딥러닝 기반 병원네트워크 이상행위 탐지 시스템에 관한 연구

김강현, *정성수, *한현욱
차의과학대학교
anomii1@naver.com, jssdisec@gmail.com, stepano7@gmail.com

A Study on the Anomaly Detection System of Hospital Network Based on Deep Learning

Kim Kang Hyun, *Jung Sung Soo, *Han Hyun Wook
CHA Univ.

요 약

최근 의료계는 네트워크 기반 의료시스템이 고도화되면서 스마트 의료 환경 조성이 가속화되고 있으나 병원내부의 보안 관리가 미흡한 현실이다. 또한 병원 내부의 데이터 전송 프로토콜이 다양화 되면서 패킷 데이터 분석과 파싱의 어려움이 있으며, 통계 및 룰 기반 보안시스템으로는 병원 네트워크의 이상행위를 탐지하는데 한계가 있다. 본 논문에서는 이러한 한계점들을 극복하기 위해서 병원 네트워크 시뮬레이터의 활용, 학습데이터 확보, 딥러닝 기술 활용함으로써 알려지지 않은 새로운 공격에 대비하고, 실시간으로 대응할 수 있는 이상행위 탐지시스템을 제안하고자 한다.

Ⅰ. 서 론

최근 의료계는 네트워크 기반 의료기기 및 의료정보시스템을 도입을 하여 스마트 의료 환경을 조성하고 있다. 이런 환경은 개인의료정보를 생산, 보관, 관리하고 있는 전자 의무기록(EMR), 의료영상 저장전송 시스템(PACS) 등의 정보시스템을 통해 개인의료정보를 생산, 보관, 관리하고 있다[1]. 현재 의료 네트워크 보안 솔루션은 Firewall이나 IDS, IPS에 의존하고 있으나, 사이버 공격 기법이 날로 다양해지고 고도화됨에 따라, 새로운 공격을 모두 탐지하기 어렵고, 1차 내부 네트워크로 잠입 후 탐색, 확산, 유출하는 후속 단계의 의료기기 및 의료정보시스템에 대한 내부 공격을 탐지하기 어렵다.

또한 의료 환경에는 DICOM(Digital Imaging and Communicati-ons in Medicine) 및 HL7(Health Level7)등과 같은 의료환경에 특화된 표준 프로토콜을 포함한 다양한 프로토콜이 사용되고 있다[2]. 그러나 의료 프로토콜은 다양한 버전이 존재해 패킷 분석이 어렵다. 의료 정보 송신의 로그 및 보안기록에 대해서 일관적인 프로토콜 보안체계 확립과 데이터 파싱(Parsing)의 난해함이 있어, 의료 프로토콜에 특화된 신종 공격에 대해 실시간 탐지 및 대응이 어렵다.

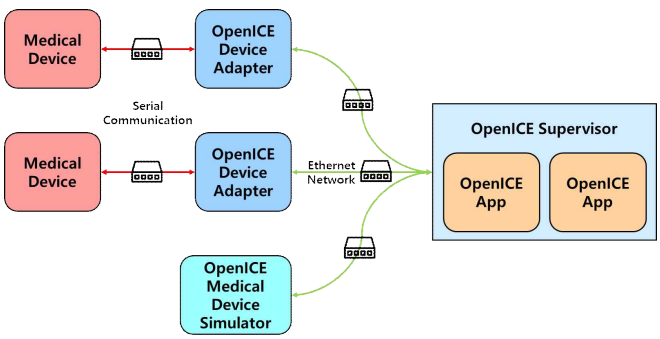
따라서, 이러한 프로토콜 환경에서 이상행위를 실시간으로 탐지가 가능하고 다양한 병원의 데이터 전송 프로토콜에 대한 적절하게 적용할 수 있는 인공지능 기반의 네트워크 보안체계를 구현하는 방법을 논하고자한다[3].

Ⅱ. 본론

본 논문에서는 의료정보시스템, 의료기기, 통신 프로토콜 등의 다양한 IT 인프라로 구성된 병원 네트워크 환경에서 알려진 사이버 공격외에도 알려지지 않은 공격도 탐지할 수 있는 차세대 AI기반 병원 네트워크 이상행위 탐지 시스템을 연구했다.

