HL7 FHIR 트래픽 모니터링 시스템 설계

진창규, 방지원, 정한길, 최미정
강원대학교
jinchanggy@gmail.com, {jiwonbang, jeong00400, mjchoi}@kangwon.ac.kr

Design of an HL7 FHIR Traffic Monitoring System

Changgyu Jin, JiWon Bang, Hangil Jeong, Mi-Jung Choi
Kangwon National University

요 약

의료데이터의 디지털 전환이 가속화되면서 시스템 간 데이터 상호운용성을 보장하는 표준의 중요성이 커지고 있다. HL7 FHIR(Fast Healthcare Interoperability Resources)은 의료데이터 교환의 핵심 표준으로 자리 잡았으나, 웹 API 기반 구조로 인해 개인정보(PII, PHI)가 전송 과정에서 보안 위협에 노출될 가능성이 존재한다. 기존 네트워크 계층 보안 기법만으로는 이러한 응용계층 수준의 위협을 완전히 차단하기 어렵기 때문에, FHIR 메시지 단위의 세밀한 모니터링이 필요하다. 본 연구는 이러한 한계를 보완하기 위해 HL7 FHIR 환경에서 발생하는 트래픽을 응용계층 수준에서 수집·정제·분석할 수 있는 트래픽 모니터링 시스템을 설계하였다. 제안된 시스템은 트래픽 복제, 전처리, 데이터 저장, 모니터링의 4단계 구조로 구성되어 비정상 행위 및 개인정보 유출 가능성을 조기에 탐지할 수 있다. 이를 통해 의료기관의 데이터 전송 투명성과 보안성을 향상시키며, 향후 머신러닝 기반 이상 탐지 기법과 결합하여 지능형 의료데이터 보안 인프라로 확장될 수 있는 가능성을 제시한다

Ⅰ. 서 론

최근 의료 분야에서는 디지털 전환(Digital Transformation)과 함께 데이터 기반 진료, 연구, 행정의 통합이 빠르게 진행되고 있다. 병원 내 전자의무기록(Electronic Medical Record, EMR)뿐만 아니라, 유전체 정보, 웨어러블 디바이스, 환자 개인의 헬스케어 앱 등 다양한 출처에서 생성되는 데이터가 폭발적으로 증가하고 있으며, 이들 간의 상호운용성을 확보하는 것이 의료 혁신의 핵심 과제로 부상하고 있다. 이런 이유로 HL7(Health Level Seven) 표준화 단체가 제시한 FHIR(Fast Healthcare Interoperability Resources)는 의료데이터 교환의 국제적 표준으로 자리 잡고 있다.[1, 2] FHIR는 RESTful API 기반의 경량 구조를 채택함으로써 기존 HL7 v2, v3의 복잡한 메시지 포맷을 단순화하고, JSON 및 XML 기반 표현을 통해 웹 서비스, 클라우드, 모바일 환경과의 호환성을 극대화하였다. 그 결과 병원정보시스템(HIS), 임상데이터웨어하우스(CDW), 연구데이터플랫폼 등 다양한 시스템 간 실시간 데이터 교환이 가능해지며, 의료기관 간 데이터 연계와 환자 중심 서비스 구현을 촉진하고 있다.

그러나 이러한 개방적 구조는 동시에 새로운 보안 위협을 야기한다. RESTful API는 HTTP 기반으로 작동하기 때문에, 전송 중인 요청(Request)과 응답(Response) 메시지에 환자식별정보(Personally Identifiable Information, PII)나 민감정보(Protected Health Information, PHI)가 포함될 수 있으며, 이들이 암호화 구간 외부에서 노출될 가능성이 존재한다. 특히 개발 환경 또는 외부 연계 시스템에서 잘못된 접근 권한 설정, 로그 관리 부재, 비정상 API 호출 등으로 인해 민감정보가 유출될 위험이 상존한다. 기존의 네트워크 계층 보안기법(예: 방화벽, SSL/TLS 암호화, 침입탐지시스템 등)은 이러한 응용계층(Application Layer) 수준의 위협을 완전히 차단하기 어렵다. 즉, 패킷 단위의 전송 보안만으로는 FHIR 메시지 단위에서 발생하는 데이터 접근 행위를 감시하거나, 비정상 요청 패턴을 실시간 탐지하는 데 한계가 있다. 이에 따라 최근 의료기관에서는 응용계층 수준의 모니터링 체계(Application-Layer Traffic Monitoring)를 통해 API 호출 로그를 분석하고, 민감정보 탐지 및 이상 행위를 조기 식별하려는 연구가 활발히 진행되고 있다[3].

