RESEARCH

KEPCO Journal on Electric Power and Energy
p-ISSN 2465-8111, e-ISSN 2466-0124
Volume 6, Number 4, December 2020, pp. 399-404
DOI 10.18770/KEPCO.2020.06.04.399

Guideline on Security Measures and Implementation of Power System Utilizing AI Technology

인공지능을 적용한 전력 시스템을 위한 보안 가이드라인

Inji Choi, Minhae Jang, Moonsuk Choi
최인지, 장민해, 최문석

Abstract

There are many attempts to apply AI technology to diagnose facilities or improve the work efficiency of the power industry. The emergence of new machine learning technologies, such as deep learning, is accelerating the digital transformation of the power sector. The problem is that traditional power systems face security risks when adopting state-of-the-art AI systems. This adoption has convergence characteristics and reveals new cybersecurity threats and vulnerabilities to the power system. This paper deals with the security measures and implementations of the power system using machine learning. Through building a commercial facility operations forecasting system using machine learning technology utilizing power big data, this paper identifies and addresses security vulnerabilities that must compensated to protect customer information and power system safety. Furthermore, it provides security guidelines by generalizing security measures to be considered when applying AI.

Keywords: *Cyber Security, Power System, AMI Big Data, Artificial Intelligence, Machine Learning, Security Guideline*

I. Introduction

A. 연구 배경

최근 전력 산업은 딥러닝 등의 새로운 기계학습 모델의 등장과 더불어 디지털 변환 추세가 가속화되고 있다. 분야별로는 지능형 전력망, 부하예측 및 수요반응, 에너지 거래, 설비 제어 및 진단 예측 분야에서 머신 러닝을 도입하여 전력 산업 전체의 효율성을 향상시키거나 생산성 및 안정화를 위한 노력을 기울이고 있다 [1]. 전력 분야에 AI를 적용하는 사례는 아직까지 전력 산업 전반의 효율 향상에 초점 맞춰져 있으나 최근 자체 생산한 데이터를 활용하여 상업화를 하려는 시도가 있다 [2]. 전력회사에서 보유 중인 빅데이터와 AI 기술을 융합하여 활용성을 극대화할 뿐만 아니라 이를 통한 신규 사업 확장을 도모하려는 것이다.

문제는 전통적인 영역에 존재하던 전력 산업에 최첨단 AI 시스템이 도입되면서 직면하는 보안 위협이다. 전력 시스템에 AI를 적용할 때에는 융복합 성격의 산업 특성을 보이기 때문에 새로운 보안 위협이나 취약점이 드러난다. 특히 신 비즈니스를 창출하고 상업화를 위한 시스템을 구축할 때에는 전력회사 소유의 데이터라 할지라도 고객 정보에 대한 민감성을 가지고 개인 프라이버시를 보호할 수 있어야 한다 [3][4]. 아울러 전력 산업에 AI를 적용한 정보 시스템을 구축할 때에는 물리적, 기술적, 관리적 차원에서의 보안 조치 후 시스템을 구축해야 할 법적 의무가 있다 [5].

지금까지 전력 IT, 스마트 그리드 등에 적용될 보안 정책 연구나 [6] AI 자체로 인한 보안 위협을 다룬 연구는 있었지만 [7]-[10], AI를 적용한 전력 시스템에 보안 정책을 구현한 사례는 드문 실정이다. 본 논문에서는 머신 러닝을 적용한 전력 시스템을 대상으로 보안 조치 연구 및 구현까지 다루고 있다. 그동안 전력 제어 시스템에 적용할 보안 정책 연구에는 구체적인 실증이 없었고, AI 서비스로 인한 보안 위험성 대비 전력 시스템에 적용한 사례가 부족하기에 본 연구의 필요성이 강조된다.

B. 연구 목표

본 논문에서는 전력 빅데이터를 활용한 상업시설 영업예측 시스템을 구축하며 고객 정보 보호는 물론 전력 시스템의 안전성을 위하여 경계해야할 보안 취약점들을 도출하고 전력 제어 시스템에 실제 구축한 보안적 조치결과를 보이고 있다. 더 나아가 전력 산업에 AI 기술을 적용할 때 고려할 보안 조치 사항을 일반화하여 보안 가이드 라인을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 먼저는 전력 빅데이터와 AI가 접목되었을 때 발생할 수 있는 개인 프라이버시 침해 및 시스템 보안 위협과 각각의 대응방안에 대한 선행 연구를 정리하고 분석

Article Information

Manuscript Received April 16, 2020, Revised May 14, 2020, Accepted May 20, 2020, Published online December 30, 2020

The authors are with KEPCO Research Institute, Korea Electric Power Corporation, 105 Munji-ro Yuseong-gu, Daejeon 34056, Republic of Korea.

