카드와 휴대전화 기록으로 추적할 수 있다. 전기자동차 충전의 경우에는 새로운 에너지 소비 데이터를 통한 물리적 위치의 추적 가능성이 제기된다.

집 또는 건물 안에서의 활동의 상세 내역은 기기 전자서명과 시간패턴으로 추론할 수 있다. 이러한 서명과 패턴은 소유자의 활동에 대한 파악의 근거가 될 수 있다.

3.2. 행동 유형별 취약요소

3.2.1. 개인정보의 노출

개인정보가 노출되는 경우는 일반적인 시스템 환경에

서도 공통적으로 가지고 있는 문제이다. 그러나 스마트그리드 환경에서는 에너지 소비량과 같은 스마트그리드에 특화된 데이터가 존재한다. 기존에도 개인정보의 노출 자체는 가능하였으나 기존의 전력 환경에서는 데이터 조작 또는 노출 가능성이 비교적 낮은 편이었다. 그렇지만 스마트그리드 환경에서는 스마트미터나 스마트기기에 따른 새로운 방식의 개인정보의 노출이 용이해지게 될 우려가 있다.

3.2.2. 개인의 행동패턴 · 사용기기 파악

홈 자동화 네트워크 또는 지원기술이 탑재된 스마트미터는 특정 가전기기의 사용 여부를 추적할 수 있다. 집의 특정 영역에서의 전기 사용 위치와 시기를 노출시킬 수 있는 데이터 사용 프로필은 작동되거나 사용된 가전기기의 유형을 노출시킬 수 있다. 이러한 정보는 가전기기 제조업체의 제품 신뢰성 및 품질 보증을 위해서, 혹은 표적 마케팅을 위해서 활용될 수 있다.

3.2.3. 실시간 원격감시 실시

실시간 에너지 사용데이터에 엑세스되는 경우, 어느 시설이나 주거지에 사람이 있는지 여부, 무엇을 하고 있는지에 대한 정보, 기상 및 수면 패턴, 건축물 내부의 어디에 위치하고 있는지, 몇 명이나 있는지에 대한 정보 등이 노출될 수 있다.

현재 여러 종류의 실시간 감시 방법이 존재하며, 에너지 사용 데이터를 토대로 향후에도 여러 가지의 감시 방법이 개발될 수 있다.

3.2.4. 상업적인 데이터 사용

소비자의 에너지 사용 데이터 저장은 광범위한 제품 및 서비스의 공급업자를 비롯한 다수의 업체에게 가치를 가지는 생활 방식 및 정보를 노출시킬 수 있다. 공급업자는 표적 판매 및 마케팅 캠페인에 유용한 속성 목록을 입수할 수도 있는데, 정작 대상은 이를 긍정적으로 생각하지 않는 경우가 많다. 보험 등의 목적으로도 데이터가 활용될 수 있을 것이다.

기존의 계측 시스템에서는 활동에 관한 상세 정보를 노출시킬 정도로 세부적인 파악은 어려웠으나, 스마트미터는 에너지 관리 분석 및 동종업계 비교를 위해 판매되고 사용될 수 있는 사용 시기, 수요, 장비의 직접 부하 제어에 관한 상세한 데이터를 생성하며, 이러한 정보는 제3자에게 유용하게 활용될 수 있을 것이다.

3.3. 데이터 유형별 취약요소

3.3.1. 에너지 사용 데이터

에너지 사용 데이터로 다양한 정보에 대한 파악이 가능하다. 집안에서의 개인의 행동 패턴과 활동, 수면, 샤워, TV시청과 같은 활동을 비롯하여 전기 사용 패턴과 가전기기 사용을 모니터링하여 파악할 수 있는 집안에서 일어나는 행동 패턴, 습관, 활동에 대한 정보가 노출될 수 있다. 또한, 실시간 에너지 사용 데이터를 통해 집안에 사람이 있는지 여부와 무엇을 하고 있는지, 집 안의 어디에 위치하고 있는지 등 실시간 행동에 대한 모니터링도 가능해진다는 우려가 있다.

3.3.2. 전기자동차의 충전 정보

전기자동차의 충전 정보를 통해 위치정보의 파악이 용이해진다. 즉, 이러한 정보는 전기자동차의 충전 이력을 통하여 마지막 충전 이후 사용범위를 파악하는데 사용될 수 있다. 따라서 이러한 정보는 사용자의 운전 습관 등에 대한 파악을 통하여 보험료 산정이나, 마케팅 등에 활용될 수 있다.