또한 본 연구는 기존 네트워크 보안체계의 한계를 넘어, FHIR 메시지 수준의 세밀한 가시화 및 추적(Traceability)을 가능하게 하는 새로운 보안 아키텍처의 방향성을 제시한다. 향후 본 시스템은 머신러닝 기반 이상탐지 기법과 결합함으로써 지능형 보안 인프라(Intelligent Security Infrastructure)로 확장될 수 있으며, 의료데이터의 안전한 활용과 신뢰성 확보를 위한 기반 기술로 발전할 가능성을 갖는다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 HL7 FHIR의 기술적 개요와 관련 연구를 검토하고, Ⅲ장에서는 제안하는 HL7 FHIR 트래픽 모니터링 시스템의 구조와 동작 원리를 상세히 설명한다. Ⅳ장에서는 시스템의 기대효과 및 향후 확장 방향을 논의한다.

Ⅱ. 관련연구

HL7 FHIR은 기존 HL7 v2, v3 메시지 표준의 복잡성과 한계를 극복하기 위해 제안된 차세대 의료데이터 교환 표준으로, JSON(JavaScript Object Notation)과 XML(eXtensible Markup Language)을 지원하는 RESTful API 구조를 기반으로 한다. 이에 따라 웹 서비스 및 클라우드 환경과의 호환성이 뛰어나고, 다양한 의료 정보 시스템 간의 상호운용성을 효과적으로 강화할 수 있어 전 세계적으로 FHIR 표준의 도입 사례가 빠르게 증가하고 있다. Vorisek 등(2022)은 FHIR 관련 연구를 체계적으로 검토하면서 데이터 수집, 분석, 표준화 측면에서 다양한 활용 가능성을 제시하였으나, 보안 및 개인정보 보호에 대한 연구는 상대적으로 부족하다고 지적하였다[4]. Kim Hoang Le 등(2024)은 FHIR 기반 온라인 의료 데이터 관리 시스템을 설계·구현하면서 마이크로서비스 아키텍처를 적용하여 데이터 흐름의 가시성과 자원 단위의 접근 통제가 중요함을 강조했다[5]. 그러

나 해당 연구 역시 데이터 보안 위협이나 개인정보 보호보다는 서비스 운영 효율성에 중점을 두고 있어, 실제 의료 환경에서 요구되는 데이터 보안 위협 및 개인정보 유출을 탐지하는 실질적인 모니터링 체계로 확장되기에는 한계가 있다.

Ⅲ. 시스템 설계

본 연구는 HL7 FHIR 기반의 의료데이터 교환 환경에서 발생하는 트래픽을 응용계층(Application Layer) 수준에서 직접 수집·분석할 수 있는 모니터링 시스템을 설계하였다. 이는 단순한 네트워크 패킷 감시를 넘어, 실제 FHIR 메시지의 구조적 의미와 데이터 흐름을 파악하여 비정상 행위를 조기에 탐지하는 것을 목표로 한다. 제안된 시스템의 전체 구조는 [그림 1]과 같으며, 주요 기능은 트래픽의 복제(Mirroring)에서부터 정제(Pre-Processing), 저장(Data-Store), 분석 및 시각화(Monitoring)까지 단계적으로 구성되어 있다. 각 모듈은 상호 독립적으로 동작하면서도, 전체 데이터 흐름 내에서 유기적으로 연결되어 의료데이터 보안 관리의 완전성을 확보하도록 설계되었다.

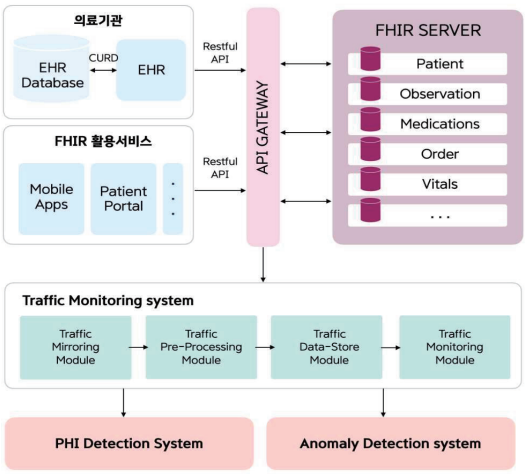

그림 1. 시스템 구성도

Traffic Mirroring 모듈에서는 운영 중인 FHIR 서비스의 성능에 영향을 주지 않으면서 API의 트래픽을 안전하게 복제하여 분석 시스템으로 전달한다. Traffic Pre-Processing 모듈에서 전달받은 트래픽에서 불필요한 데이터를 제거하고, 개인정보 탐지 및 이상 행위 분석에 적합하도록 정형화된 데이터로 파싱 및 변환한다. Traffic Data-Store 모듈은 전달받은 데이터와 전처리된 데이터를 저장하여 정상 및 비정상 트래픽 패턴과 공격 시나리오 기반 학습을 위한 데이터셋을 제공하고, 통계 기반의 추세 분석이 가능하도록 지원한다. 마지막으로 Traffic Monitoring 모듈은 저장된 데이터를 기반으로 실시간 트래픽을 분석하여 비정상 접근 및 개인정보 유출 가능성을 조기에 탐지하며, 이를 탐지 이벤트 기반 대응 체계와 연계함으로써 차세대 의료 데이터 보안 인프라로서의 역할을 수행한다.