Correspondence Authors: *Inji Choi* (*inji.choi@kepco.co.kr*), *Moonsuk Choi* (*freewill@kepco.co.kr*)

TABLE 1
생활패턴 예측 관련 선행 연구 분석

머신러닝 기법	보안 위협 특징	공격기법 평가	논문
정수 계획법	• 전력 사용량 데이터로부터 전기를 사용하는 생활 패턴을 예측하는 NIALM (Non-Intrusive Appliance Load Monitoring) 과정에 관한 연구 • 정수 계획법이라는 제한된 조건 안에서 최대한의 이익을 보는 방법을 찾아내는 수학적 기법을 사용함으로써 특정 상황에서 작동한 전기 기기의 사용 환경을 찾아냄	• 예측 성공률 60% 이상. 매우 높은 해상도의 데이터가 필요함 • 두 환경의 실험에서 예측 성공률의 차이가 크므로 다양한 환경에 안정적으로 적용할 수 있는 방법이라고 보기는 어려움	[7]
k-NN, SVM	• 센서로부터 appliance의 상세한 전기사용량 데이터를 수집해 NIALM 기법을 적용한 연구 • k-NN 기법과 SVM 기법을 적용해서 특정 전기 사용 기기가 전기를 사용하고 있는지 아닌지 아닌지를 개별적으로 판단	• 예측 성공률은 65%를 넘지만, 고해상도의 데이터가 필요 • 기법을 적용하기 위해서는 appliance 각각에 대해 상세한 전기사용량 데이터 필요	[8]
HMM	• HMM 기법을 사용해 전기사용량 데이터로부터 전기 기기의 사용 여부를 파악하는 연구 • 대표적인 전기 기기들의 전기사용량 모델은 일반적인 경우로 가정한 뒤, 전체 전기사용량 데이터에 맞춰 훈련을 시키는 방법을 사용	• 예측 성공률은 낮지 않지만, 전기사용량이 높은 세 개의 전기 기기를 제외하였기 때문에 실질적으로 다양한 전기 기기를 사용한 환경에는 적용이 어려움	[9]
NN	• 15분 주기로 수집한 저 해상도 전력 사용량 데이터로부터 주요 전기 기기 사용 패턴을 식별하는 연구 • NN 훈련에 사용하는 데이터를 전처리하는 과정에서 데이터들을 비지도 학습 기법으로 분류하고 목표로 하는 주요 전기 기기가 포함된 데이터들만을 학습에 포함함	• 사용하고 있는 전기 기기의 종류에 대해 자세히 파악하는 정밀도는 낮음 • 전체적인 예측 정확도 또한 약 72%로 높지 않음	[10]

한다. 다음으로 한국전력공사의 전력사용량(AMI) 빅데이터를 활용한 상업시설 영업예측 시스템에 적용된 머신러닝 기술과 시스템 요소들을 소개한다. 이후 모의 해킹을 통해 실제 전력 설비와 접목하면서 드러나는 보안 취약점을 도출해 낸다. 마지막으로 실제 구축을 하면서 취한 보안 조치와 보안 정책을 종합하여 AI를 전력 시스템에 적용했을 때 고려해야할 보안 가이드 라인을 제시한다.

II. AI 시스템 보안 취약점 분석

A. 전력 시스템 프라이버시 보호 선행연구 분석

전력시스템의 IT 접목과 함께 대두된 프라이버시 침해 문제로는 크게 제 삼자에 공개되었을 때 생활 패턴 예측에 따른 보안 위협으로 소개되고 있다. 본 연구에서 목표로 하는 상업시설 영업예측 시스템은 일종의 생활 패턴을 예측하는 분야로서 전기사용량 데이터를 이용하여 생활 패턴을 예측할 때 발생할 수 있는 보안 위협에 관한 선행 연구를 조사, 분석할 필요가 있다. 조사된 논문은 정수 계획법, HMM과 SVM, k-NN의 기계 학습 방법을 사용한 생활 패턴 예측 방법론에 있어 공격 기법에 따른 분석 결과로서 TABLE 1과 같이 보안 위협을 평가할 수 있다.

조사된 논문 분석에 적용된 분류 기준은 생활 패턴 예측에 사용된 기법의 종류로서 유출된 데이터로부터 프라이버시 침해에 이르기까지 다양한 방법을 통해 접근할 수 있다는 것을 의미한다. 비록 공격 기법의 유용성에 대한 평가로는 복잡한 실제 환경 대비 공격 효용성에 의문을 제기할 수밖에 없지만, 전력회사에서는 공공데이터와 함께 고객 데이터를 취급하므로 정보 보호 관점에서 정책적, 선제적 조치가 요구된다. 예를 들어 전력계량기는 현장에서의 물리 보안 조치 및 모뎀을 통한 데이터 전송 시 암호화 전송이 필요하고, AMI 데이터와 고객 데이터를 함께 취급하는 서버 시스템의 경우 데이터 관리와 네트워크 보안 관리 측면에서 다중 보안 조치가 필요하다.

