AI 기반 디지털 의료기기 소프트웨어 자재명세서(SBOM) 구현

이준희*, 유도진**, 이용준**
*극동대학교 인공지능보안학과 석사과정
**극동대학교 해킹보안학과 교수
e-mail:201963026@student.kdu.ac.kr

Implementing of AI-Based Digital Medical Device Software Bill of Materials

Jun-Hee Lee*, Do-Jin Yoo**, Young-Jun Lee**
*Dept. of AI Security, Far East University
**Dept. professor of Hacking Security, Far East University

요 약

디지털 의료기기의 발전으로 환자 치료의 효율성과 효과성이 높아졌지만, 이로 인한 사이버 보안 위험도 증가하고 있다. 특히 의료기기 제조업체의 서드파티 소프트웨어 컴포넌트 활용에 따른 취약점은 의료기기 전반의 보안을 위협하고 있다. 이에 본 연구는 소프트웨어 자재 명세서 활용을 통해 디지털 의료기기의 사이버 보안 강화를 위한 SBOM 구현의 필요성을 제시한다.

1. 서론

의료기기 산업은 4차 산업혁명과 함께 디지털화가 가속화되고 있다. 이에 따라 의료기기의 성능과 기능이 향상되면서, 환자 치료의 효율성과 효과성이 크게 개선되고 있다. 그러나 이러한 디지털 의료기기의 발전은 사이버 보안 위험 증가로 이어지고 있다. 특히 의료기기 제조업체가 서드파티 소프트웨어 컴포넌트를 활용함에 따라 발생하는 취약점은 의료기기 전반의 보안을 위협하는 주요 요인이 되고 있다[1].

SBOM을 활용하여 디지털 의료기기의 소프트웨어 구성 요소를 투명하게 공개함으로써 사이버 보안 위험을 관리하고자 한다. SBOM은 의료기기 제조업체와 사용자 간 소프트웨어 투명성을 높여 사이버 보안 위험 관리에 활용될 수 있다. 특히 디지털 헬스케어 분야에서 SBOM의 적용은 환자 데이터 보호와 디지털 헬스케어 기기 안정성 확보에 필수적이다[1].

본 연구에서는 사용자의 정신 건강 관리를 위한 다양한 기능과 치료를 제공하는 디지털 의료기기인 전문 심리상담 앱 세 가지를 대상으로 디지털 의료기기의 SBOM을 구현하고, SBOM 항목 중 저자가 재구성하여 선정한 열 가지 항목의 데이터 현황을 분석하였다. 2장에서는 관련 연구를 분석하며, 3장에서는 논문의 실험 구성도와 연구의 방법을 제안한다. 또한 4장에서는 연구 및 실험에 대한 구현을 진행한다. 5장에서는 연구 및 실험에 대한 실증 평가를 제시하고 마지막으로 6장에서는 결론으로 실험 내용을 정리하며 마친다.

2. 관련 연구

현대 보건의료 분야는 디지털 혁신을 통해 진보하고 있으며, SBOM은 기본 또는 보조 자원으로서 제품 수명 전주기 전반의 사이버보안 위험 관리 절차 개선을 지원할 수 있다[1]. 이를 통해 의료기기의 소프트웨어 구성 요소를 더 빠르고 포괄적으로 식별하고, 더 나은 정보에 기반한 의사 결정으로 더욱 안전하고 신뢰할 수 있는 의료기기 소프트웨어 개발을 지원하며, 의료기기 제조업체와 사용자 간의 의료기기 소프트웨어의 구성 및 취약점에 대한 투명성을 높일 수 있다.

본 연구는 디지털 의료기기의 소프트웨어 투명성을 보장하기 위해 중요한 구성 요소인 SBOM의 관련 연구를 분석하고, 디지털 의료기기의 SBOM을 구현해 개선점을 제시하고자 한다.

2.1 공급망 보안의 주요 위협 사례

소프트웨어 공급망 공격은 국내외를 막론하고 전 세계적으로 발생하고 있으며, 그 피해 또한 심각한 수준에 이르고 있다. 따라서, 소프트웨어 공급망 공격을 각국은 사이버 보안의 최대 위협 중 하나로 다루고 있다[3]. 소프트웨어 공급망 공격은 공급업체의 취약점을 악용하여 악성코드를 유포하거나, 정상적인 소프트웨어에 악성 요소를 삽입하는 등의 방식으로 이루어진다.

[표 1] 공급망 공격 위협 사례

Major Incidents	Main Contents
솔라윈즈 해킹	- 2020년 IT 관리솔루션의 업데이트 파일에선 버스트 악성코드 감염 - 美국방부 등 200여 기관과 IT 기업을 포함한 18,000곳이 해킹 피해
MS Exchange Server 해킹	- 2021년 MS사 Exchange Server 해킹, 정부, 기업 등 미국만 3만 개 피해 - 공격자는 중국 하프니움(Hafnium) 해킹그룹의 소행으로 추정
kaseya 해킹 사건	- 2021년 미국 Kaseya의 원격관리 도구 통해 악성코드 유포 - 소디노키비 랜섬웨어가 유포되어 최대 2,000개 기관에 피해가 발생
Log4j 취약점	- 2021년 서버 대부분에 사용되는 오픈소스 Log4j에 위험도 최고 취약점 발견 - 악용한 벨기에 국방부 등 공격, 패치를 하고 있으나 아직 위험 상존
Protestware 등장	- 2022년 러시아의 우크라이나 침공에 항의하기 위해 오픈소스 개발자가 자신의 라이브러리에 악성 기능삽입 - 이를 재사용하는 응용프로그램과 그 사용자에게 피해 확산