본 시스템을 기반으로 데이터 전송 과정에서의 보안 위협을 최소화하고, 안전한 데이터 활용을 보장하는 모니터링 체계를 구현하기 위해 FHIR 시스템의 트래픽 내에서 발생할 수 있는 비정상 패턴을 효과적으로 식별하고, PHI(Protected Health Information)와 같은 민감 정보의 노출 여부를 탐지할 수 있도록 확장 가능한 형태로 설계되었다.

Ⅳ.결론

본 연구에서는 HL7 FHIR 환경에서 발생하는 API 트래픽을 응용계층에서 직접 수집·정제·분석할 수 있는 트래픽 모니터링 시스템 설계 방안을 제시하였다. 제안된 시스템은 기존의 네트워크 계층 중심 보안체계가 갖는 한계를 보완하고, 실제 FHIR 메시지 단위에서의 데이터 흐름을 가시화함으로써 의료데이터 전송 경로 전반의 투명성과 신뢰성을 확보할 수 있도록 한다. 본 연구 장점은 네트워크 보안에서 응용계층 보안으로의 전환(paradigm shift)을 구체적인 시스템 구조로 제시했다는 점이다. 기존에는 암호화나 방화벽 등 전송 구간의 보안에 초점이 맞춰졌다면, 연구에서는 실제 데이터 객체(FHIR 리소스)의 이동과 접근을 감시함으로써, 의료데이터 관리의 실질적 보안성과 감사(Compliance Traceability)를 높이고자 했다. 이는 향후 의료기관의 데이터 거버넌스 강화, 가명정보 처리 구역 관리, 보안감사 자동화 시스템 구축 등에 중요한 기초 기술로 활용될 수 있다.또한, 제안된 구조는 단순한 모니터링 시스템을 넘어 인공지능 기반 지능형 보안 인프라(ML-driven Security Infrastructure)로의 확장을 염두에 두고 설계되었다. 향후 머신러닝 기반 이상 탐지 모델을 결합할 경우, 정상 트래픽 패턴의 학습과 비정상 행위의 자동 분류가 가능해져 실시간 대응 능력이 비약적으로 향상될 것이다. 나아가 다양한 병원 환경과 클라우드 네이티브 플랫폼(Kubernetes, Docker 등)에 적용될 수 있는 범용 보안 프레임워크로 발전할 잠재력을 지닌다.

본 연구의 경우 아직 설계 중심의 제안 단계이지만, 실제 의료기관의 FHIR 서버 환경에서 프로토타입을 구현하고 실 트래픽 데이터를 기반으로 검증을 수행한다면, 의료데이터 보안 분야에서 실질적인 기술적 성과를 기대할 수 있다. 그리고 향후에는 PHI 탐지 알고리즘의 정밀도 향상, 이상 트래픽 탐지 정확도 향상을 위한 피드백 루프 설계, 보안 이벤트 기반 자동 대응체계(Incident Response Automation) 구축, FHIR 로그 기반 감사 및 인증 프레임워크 확립 등으로 연구를 확장할 계획이다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-지역지능화혁신인재양성사업의 지원을 받아 수행된 연구임 (IITP-2025-RS-2023-00260267)

참 고 문 헌

[1] Tabari, P., Costagliola, G., De Rosa, M., and Boeker, M., "State-of-the-Art Fast Healthcare Interoperability Resources (FHIR) - Based Data Model and Structure Implementations: Systematic Scoping Review," JMIR Medical Informatics, Vol. 12, e58445, Sep. 2024.

[2] HL7 International and Firely, "2025 State of FHIR® Survey Results," May 2025, (https://hl7chile.cl).

[3] Avireneni, R. T. (2025). API-Driven Security and Compliance in Digital Health Infrastructure: Leveraging Middleware for Comprehensive Protection of Patient Data. European Journal of Computer Science and Information Technology, 13(34), 49-59.

[4] Vorisek, C. N., Bruland, P., Dugas, M., and Fritz, F., "Fast Healthcare Interoperability Resources (FHIR) for interoperability in health research: Systematic review," JMIR Medical Informatics, Vol. 10, No. 7, e35724, Jul. 2022.

[5] Le, T. K. H., Kongsiriwattana, W., Meny, A., and Kaewsaeng-On, R., "Enhancing healthcare interoperability with FHIR: A systematic approach to online data management," Proc. 9th International Conference on Information Systems Engineering (ICISE), 2024, pp.