B. AI 시스템 공격 시나리오 조사

다음으로 AI 기술을 응용한 전력 시스템이 증가되고 있는 시점에 머신러닝 모델 자체를 공격하거나 학습 데이터를 오염시키는 등 AI 기술의 맹점을 공격하는 기법들에 대한 조사와 대응 방안을 조사하였다.

보안 취약점을 통한 사이버 공격 기법은 매우 다양하지만 본 논문에서 구현한 전력사용량 빅데이터를 활용한 상업시설 영업예측 시스템 적용된 모델에 가능한 공격으로서, 사람과 기계의 인식 차이를 극대화한 Adversarial Machine Learning 기법과 준지도 학습 상황에서 학습 데이터 오염(Training Data Poisoning)기법을 중심으로 논한다.

1) Adversarial Machine Learning 공격 시나리오 및 대응방안

Adversarial Machine Learning은 사람과 기계의 인식 차이를 극대화하는 데이터를 생성해 사람이 보기에는 이상이 없지만, 기계는 이상을 감지할 수 있는 상황을 만드는 것을 목표로 머신러닝 모델의 취약점을 공격하는 분야이다 [11]. Adversarial Machine Learning 공격 기법은 다음의 두 가지 시나리오가 가능하다. 첫 번째 방법은 대상 모델에 데이터를 넣고 얻는 결과 셋을 통해 훈련 데이터를 수집하여 유사 모델을 훈련하여 이를 이용하는 방법이고, 두 번째 방법은 이미 존재하는 비슷한 역할을 하는 유사 모델을 선정해 공격에 사용하는 방법이다. 두번째 방법은 기존에 있는 유사한 역할을 하는 white box 모델을 사용하는 것이기 때문에, 새로 데이터를 모으고 그 데이터를 사용해 모델을 학습시키는 과정이 생략되어서 첫 번째 방법에 비해 비교적 시간이 적게 걸린다. 하지만 두번째 방법을 적용하기 위해서는 대상 모델이 다루는 분야가 범용적으로 많은 사람들이 이용하는 분야인지 여부가 중요하다. 만일 타겟 모델이 하는 역할이 범용적이지 않은 분야를 다룬다면 비슷한 역할을 하는 공개되어 있는 모델이 없을 가능성이 높다. 이러한 관점에서 AMI 데이터로부터 영업 여부를 실시간으로 예측하는 서비스는 전국의 전력량 데이터를 학습에 사용한다는 점에서 접근이 어렵고, 모델의 내부 구조를 공개하는 비슷한 종류의 모델을 찾기가 어렵다. 이와 같은 공격 시나리오에 대한 대응 방안으로는 서비스 요청 횟수 제한, adversarial example 모델 훈련 재사용, 공격에 강건한 모델 설계와 같은 기술적 방안이 있다.

2) 준지도학습 Training Data Poisoning 공격 시나리오 및 대응방안

훈련 데이터에 접근할 수 있는 권한이 주어져 있다는 가정하에 영업여부 예측 시스템에 대해서 training data poisoning 공격

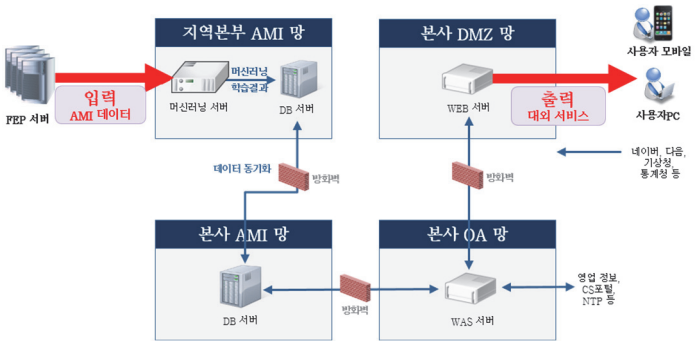

Fig. 1. AMI 데이터를 연동한 상업시설 영업예측시스템

이 가능하다. 처음의 영업여부 예측 모델은 데이터-레이블이 정상적으로 입력된 참 데이터만을 이용한다. 추가로 훈련시키는 online training 단계에서는 기존 모델에서 신뢰도 값이 일정 수치 이상인 데이터만 훈련에 추가하는 최소한의 안전장치를 거치면서 부족한 데이터의 양을 보충하는 방식을 사용하고 있다. 따라서 극단적으로 치우친 데이터를 계속 삽입해 모델을 오염시키는 공격은 성공하기 힘들다. 하지만 신뢰도 값 threshold boundary 근처의 데이터를 지속적으로 주입하는 방식의 공격은 훈련에도 포함될 수 있고, 모델에 지속적인 오염을 누적할 수 있다.

