DNN 기반 병원 환경 네트워크 이상행위 탐지 시스템 제안

진정하, 한근희
스마트의료보안포럼
nemoda75@gmail.com, khhan1@korea.ac.kr

Proposed Network Abnormal Behavior Detection System in a Hospital Environment Based on Deep Neural Networks

Jungha Jin, Keunhee Han
Smart Medical Security Forum

요 약

현재 병원내에서 사용되는 인프라를 살펴보면, 제조사의 자체 프로토콜, 다시말해 비표준 프로토콜로 동작하는 기기들이 상당히 많아 이상행위 탐지에 많은 어려움을 갖고 있다. 이러한 병원 환경에서 사용되는 다양한 의료기기가 존재함에 따라서 그에 대한 이상행위를 탐지 및 대응에 부족한 부분이 존재하게 되어 병원내 보안에 문제점으로 작용하게 된다. 상기와 같은 문제를 해결하기 위해 심층신경망 기반의 딥러닝 알고리즘을 통한 병원 네트워크 환경에서의 이상행위 탐지 방안에 대한 연구를 수행하기 위해, DNN 기반의 AI 학습 방식을 적용하여 병원 내부 네트워크 패킷을 수집하여 분석을 수행하는 방안에 대하여 논하고자 한다.

Ⅰ. 서 론

ICT 기술의 발전에 따라 병원 환경은 IT 영역과 의료서비스 영역이 점차 융합하여 상호부조의 관계로 동작하고 있다. 이러한 환경에서 가장 큰 문제점으로 대두되고 있는 사항은 바로 병원내 환경의 보안에 관련한 이슈사항이다. 특히, 병원 환경은 그 특수성으로 인하여 보안 기능의 추가에 많은 어려움이 따른다. 예를 들면, 환자 상태 모니터링 장비가 PC 기반으로 동작하게 되는 경우, 수술장과 같은 위급 상황에서 보안 업데이트로 인하여 중요 프로세스가 제한을 받아 서비스를 적시에 제공하지 못하게 되면, 환자의 생명에 큰 위험을 초래하게 된다. 또한, 환자 부착 장치들과 같은 네트워크 기능이 포함되어 있음에도 불구하고, 시스템 리소스의 부족으로 보안 기능을 제공하지 못하는 경우도 허다하여, 이러한 부분도 병원 환경에서의 보안에 가장 큰 문제점으로 인식되고 있다.[1]

상기와 같은 문제로 인하여 병원 환경에서의 이상행위 탐지에 관한 연구가 다양하게 진행중에 있으나 지금까지 도출된 문제점을 해결하기에는 많은 어려움이 따르고 있다. 특히, 랜섬웨어와 같은 보안이 취약한 기기를 대상으로 발생하는 공격은 아무리 보안이 철저하게 보장된다고 하더라고, 네트워크에 연결된 한 개의 노드에서 감염되는 순간 병원 환경 전체로 공격이 발전하게 되는 이유로 병원 환경의 개별 사용자 및 기기들에 대한 이상행위 탐지 및 대응 방안의 필요성이 증가하고 있다.

본 논문에서는 병원 환경이라는 특수한 환경에서의 이상행위 탐지를 수행하기 위하여 심층신경망 기반의 머 기술을 통해 네트워크 이상행위 탐지 시스템을 제안하고자 한다. 이를 위해 1장의 서론에 이어서, 2장의 관련연구, 3장의 DNN 기반 이상행위 탐지 시스템 제안 내용, 4장의 결론으로 설명하고자 한다.

Ⅱ. 관련 연구

가. 심층신경망(Deep Neural Network, DNN)

다양한 데이터를 활용하여 컴퓨터가 사람과 같이 학습을 스스로 가능하게 하는 인공 신경망(Artificial Neural Network, ANN) 구성 기술을 딥러닝(Deep Learning)이라고 칭한다. 이러한 딥러닝 알고리즘 중에서 심층신경망 알고리즘은 입력층(input layer)과 출력층(output layer) 사이에 다수의 은닉층(hidden layer) 들로 구성된 인공 신경망(Artificial Neural Network, ANN) 구조를 갖는다.[2-3] 일반적인 인공 신경망 구조와 동일하게 심층 신경망 구조는 복잡한 구조의 비선형 관계(non-linear relationship)들에 대한 모델링을 통해 구성이 가능하다.[4] 심층 신경망은 여러개의 층으로 구성되고, 각각의 층은 다수의 노드들로 이루어지게 된다. 각각의 노드에서는 연산이 발생하는데, 이때의 연산 과정은 인간의 신경망을 구성하고 있는 뉴런에서 일어나는 일련의 과정과 동일하게 설계된다.