3.3.3. 소비자 소유의 장비

소비자 소유의 장비는 스마트 가전기기를 통해 직접적으로 파악이 될 수 있다. 이러한 정보는 손해사정(예를 들어, 기기가 주택 화재로 인해 파괴되었다고 주장할 경우), 위험을 증가시킬 수 있는 기기 존재시의 보험료 산정 등에 활용이 될 수 있다. 한편, 절도할 표적자산을 확인하는 행위, 개인정보를 수집하기 위해 바이러스 또는 기타 공격을 유입시키는 행위 등의 악의적인 목적으로 활용될 우려도 존재한다.

Ⅳ. 정보 취급시 정책적 고려사항

여기서는 NIST의 개인정보보호 실무지침 권고사항[1]을 기반으로 제3자에 대한 개인정보 취급시 고려사항에 대하여 살펴본다. 본 장에서 설명하는 고려사항은 개별적으로 고려될 경우에는 효과가 크지 않을 수 있으므로 종합적으로 고려되어야 할 것이다.

4.1. 개인정보보호 고지

에너지 사용 데이터를 공유하려는 제3자는 데이터 처리에 관한 사항 및 소비자의 허가 없이는 해당 데이터가 다른 제3자에게 공개되지 않을 것을 명시한 명확한 내용을 소비자에게 고지할 필요가 있다.

또한, 규정에 의해 조직 내에서 발생한 중대한 변화가 있을 경우, 이러한 부분이 제3자 또는 계약대리인에게 에너지 사용 데이터의 공개와 관련이 있을 경우에도 별도로 고지되어야 할 것이다.

고지는 소비자와 사업적 관계를 가지는 제3자가 작성해야 하며, 해당 트랜젝션에 직접적으로 관여하지 않는 주체는 별도로 고지를 전달할 필요는 없다.

4.2. 공개에 관한 소비자의 허가

개인정보는 소비자가 공개를 허가하지 않는 한 다른 제3자에게 공개해서는 안되며, 이러한 허가를 획득하는 과정에서 다른 제3자의 신원을 소비자에게 고지해야 한다. 제3자가 소비자의 허가를 구하고자 할 경우, 허가 절차 가운데 에너지 소비 데이터의 공개에 관해 소비자가 선택할 수 있는 범위를 명시해야 한다.

만약 소비자가 이미 허가한 서비스 또는 제품을 공급하거나, 소비자에 대한 기타 의무를 이행할 때에는 회사가 법률을 준수하는 한도 내에서는 별도로 소비자의 허가를 취득할 필요는 없다.

한편, 제3자는 소비자가 본인의 에너지 전력 소비 데이터에 대한 접근 권한을 가지고 데이터에 존재하는 부정확성의 시정을 요청할 수 있는 절차를 개발하고 소비자에게 알려야 한다. 데이터 접근 권한을 획득하기 위한 절차는 평균적인 소비자에게 비교적 간단한 절차가 되어야 할 것이다.

4.3. 정보 공개의 범위

제3자가 수집할 수 있는 에너지 사용 데이터는 소비자가 허가하는 특정한 목적을 이행하는 데 필요한 데이터로 한정하여야 한다. 만약, 기존에 허가된 목적과 다른 목적으로 사용하여야 할 경우는 별도로 소비자의 허가를 취득해야 한다.

4.4. 소비자 교육 및 인식

제3자는 제3자의 개인정보보호 정책 및 지침을 소비자에게 알려야 하며, 조직이 개인정보의 무단 사용에 관한 잠재적 위험을 완화하기 위해 취하는 조치를 요약하고 소비자가 본인의 위험을 완화하기 위해 취할 수 있는 조치를 설명한 교육 및 인식 자료를 소비자에게 제공할 필요가 있다.

한편, 에너지 소비 데이터는 기술, 시기 및 평가상의 차이와 같은 요인에 다소 차이가 발생할 수 있다는 점을 소비자에게 인식시킬 필요도 있다.

4.5. 정보 수집의 최소화

제3자에 의한 에너지 사용 데이터 수집은 서비스 또는 제품의 제공 등 소비자가 허가한 목적을 이행하는 데 필요한 정보에 국한되어야 한다. 만약 필요에 의해 수집된 데이터가 특정 시간 이후 필요성이 사라졌을 경우는 정책에 따라 폐기조치를 해야 할 필요가 있다.