위의 공격에 대한 대응 방안으로는 online training을 하면서 기존 모델에 추가적인 훈련을 시키는 방식이 제안되지만, 현재 사용 중인 방식은 모델이 잘못된 방향으로 학습을 시작했을 시 그것을 바로잡아주는 기준이 없기 때문에 한번 모델이 오염되기 시작하면 추후 진행되는 준 지도 학습 역시 영향을 받게 되고 추가적으로 모델의 성능이 하락할 위험이 있다. 따라서 준 지도 학습이 진행되기 전의 실제 레이블로만 학습시킨 모델을 기준 모델로 삼고, 주기적으로 같은 데이터에 대해 현재 모델과 기준 모델의 정확도를 비교하여 큰 차이가 날 경우 모델을 새로 갱신하는 대응 방안을 통해 점진적인 모델의 오염에 대처할 수 있다.

이처럼 AI 기술 취약성으로 인한 공격 기법들은 모델 자체에 변형을 가하기 위해 오랜 기간 내부에 침투하여 데이터에 접근 가능해야 한다는 점에서 원천 봉쇄를 위한 내부 시스템 보안, 체크리스트 기반의 가이드 제공이 더욱 중요하다는 시사점을 남긴다. 이에 따라 한국전력공사의 AMI 데이터를 활용한 상업시설 영업예측 시스템에 적용된 머신러닝 기술과 시스템 요소들을 소개하고 이에 기반한 보안 가이드를 제시하고자 한다.

III. 상업시설 영업예측 시스템 개발

A. 전력 빅데이터 활용성

한전은 2,400만여 저압 고객에 AMI를 보급할 계획을 갖고 있다. AMI 시스템에서 수집하는 데이터는 한 고객 당 15분 단위의 검침정보로서 상업시설의 전력사용량은 영업 여부와 밀접한 관련이 있다. 구글, 네이버, 다음을 포함한 국내외 포털 사이트에서 제공되는 상점의 영업 정보는 해당 상점이 직접 기입한 정보로서 휴무일이 바뀌거나 휴가기간 등 예외적인 상황을 반영하지 못한다. 만일 AMI 데이터를 통해 실시간 영업여부(Open/Close)와 영업개

TABLE 2
모의해킹 발견 취약점 및 대응방안 예시

구분	취약점	대응 방안
WEB 서버	사용자 웹 인터페이스 임의의 게시판 데이터 수정/삭제/등록 가능	공지사항 글 작성이나 수정/삭제와 같은 중요한 기능은 서버 측에서 허가된 사용자에게만 노출
	임의의 게시판 파일 등록, 수정, 삭제 가능	파일 등록 삭제에 권한 확인 코드를 추가하여 인가되지 않은 사용자가 게시판 첨부파일을 권한 없이 수정, 삭제 방지
	인증서 암호화 키가 코드에 그대로 저장됨	인증서의 암호화 키는 웹서버나 프로그램 로딩 시에 직접 입력하고 평문으로 암호키를 저장하지 않도록 조치
	만료된 TLS/openSSL 버전	최신 버전(TLS 1.3, IETF RFC 8446/openssl 1.1.1c)으로 업데이트
	충분하지 않은 RSA키 길이	4,096 bit 키 사용
WAS 서버	서비스 관리자 웹 인터페이스 인증 부재	세션 권한 체크와 같은 중요 요소는 클라이언트에서 수행하지 않고 서버에서 수행
	해시되지 않고 저장되는 비밀번호	비밀번호 등 사용자 정보는 반드시 해시화하여 저장
DB 서버	DB 통신 보안 강화 가이드라인 미준수	제조사(오라클) 제안, 강화된 보안 설정 필요
통신 구간	서버 간 통신 암호화 미적용	서버간 암호화 통신
방화벽	전 서버가 자체 방화벽 비활성화	접속에 필요한 서버들의 IP 및 필요한 서비스들만 허용하도록 정책 설정

폐 시간(Operations Time)을 제공한다면 국민 편익을 실현할 수 있으며 전력회사 입장에서는 새로운 수익 모델이 될 수 있을 것이다. 따라서 한국전력공사에서는 기존 서비스의 한계를 극복하고 전력사용 데이터 활용을 극대화하기 위하여 AMI데이터와 머신러닝 기술을 융합하여 영업정보 예측시스템을 개발하여 실증하고 있다.