Ⅱ-1 가상 병원 네트워크 구현 및 학습 데이터 확보

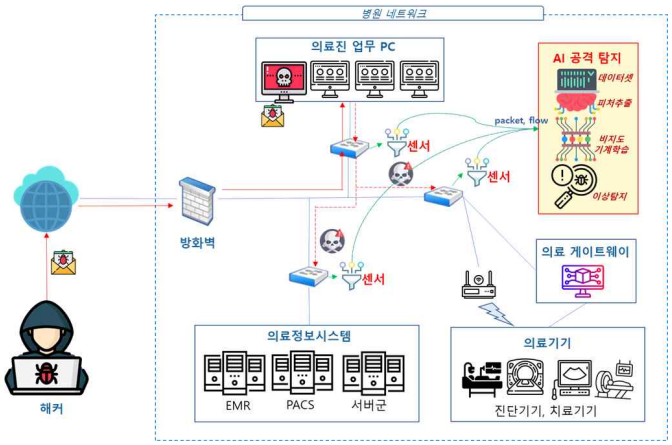
인공지능의 기계학습를 위해서는 학습용 데이터셋 확보가 가장 중요하다. 폐쇄 네트워크를 사용하는 병원 네트워크의 특성상 실제 병원 트래픽에선 이상행위 데이터 셋을 확보하기가 어렵다. 환자의 생명에 직접적 영향을 주는 의료기기와 같은 의료 환경 특성상 실제 의료 네트워크에 이상행위 데이터를 생성할 수 없다는 문제가 존재한다.



[그림 1] 데이터셋 생성을 위한 병원네트워크 시뮬레이터 개요도

따라서 이상행위가 포함된 데이터셋의 확보를 위해 OpenICE를 활용하여 가상의 의료기기 네트워크를 구성하는 방안을 제안한다.OpenICE는 가상의 병원 네트워크 환경을 구현해주는 오픈소스 시뮬레이터이다[4]. [그림1]과 같이 의료기기와 의료정보시스템,

의료진 데스크탑 등 의료 환경 프로토타입과 IoT 디지털 헬스케어 환경을 구현할 수 있다. 또한 인공지능 분석을 위한 학습데이터를 확보하기 위해서 칼리 리눅스(Kali Linux) 사용하였다. 칼리 리눅스는 해킹과 관련된 도구를 제공하고 네트워크 등의 사이버 침투 테스를 할 수 있는 OS로 네트워크 이상 행위 데이터 생성이 가능하다[5].



〔그림 2〕딥러닝 기반 병원네트워크 이상행위 탐지 시스템

Ⅱ-2 시스템 아키텍처

본 논문의 시스템은 [그림1]과 [그림2]의 아키텍처와 같이 병원 네트워크 시뮬레이터, 트래픽 캡쳐 센서, 학습서버, 탐지서버로 구성된다. 병원네트워크 시뮬레이터는 OpenICE를 활용하여 가상 의료기기와 가상 네트워크망을 구현하였다. 스위치 미러링 또는 탭 미러링을 수행하는 트래픽 캡쳐 센서는 의료 프로토콜 파싱을 통해 의료 프로토콜 파싱이 가능한 트래픽 피처를 수집 및 추출(feature selection)할 수 있게 설계했다. 학습서버는 [그림1]에서 확보된 학습데이터 기반으로 이상치 탐지(Anomaly Detection)[3,6]을 위한 LSTM, Autoencoder등과 같은 비지도학습 딥러닝기반 알고리즘을 통해 학습을 거쳐, 탐지서버에서 트래픽의 이상행위 탐지할 수 있게 설계했다. 탐지서버에서는 학습서버에서 기계학습을 통해 개발된 이상행위 탐지 모델을 사이버 공격 탐지엔진으로 구현하여 실시간 공격 탐지 및 모니터링을 수행하도록 설계하였다.

Ⅲ. 결론

본 연구에서는 병원 네트워크의 프로토콜 복잡성, 스마트 의료기기의 증가, 지능형 사이버공격의 고도화로 인해 병원 사이버 공격이 많아지고 피해도 커지고 있다. 병원 인프라를 목표로 알려지지 않은 신종 공격에도 대처할 수 있고, 프로토콜의 복잡성을 적응이 가능한 비지도학습 기반 이상행위 탐지 시스템 아키텍처를 제안하였다.

향후, 제안한 아키텍처를 바탕으로 시스템을 구현하고 실제 병원의 네트워크 환경, 프로토콜, 의료 시스템 구조에 맞춰 구현 및 실증을 할 계획이다.

ACKNOWLEDGMENT

이 성과는 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임. (No.2019-0-00224, AIM : AI 기반 차세대 보안 정보관리기법적용 Cognitive Intelligence 및 Secure-오픈 프레임워크(S-OFW)기술 개발)

참 고 문 헌

[1] 스마트의료 사이버보안 가이드. 한국인터넷진흥원, 2018/05

[2] Institute of Medicine (US) Committee on Data Standards for Patient Safety; Aspden P, Corrigan JM, Wolcott J, et al., editors. Patient Safety: Achieving a New Standard for Care. Washington (DC): National Academies Press (US); 2004. 4, Health Care Data Standards.

[3] Du, Min, et al. "Deeplog: Anomaly detection and diagnosis from system logs through deep learning."Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. p.1285-1298, 2017

[4] OpenICE, https://www.openice.info/

[5] Kali Linux, https://www.kali.org/

[6] Khatuya, Subhendu, et al. "Adele: Anomaly detection from event log empiricism."IEEE INFOCOM 2018-IEEE Conference on Computer Communications. IEEE, pp.2114-2122, 2018.

[7] 디지털 헬스의 최신 글로벌 동향, 의료정책연구소, 2020/05