4.6. 데이터 품질

에너지 사용 데이터를 사용하는 제3자 및 제3자 계약대리인은 데이터의 정확성과 완전성을 보장하기 위해 할 수 있는 최대한의 조치를 수행할 필요가 있다.

경우에 따라 제3자는 에너지 사용 데이터를 수정해야 하는 경우도 있을 것이다. 따라서 데이터의 정확성 및 완전성은 데이터를 제공받은 당시에 한한 것이라는 것을 염두에 두어야 한다.

4.7. 데이터 보안

제3자는 데이터 보안에 관한 정책, 절차 등을 통해 무

단 접근, 복사, 수정, 부적절한 공개, 또는 분실로부터 정보를 보호해야 하고, 제3자의 계약대리인 또는 다른 제3자에게 공개되는 데이터의 정확성을 보장해야 한다. 이러한 정책 또는 절차는 정기적으로 검토 평가가 이루어져야 하며, 에너지 사용 데이터를 적절히 처리할 필요성에 따라 갱신해야 한다. 또한, 제3자는 보안 및 개인정보보호정책을 적절하게 유지, 갱신 및 준수할 업무를 담당할 직위 및 직원을 배정하여야 한다.

4.8. 위험 평가

제3자는 제3자의 계약대리인에게 에너지 사용 데이터를 공개하는 절차에 대해 정기적인 영향 및 위험평가와 분석을 실시하고 문서화해야 한다. 해당하는 경우, 관련 정책 및 실무지침을 갱신하는 경우에도 개인정보보호 위험분석 및 영향평가를 실시해야 한다.

4.9. 데이터 보관 및 폐기

특별한 경우를 제외하고, 제3자는 수집 목적을 이행하는데 필요한 경우나 합리적으로 판단했을 때 법적 또는 규제적 요건을 준수해야 할 의무를 진 것으로 해석되는 경우를 제외하고는 에너지 사용 데이터를 보유하지 않아야 한다. 만약 에너지 사용 데이터가 연구용으로 사용될 경우, 이러한 활동에 관해 데이터를 보유 및 익명화할 정책 및 절차를 확립해야 할 필요가 있다.

또한, 데이터 보유 정책을 소비자 고지 형식으로 소비자에게 고지해야 하며, 수집 보유에 대한 허가를 철회한 이후에 데이터를 영구적으로 파기해야 하는 상황과 방법을 명시해야 할 필요가 있다.

4.10. 데이터 침해

제3자는 제3자 또는 계약대리인에게 적용될 수 있는 데이터 침해에 대한 제도적인 요건을 사전에 숙지해야 하며, 무단 침해가 발생하는 경우 정책에 따라 고지의 의무를 다해야 한다.

4.11. 직원 교육

제3자 및 제3자의 계약대리인은 문서화된 시행 절차와 함께 공식적으로 문서화된 보안 및 개인정보보호 인식/교육 정책을 개발, 배포하고 정기적으로 검토하고 갱신할 필요가 있다.

또한, 조직은 개인정보보호에 관한 기초 인식 교육을 비롯하여 각 직원의 보안 및 개인정보보호 교육에 대한 활동을 문서화하고 유지 및 모니터링 할 필요가 있다.

4.12. 감사

제3자는 개인정보보호 및 보안 실무지침에 대해 독립적으로 정기 감사를 실시할 필요가 있다. 또한, 개인정보보호 실무지침을 정기적으로 검증해야 한다.

Ⅴ. 결 론

안전한 스마트그리드 환경은 보안에 관한 부분 뿐만이 아니라, 개인정보보호에 대한 부분도 포함한다. 개인정보보호에 대한 신뢰성이 없는 시스템은 결국 사용자에게 부정적인 영향을 끼칠 것이며, 시스템의 도입에 있어 결정적인 실패 원인이 될 것이다.

본 고에서는 스마트그리드 환경에서의 개인정보보호를 위하여 정책적인 고려사항을 살펴보았다. 이를 위해, 스마트그리드 프라이버시 개념과 취약점에 대하여 살펴보았고, 제3자에 의한 정보 취급시의 정책적인 고려사항에 대하여 분석해 보았다.