B. 상업시설 영업예측 시스템 개요

본 시스템에서 입력할 데이터는 대표적인 시계열 데이터로서 실시간 예측이 필요함에 따라 연산시간, 성능, 복잡도를 고려하여 CNN을 주요 모델로 선정하였다. 인공신경망에 학습시키기 위해서는 충분한 양의 라벨이 필요한데 매 시각 영업점의 개폐여부를 수집하는 데는 많은 시간과 비용이 소요된다. 따라서 소수의 라벨 데이터와 많은 양의 데이터를 이용하는 준지도학습법을 적용한다. 본 연구에서는 강남구, 서초구 내 상업시설을 샘플링하여 영업 패턴 정보를 설문 조사한 실측 데이터를 라벨 데이터(Ground-truth)로 활용하였다.

상업시설 영업예측 시스템 구성은 다음과 같다. Fig. 1에서 머신러닝 서버는 위의 모델을 활용하여 AMI 데이터를 일정 기간(6주치) 이상 누적하여 학습 및 재학습 과정을 수행한다. 이때, 실시간 전력사용량 데이터를 최대한 전송지연 없이 입력시키기 위하여 시범사업 대상 지역본부 내에 머신러닝 서버와 AMI FEP서버를 직접 연동하였다. 상업시설 영업정보 예측 서비스를 일반 고객에 제공하기 위한 웹 서비스 제공을 목적으로 운영 서버(WAS, WEB)를 구축하고 내부적으로는 영업정보시스템, CS메세지 포탈 시스템과 연계하였고, 외부적으로 카카오맵을 연계하였다.

IV. 모의 해킹을 통한 취약점 도출

모의해킹 테스트 베드는 5종의 서버로 구성되어 있다. 실제 네트워크에서는 지역본부 AMI망, 본사 AMI망, 본사 OA망, DMZ망의 4개 망에 나누어서 분포돼 있지만, 테스트 베드에서는 하나의 단일 허브에 모든 서버가 연결돼 있다. 따라서 개별 서버의 취약점을 도출하고 보안 수준을 점검하기에 유용하다.

테스트베드 내 서버에 대한 모의해킹은 KAIST 보안 연구실의 화이트 해커들에 의뢰하여 수행하였다. 기본적으로 해킹 대회인 CTF (Capture the Flag)의 문제 풀이에 사용되는 방법론을 적용하여 리버싱/바이너리·네트워크·웹 부분 문제 유형을 풀이하는 방법론이 적용되었다. 다양한 외부자들이 내부망에 시스템 유지 관리를 위해서 접속할 것을 가정하여 분석 경로를 단지 망 외부로부터의 위협에 국한하지 않고 악성 내부자에 의한 위협을 분석하기 위해서 5종의 서버 각각에 접속 권한을 가진 상태로 취약점을 조사하였다. TABLE 2는 모의 해킹에서 발견한 취약점들과 그 대응방안을 정리한 것이다.

V. 보안 체계 설계 및 가이드 라인 제시

선행연구 분석과 실제 시스템의 모의해킹 결과를 종합하여 AI를 활용한 전력 시스템의 보안 가이드 라인을 제시하고자 한다.

물리적인 접근을 제외한 데이터 유출 및 서버에 대한 직간접적인 공격은 네트워크를 통해 이루어진다. AMI 데이터를 활용한 상업시설 영업예측 서비스와 같이 여러 구간의 네트워크로 분할된 시스템의 경우에는 각 네트워크에 대한 접근제어, 침입 탐지, 침입 방지가 이루어질 수 있도록 각 네트워크를 제대로 구성하고 제어하는 것이 무엇보다 중요하다.

A. 서버 접근제어

네트워크를 구성하고 통신을 제대로 제어하기 위해서는 일차적으로 각 서버 별로 운영체제 단에서 외부 접속을 허용하는 포트와 프로토콜을 설정해야 한다. 예를 들면 아래와 같은 서버 제어 원칙을 확립할 수 있다.

• 서비스에서 사용되는 프로토콜 및 포트는 모두 TCP 기반이다. 따라서 TCP 계층보다 상위 계층에 해당하는 프로토콜만을 허용하고 그 이외의 UDP, ICMP 등의 프로토콜에 대해서는 차단한다.

• IP 및 도메인 화이트리스트를 적용하여 각 서버 별로 서비스를 위해 필수적인 IP 및 도메인을 제외하고는 여타의 모든 서버로부터의 접근을 막는다.

상기 원칙을 적용하여 서버 제어 규칙을 확정하는 예를 들면, WEB 서버로의 인바운드 트래픽의 경우에는 사실상 HTTPS이외의 트래픽을 허용할 필요가 없다. WEB 서버로부터의 아웃바운드 트래픽의 경우, 외부망으로 향하는 유일한 아웃바운드 트래픽은 계정연동·기상·통계·우편·휴일정보 수신을 위해서 존재하는데 WEB 서버로부터의 접속이 필요한 서버들을 기준으로 화이트리스트를 만들어서 해당 서버들만 접속하도록 조치한다.