나. 병원환경의 보안위협

병원은 환자가 의료진에게 진료를 위하여 방문 예약, 방문 진료 위주로 이루어지게 된다. 현재는 비대면 환경에서의 스마트의료 서비스가 도입되면서 병원 환경의 변화가 발생하고 있는 상황이다. 의료기기 및 의료정보 시스템이 병원에서의 폐쇄적인 네트워크 환경에서 게이트웨이를 사용하여 제한적으로 외부 네트워크와 연결되어 원격으로 의료서비스를 제공하고 있는 상황으로 변하고 있으며, 이러한 환경에서 병원은 비대면 스마트 의료 서비스를 제공하고 있다. 이런 변화되는 환경에서 병원 환경은 네트워크 연결을 통하여 전자의료기록(EMR), 전자건강기록(EHR) 등을 다른 병원 및 플랫폼 제공자, 혹은 환자 본인과 직접적으로 주고받을 수 있어야 한다.

병원 환경에서 사용되는 관련 의료기기를 살펴보면 통합 모니터링을 수행하는 모니터와 EMR, PACS와 같은 서버들이 모여있는 서버팜의 '모니터 및 서버팜'영역이 존재하고, EMR 및 OCS 등을 유통하는 '전자의무기록 및 처방전 전달 시스템'이 존재하며, RIS 및 LIS와 같은 '영상의학 및 임상 병리학'이 존재한다. 마지막으로 '환자영역'에서 사용되는 기기들오

구분이 가능하다. 다음의 표1은 병원에서 사용되는 의료기기 유형을 구분한 예제이다.

표 1. 병원에서 사용되는 의료기기 유형 예시

구분	설명
모니터 및 서버팜 영역	I/F 서버, EMR 서버에서 수집된 정보(환자의 생체 정보, 진료 정보)를 통합하여 환자의 위험도를 계산한 뒤 고위험군에 속하는 환자를 관리하는 영역 RTLS 서버에서 수집된 정보를 통해 이동형 의료자산 관리와 환자의 동선 파악을 할 수 있는 영역
	의료기기 또는 의료인을 통해 수집된 정보들을 각각의 목적 및 프로토콜에 맞게 서버에서 처리한 뒤 데이터베이스에 저장하는 영역
EMR/OCS (전자의무기록, 처방전달시스템)	환자의 간호/진료 내역의 디지털화를 통해 원활한 원내 진료 작업이 될 수 있도록 도와주는 시스템
RIS/LIS (영상의학/임상병리학)	CT/MRI/초음파 등 영상의학기기의 결과를 다루는 영역 DICOM 프로토콜을 통해 기기로부터 수집된 이미지 데이터를 EMR에 전송하고 PACS DB에 저장
환자영역	의료 기기로부터 환자 정보를 수집하고 게이트웨이를 통해 이더넷으로 데이터를 EMR 서버 또는 인터페이스 서버로 전송 특정 의료기기는 블루투스 또는 WiFi 지원이 가능하다면 비콘을 통해 데이터 전송 가능

Ⅲ. DNN 기반의 이상행위 탐지 시스템 제안

병원 환경에서 사용되는 의료기기에서 AI를 적용하여 이상행위 탐지를 수행하면 빠르게 이상행위 패턴 분석을 수행할 수 있어서 매우 효율적일 것으로 판단된다. 병원 환경에서 의료서비스의 중요 정보는 환자 정보를 수집하거나 생성하는 의료기기로부터 시작이 되게 되며, 대부분의 의료기기들이 환자 데이터의 교환, 수집 및 저장 등을 위해서 원격지 또는 네트워크로 연결된 병원 내 서버, 환자 단말기, 의사 컴퓨터로 전송을 수행하게 되는 구조를 갖는다. 이러한 병원 환경에서의 의료기기 관련 문제점 예시로는, 제한된 자원을 사용하는 의료기기의 특성으로 인해 의료기기 내 백신과 같은 보안솔루션을 탑재하기에는 무리가 있다는 점과, 사용하는 운영체제 또한 노후화된 운영체제를 사용하여 다양한 위협에 노출되어 있다는 것들과 같은 내용이 존재한다. 이러한 병원환경에서 DNN 기반의 AI 학습 알고리즘을 적용한 이상행위 추론 알고리즘을 다음의 그림 1과 같이 제안하고자 한다.