스마트그리드 개인정보보호를 위해 안전한 정책 수립은 매우 중요하며, 본 고에서 설명한 고려사항을 기반으로 보다 안전한 스마트그리드 정책 수립이 가능해 질 것을 기대해 본다.

참 고 문 헌

[1] NIST, "Guidelines for Smart Grid Cyber Security, Volume 2 - Privacy and the Smart Grid", U.S. Department of Commerce, pp. 291-473, Sep. 2014.

[2] Namje Park, Marie Kim, "Implementation of load management application system using smart grid privacy policy in energy management service environment", Cluster Computing, Springer, 17(3), pp. 653-664, Sep. 2014.

[3] Namje Park "Implementation of Privacy Policy-based Protection System in BEMS based Smart Grid Service", International Journal of Smart Home, pp. 91-100, Nov. 2013.
[4] P. Ohm, “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,” University of Colorado Law Legal Studies Research Paper, 57(9-12), pp. 1701, Aug. 2009.
[5] A. John, R. Peter, "Electric Communication Development", Communications of the ACM, 40, pp. 71-79, May 1997.
[6] Rebecca Herold, "Smart Grid Privacy Concerns", Oct. 2009.
[7] 강성규, 김신규, "스마트그리드 기기 보안 침해사고 대응을 위한 원격 증거 수집 시스템 설계", 정보보호학회논문지, 25(1), pp. 49-60, Feb. 2015
[8] 전용희, "사물인터넷(IoT) 기반 스마트 그리드 보안 특성 및 쟁점 분석", 정보보호학회지, 24(5), pp.59-65, Oct. 2014.
[9] 허옥, 김승주, "한국형 스마트그리드의 가용성을 고려한 정보보호 관리체계 평가 기준 제안", 정보보호학회 논문지, 24(3), pp. 547-650, Jun. 2014
[10] 이건희, 서정택, 박응기, "스마트그리드 보안위협 및 보안 요구사항 분석", 정보보호학회지, 21(7), pp. 7-17, Nov. 2011.
[11] 정교일, 박한나, 정부금, 장종수, 정명애,"스마트그리드의 안전성과 보안 이슈", 정보보호학회지, 22(5), pp. 54-61, Aug. 2012.
[12] 박남제, 안길준, "스마트그리드에서의 프라이버시 보호", 정보보호학회지, 20(3), pp.62-78, Jun. 2010.
[13] 곽지섭, 김완홍, 강순희, 김재성, "한국의 스마트그리드 보안현황과 사이버 보안 추진방향", 대한전기학회 학술대회 논문집, pp.1209-1210 Jul. 2010.
[14] 박남제 외, "지능형 전력장치를 활용한 스마트빌딩에서의 프라이버시 보안 가속화처리 및 관리기술 개발", 2013년 산학연공동기술개발사업 최종보고서, Jun. 2013.
[15] 이경복, 독고지은, 유지연, 이숙연, 임종인, "그리드에서의 소비자 참여와 보안 이슈", 정보보호학회지, 19(4), pp. 21-35, Aug. 2009.
[16] 박남제 외, "국내외 스마트그리드 개인정보보호 동향분석 및 개선방안 연구", 한국인터넷진흥원 위탁과제 최종보고서, KISA-WP-2015-0030, Nov. 2015.

〈저자소개〉

이 동 혁 (Donghyeok Lee)
정회원

2007년 2월 : 동국대학교 전자상거래기술전공 공학석사
2007년 6월~2008년 5월 : 한국전자통신연구원 정보보호연구단 연구원
2008년 11월~2015년 6월 : KT 플랫폼개발단 과장
2015년 9월~현재 : 제주대학교 컴퓨터교육전공 박사과정
<관심분야> 클라우드 보안, 스마트그리드 보안, 데이터베이스 보안

박 남 제 (Namje Park)
종신회원

2008년 2월 : 성균관대학교 컴퓨터공학과 박사
2003년 4월~2008년 12월 : 한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월~2009년 12월 : 미국 UCLA대학교 공과대학 Post-Doc,WINMEC 연구센터 Staff Researcher
2010년 1월~2010년 8월 : 미국 아리조나 주립대학교 컴퓨터공학과 연구원
2010년 9월~현재 : 제주대학교 교육대학 초등컴퓨터교육전공 교수
<관심분야> 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드 등