B. 망 접근제어

서버 내부에서의 네트워크 설정 뿐만 아니라 망간 및 망 내부에서도 접근 제어를 위한 시스템을 구축하여야 한다. 각 망 사이에 방화벽 또는 자료연계시스템이 존재하는데 이러한 망 접근제어 시스템들은 외부로부터 들어오는 불필요한 트래픽을 우선적으로 차단하며 망내 서버의 부하를 덜어주는 역할을 한다. 만약 이 시스템들이 존재하지 않는다면 외부로부터 DDoS와 같은 공격이 들어왔을 때 망내 서버의 네트워크 버퍼가 가득 차 데이터를 제대로 처리하지 못하는 상황이 발생할 수 있으며, 이는 정상적인 사용자의 접근 또한 불가하게 만든다.

보다 강화된 망 접근 제어를 위해서는 방화벽을 위시한 망간 접근제어 시스템 뿐 아니라 IPS/IDS와 같은 망내 감시/접근제어 시스템의 도입이 필요하다. 이들 망내 감시/접근제어 시스템들은 정상적인 접근을 위장한 공격이나 소프트웨어 취약점을 이용한 공격과 같이 망간 접근제어 시스템이 차단할 수 없는 악성 트래픽을 실시간 모니터링을 통해 식별하고 차단하는 역할을 수행한다.

C. 안전한 프로토콜 및 시스템 설계

1) 망간 통신 암호화

현재 본사 AMI 망에 있는 대외서비스 DB 서버는 OOO지역본부 AMI 망에 있는 머신러닝 DB 서버와 연계가 되고 주고받는 데이터는 모두 TCP 프로토콜을 기반으로 교환된다. 이러한 상황에서 망 사이에서의 데이터 통신을 암호화하지 않는다면 공격자가 장악한 망에 의해 데이터가 유출될 가능성이 있다. 웹 보안 표준화 비정부기구인 OWASP (Open Web Application Security Project) 및 Let's Encrypt에 의하면 모든 데이터 통신을 암호화해야 한다 [12][13]. 데이터베이스 접근 관련 통신 암호화와 더불어 WAS 서버와 WEB 서버의 데이터 연동 시 IPSec과 같은 상위 계층 보안 프로토콜을 사용하여 데이터를 암호화하여 전송하는 것이 권장된다.

2) 인증서 고정(Pinning)

전력사용 데이터를 활용한 서비스를 구현하는 데에 활용되는 프로토콜 중에는 TLS, HTTPS와 같이 공개키 암호화를 기반으로 한 프로토콜이 다수 존재한다. 공개키 암호화 방식은 데이터를 보호하는 데에 아주 유용한 방법이지만, 통신 주체의 올바른 인증 없이는 중간자 공격을 당할 위험이 있다. 따라서 이를 방지하기 위해 각각의 서버에 인증서(X.509)들을 미리 고정 설치(pinning)한 후 해당 인증서를 이용하여 통신 상대방을 인증하는 과정이 필요하다.

3) 사용자 인증 및 세션 관리

상업시설 영업예측 시스템은 고객의 요청에 따라 WAS와 WEB 서비스를 이용해야 한다. 아래는 사용자 인증 정보와 관련하여 고려해야 할 보안 조치 사항들이다.

• 로그인 정보 저장/관리(User Credential): 상업시설 영업예측 서비스에서는 따로 회원가입을 통한 로그인을 운영하지 않고 네이버/카카오 등의 오픈 로그인을 활용하므로 해당 세션을 HTTPS로 보호하는 등의 조치가 필요하다. 추후 추가적으로 회원가입을 직접 처리하는 경우에는 평문 패스워드가 시스템에 저장되지 않도록 사용자 로그인 정보를 해시화 해서 저장한다.

• 로그인 세션 만료 시간 지정: 일반적으로 사용자는 로그아웃하지 않은 채 서비스를 종료하는 경우가 많다. 따라서 일정 시간이 지나면 로그인 세션을 강제로 종료하도록 하여 사용자의 세션을 임의의 다른 사람이 사용할 수 없도록 만든다.

• 2FA (2 Factor Authentication) 의무화: 2FA을 활용하여 내부 DB에 데이터를 요청할 수 있는 고객의 로그인 정보가 유출되어도 추가적인 보안 절차를 거쳐야만 작업을 요청할 수 있도록 한다. 2FA 방법으로는 이메일, 문자메시지, OTP (One Time Password)를 사용하는 방법 등이 있다.