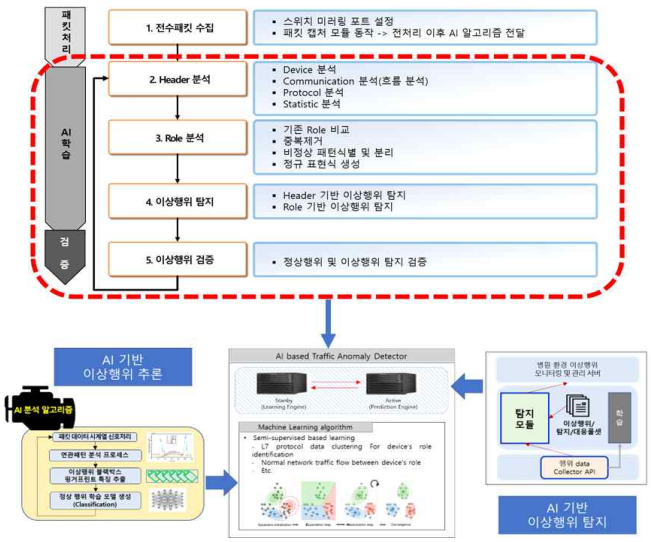

그림 1. AI 기반 이상행위 추론 알고리즘 아키텍처

그림 1을 살펴보면 AI 학습과 검증을 통해 이상행위에 대해서 추론하여 판단하는 구조를 갖게 됨을 알수 있다. 여기서 AI 학습 방식은 심층신경망 기반의 AI 학습 알고리즘을 적용하여 이상행위에 대해 분석을 수행하고, AI 학습 알고리즘에서 판단한 결과를 기반으로 이상행위 탐지를 수행하게 된다. DNN 기반의 AI 학습 알고리즘에서는 이상행위 추론을 위해 네트워크 패킷 헤더 분석 방식이나 기기 및 접속자 정보등의 식별 가능한 정보를 기반으로 하는 Role 분석과 같이 2가지 방식으로 분석을 수행하게 된다. 우선 네트워크 패킷 헤더 분석을 살펴보면, 출발지 및 목적지 IP 정보 등을 기반으로 하는 기초적인 내용 분석과 TCP 연결의 경우 흐름 분석등을 수행할 수 있고, Application Protocol 분석 등을 통해 이상행위 분석을 수행할 수 있다. 디바이스 및 접속자 정보 등과 같은 식별 가능한 정보를 기반으로 하는 Role 분석을 통해서는 기존 확인되어 정의되어 있는 White list 기반의 Role 과의 비교 분석을 수행하고, 비정상 패턴 식별 및 분리를 통해 시계열 처리를 통한 정규화 수행으로 정규 표현식을 생성하여 Role을 추가하여 이상행위 탐지를 수행하게 된다.

Ⅳ. 결론

본 논문에서 제안하는 DNN 기반의 이상행위 탐지 시스템을 통해 병원 환경에서의 이상행위 탐지 방안을 설명하였다. 벼우언 환경은 이상행위 탐지가 매우 어려운 구조이며, 보안의 레벨이 다양하게 존재하는 특수한 환경임에 따라 AI 기반의 이상행위 탐지를 통해 보다 효율적이고 정교한 이상행위 탐지가 가능해 질것으로 판단된다. 실제로 DNN 기반의 AI 학습 알고리즘을 통한 이상행위 탐지 모듈을 통해 ICE(Integrated Clinic Environment) 환경에서 수집한 5종의 Ransomware (WannaCry, Petya, BadRabbit, PowerGhost) 공격 실험 데이터를 시뮬레이션 해본 결과, 520차원의 행위 속성이 분류 되었으며, 이를 기반으로 유효성 분석이 가능함을 확인 할 수 있었다.

ACKNOWLEDGMENT

이 성과는 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.IITP2019-0-00224010400 2, AIM : AI 기반 차세대 보안 정보관리기법적용 Cognitive Intelligence 및 Secire-오픈 프레임워크(S-OFW)기술 개발)

참 고 문 헌

[1] 백신도 못까는 의료기기, 2018/05/04 (https://zdnet.co.kr/view/?no=20180504151307).

[2] Iasonas Kokkinos and Alan Yuille. “Inference and learning with hierarchical shape models”, In International Journal of Computer Vision, 93(2):201 - 225, 2011.

[3] Christian Szegedy, Alexander Toshev and Dumitru Erhan. “Deep neural networks for object detection”, In NIPS'13 Proceedings of the 26th International Conference on Neural Information Processing Systems - Volume 2, 2553-2561, Dec 2013

[4] Yoshua Bengio, Aaron Courville, and Pascal Vincent. “Representation Learning:A Review and New Perspectives”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 35, no. 8, 1798-1828, Aug 2013