• 제3 기관의 데이터 활용을 위한 API 접근제어: 허가되지 않은 프로그램을 사용해 데이터를 불법적인 목적으로 사용하려고 하거나 필요 이상으로 많은 양의 데이터를 수집하는 행동을 방지하기 위해 API에 대한 고객의 접근 권한을 상황에 맞게 조절한다.

• 접근제어는 반드시 서버에서 수행: 인가되지 않은 사용자 접근을 차단할 때는 반드시 차단 로직이 클라이언트가 아닌 서버에서 수행되도록 하여야 한다. 차단 로직이 클라이언트에서 수행될 경우, 공격자 본인이 클라이언트 기기에 대한 모든 관리 권한을 가지고 있으므로 간단히 우회될 수 있다.

D. 개별 서버 보안 가이드라인

네트워크를 통한 공격자의 침투가 잘 방지되는 것이 최우선이지만, 유효한 공격을 위해서는 공격자가 반드시 서버에 직접적으로 접근할 수 있어야만 하므로 개별 서버의 추가 보안 조치가 필요하다. 개별 서버 보안 위협은 사용자 입력 처리 관련 취약점, 버퍼 오버플로우 등 바이너리 상 취약점의 크게 두 가지로 나누어 볼 수 있다.

1) 사용자 입력처리 취약점 방지 가이드

거의 모든 프로그램은 외부 입력이 필요하다. 외부 입력은 SQL Injection 혹은 Command Injection을 통한 악성 명령어의 실행이 가능하여 심각한 취약점이 발생할 수 있다. 이러한 위협을 방지하기 위해서 할 수 있는 조치사항은 프로그램의 성격에 따라 두 가지로 고려해볼 수 있다.

첫째, 자체 개발 프로그램의 경우로서 사용자의 입력을 받아 처리하는 부분에서 입력의 정상성을 체크하는 로직을 추가하여 비정상적인 입력이 주입되지 못하도록 해야 한다. 예시로 입력값이 특정 범위를 넘지 않는지를 체크하거나, 프로그램 명령어로 해석될 수 있는 쿼트('), 더블 쿼트("), 세미콜론(;) 등의 제어 문자를 체크하는 로직을 들 수 있다.

둘째, 상용 소프트웨어 뿐 아니라 운영체제, 오픈소스 등 자체 개발하지 않은 모든 프로그램을 아우르는 경우다. 이들 외부 프로그램의 경우에는 최신 버전의 소프트웨어를 사용하고 모든 보안 패치를 설치하는 것이 최우선이다. 최신 버전을 사용하는데도 취약한 경우에는 일단 소프트웨어 제작 주체에게 최대한 빠른 취약점 패치를 요구하거나 취약점이 없는 다른 프로그램으로 대체한다.

2) 바이너리 취약점 방지 가이드

거의 모든 프로그램은 프로그래밍 시점에 데이터의 크기를 미리 알 수 없는 비정형의 데이터를 다루게 된다. 이런 비정형의 데이터를 프로그램에 적절하게 처리하지 않을 경우, 버퍼 오버플로우 등의 바이너리 상 취약점이 발생할 수 있다. 이러한 위협을 방지하기 위한 조치사항은 프로그램의 성격에 따라 두 가지로 나누어서 생각해 볼 수 있다.

첫째, 자체 개발 프로그램의 경우 메모리 관련 함수를 사용할 때 버퍼 오버플로우로부터 안전한 함수만을 사용하는 것이 필요하다. 또한, 함수의 반환 주소가 프로그램 실행 과정에서 변경되었는지를 확인하는 로직을 도입하여 반환 주소가 변경된 경우 오류를 발생시키도록 하는 조치를 취한다. 그 밖에 현재 실행 중인 프로그램의 코드 영역을 덮어쓰려는 어떠한 시도도 오류를 발생시키도록 할 수 있다. 이는 대부분 운영체제(OS) 상 해당 기능을 활성화시킴으로 해결 가능하다.

둘째, 외부 프로그램의 경우는 프로그램에 문제가 있더라도 직접 수정하는 것이 불가능하므로 최신 버전의 프로그램을 사용하기, 보안패치 설치, 알려진 취약점이 없는 프로그램으로 대체 등의 조치가 필요하다.

VI. Conclusion

그동안 기간산업으로서 IT에 대처가 느렸던 전력 시스템은 AI 기술과 접목함으로 폭발적으로 성장을 하고 있다. AI 기술이 적용된 전력 시스템이 디지털 변환으로 미래를 어떻게 이끌어갈지 기대하기에 앞서 공격자에 의해 악용되거나 오용되었을 때의 피해를 예상하여 대응할 수 있어야 한다.

본 논문에서는 먼저 전력 빅데이터와 AI가 접목되었을 때 발생할 수 있는 개인 프라이버시 침해 및 시스템 보안 위협과 각각의 대응 방안에 대한 선행 연구를 정리하고 분석하였다. 개인 프라이버시 침해와 시스템 보안 위협은 각각 다른 도메인 상의 보안 조치가 필요하다. 개인 프라이버시 문제는 고객의 전력 사용량 데이터를 사용하는 전력회사 입장에서 고객의 개인정보, 민감 정보 침해 방지를 위한 정책상 조치를 선제적으로 취해야 할 것이 권고되고, AI 공격 기법들은 모델 자체에 변형을 가하기 위해 오랜 기간 내부에 침투하여 데이터에 접근 가능해야 한다는 점에서 원천 봉쇄를 위한 네트워크 상에서의 보안, 내부 시스템 보안, 체크리스트 기반의 가이드 제공이 더욱 중요하다는 시사점을 남긴다.

다음으로 한국전력공사의 전력사용량(AMI) 빅데이터를 활용한 상업시설 영업예측 시스템에 적용된 머신러닝 기술과 시스템 요소들을 소개하며, 모의 해킹을 통해 실제 전력 설비와 접목하면서 드러나는 보안 취약점을 도출했다. 실제 구축한 상업 시설 영업 예측 시스템은 사업소, AMI망, OA망, DMA 망 등 여러 내부망에 걸쳐 운영 서버를 두고 있고 각 요소별로 내, 외부 사용자 및 시스템과 연계하고 있어 다양한 보안 위협요인(Cyber security attack surface)이 존재한다.

마지막으로 실제 구축을 하면서 취한 보안 조치와 보안 정책을 종합하여 일반 보안 가이드 라인을 제시하였다. 본 논문은 AI와 전력 시스템이 접목되었을 때 발생할 수 있는 보안 취약점을 도출하고, 이에 대한 정책적, 관리적, 기술적 대응책을 제시하고 실제 구축, 운영 중인 상업시설 영업 예측 시스템에 적용하였다는 점에서 실용적이다. 본 논문에서 제시하는 방법은 전력 산업에 AI를 활용하기 위해 최소한의 보안성을 지키기 위한 가이드 라인으로써 이 과정에 대한 준수는 필수적으로 하고 이를 바탕으로 각 시스템별, 용도 별로 추가적인 보안 체계를 설립할 것을 제안한다.

References

[1] 서동준, "에너지 ICT분야 인공지능 기술 동향", 정보과학회, Vol. 37, pp. 48-58, 2019.

[2] 최인지, 장민해, 최문석, "AMI 데이터와 머신러닝을 이용한 영업예측시스템 개발", 대한전기학회 하계학술대회, 2020.

[3] Stephen McLaughlin, Patric McDaniel, Willian Aiello, “Protecting consumer privacy from electric load monitoring,” Association for Computing Machinery Computer and communication security, pp. 87-98, 2011.

[4] Arijit Ukil, Soma Bandyopadhyay, Arpan Pal, “Demo Abstract: SPA: Smart Meter Privacy Analyzer,” Association for Computing Machinery, pp. 192-193, 2014.

[5] “주요정보통신기반시설 기술적 취약점 분석. 평가 방법”, 한국인터넷진흥원, 2017.

[6] 이수연, 유지연, 임종인, “주요기반시설 서비스의 안전적 운영을 위한 보안 프레임워크 설계에 관한 연구”, 한국IT서비스학회, Vol. 15, pp. 63-72, 2016.

[7] Kosuke Suzuki, Shinkichi Inagaki, Tatusya Suzuki, Hisahide Nakamura, Koichi Ito, “Non-intrusive Appliance Load Monitoring Based on Integer Programming,” SICE Annual Conference, 2008.

[8] Oliver Parson, Siddhartha Ghosh, Mark Weal, Alex Rogers, “Using Hidden Markov Models for Iterative Non-intrusive Appliance Monitoring,” Neural Information Processing Systems workshop on Machine Learning for Sustainability, 2011.

[9] Marisa Figueiredo, Ana de Almeida, Bernardete Riveiro, “Home electrical signal disaggregation for non-intrusive load monitoring system,” Neurocomputing. Vol. 96, pp. 66-73. 2012.

[10] Alberto Prudenzi, “A neuron nets based procedure for identifying domestic appliances pattern-of-use from energy recordings at meter panel,” IEEE Power Engineering Society Winter Meeting, pp. 941-946, 2002.

[11] Szegedy, Christian, Zaremba, Wojciech, Sutskever, Ilya, Bruna, Joan, Erhan, Dumitru, Goodfellow, Ian J., Fergus, Rob. “Intriguing properties of neural networks,” ICLR 2014.

[12] www.owasp.org.

[13] www.letsencrypt.org.