[표 1]에서 확인된 바와 같이, 공급망 보안에 대한 주요 위협 사례들이 지속적으로 발생하고 있음을 알 수 있다. 2020년부터 2021년까지 다양한 기업들이 랜섬웨어 공격, 악성코드 삽입, 서버 취약점 등의 공격에 노출되었다. 공격을 받은 기업 및 시설을 살펴보면 보안이 약한 기업이 아닌 각국의 국방부와 관련 기관들에 대한 공격과 대기업 및 수많은 기업이 포함된다. 이러한 공격들은 공급망의 구조적 취약성을 이용한 조직적인 범죄 활동을 나타내며, 사례들은 공급망 보안의 중요성을 강조하며, 기업들이 이에 대한 대책 마련이 시급함을 보여준다. 따라서 이 연구에서는 이러한 공급망 보안 위협 사례들을 분석하고, 효과적인 대응 방안을 모색할 필요가 있다.

2.2 SBOM(Software Bill of Materials)

SBOM(Software Bill of Materials)은 소프트웨어 구성요소의 전체 목록으로, 해당 소프트웨어에 포함된 모든 라이브러리, 패키지, 모듈 등의 출처, 버전, 라이선스 정보를 제공한다. SBOM은 개발자가 사용하는 오픈소스 및 서드파티 컴포넌트를 추적하고, 이러한 컴포넌트의 보안 취약점이 발견될 경우, 즉각적인 조치를할 수 있도록 한다. 이를 통해 SBOM은 소프트웨어 감사, 컴플라이언스 확인, 보안 관리에서 중요한 역할을 수행하며, 투명성과 신뢰성을 높이는 데 기여할 수 있다[2]. 특히 보건의료 분야에서 SBOM은 디지털 의료기기 소프트웨어의 사이버 보안 강화를 제고할 수 있다.

2.1 AI(Artificial Intelligence)

최근 AI는 실생활에 있어서 점차 많은 부분의 비중을 차지하고 있는 추세로, AI에 대한 연구가 지속적으로 이루어지고 있다[2]. 그 결과, 심리상담 앱에 AI 기술이 탑재되어 AI 챗봇 및 AI 상담 서비스가 가능해졌다. 이러한 AI 기반 심리상담 서비스는 사용자의 편의성을 높이고, 전문가의 도움이 필요한 이들에게 보다 쉽게 접근할 수 있는 기회를 제공하고 있다.

따라서 본 논문의 SBOM 구현 대상인 'Trost', 'Mindcafe', 'Ollacare'의 주요 기능을 비교하며, AI 기술 탑재 여부를 수동으로 조사하였다.

[표 3] 'Trost', 'Mindcafe', 'Ollacare' 기능 비교

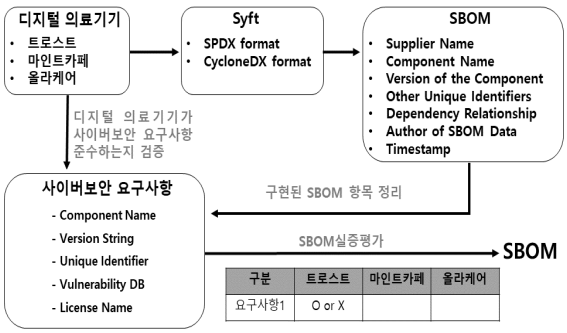
구분	Trost	Mind cafe	Ollacare
상담 방식	1대1 실시간 채팅	화상 상담, 실시간 채팅	비대면 진료
상담 내용 기록	비밀 보장	녹음 및 기록 가능	비밀 보장
AI 탑재	AI 챗봇	AI 챗봇	N/A

'Trost'는 전문 심리상담사와 1대1 실시간 채팅 상담을 제공하며, 상담 내용 비밀 보장으로 심리적 건강을 지원하고 AI 챗봇이 탑재되어 있다. 'Mindcafe'는 화상 상담, 실시간 채팅 등 다양한 상담 방식을 제공하고, 상담 내용 기록 및 일정 관리 기능으로 체계적인 관리가 가능하고 AI 챗봇이 탑재되어 있다. 'Ollacare'는 비대면 진료와 심리상담, 건강관리 기능을 통합하고 있지만 AI 챗봇이 탑재되어 있지 않은 앱이다.

3. 제안 사항

다양한 국제 안보 갈등 관계로 인해 다수의 사이버 공격 피해를 경험한 미국은 이미 2015년부터 공급망 위협을 주요한 사이버 위기관리의 대상으로 인식하고 전문 연구기관(NIST)을 통해 공급망 보안 국가 표준(SP800-161)과 사이버 보안 프레임워크(CSF)로 개발, 발생할 수 있는 사이버 위협요인을 사전 식별하고 효과적으로 관리하기 위한 체계를 마련했다[4].

본 연구에서는 사용자의 정신 건강 관리를 위한 다양한 기능과 치료를 제공하는 디지털 의료기기인 전문 심리상담 앱 'Trost', 'Mindcafe', 'Ollacare'를 대상으로 SBOM을 구현하고자 한다. SBOM 구현을 통해 TTA[5]에서 제시한 15가지 SBOM 필수 항목 중 저자가 재구성하여 "Component Name", "Version String", "Unique Identifier", "Vulnerability DB", "License Name" 항목 등 열 가지 항목을 충족하는지 실증적으로 평가할 것이다.



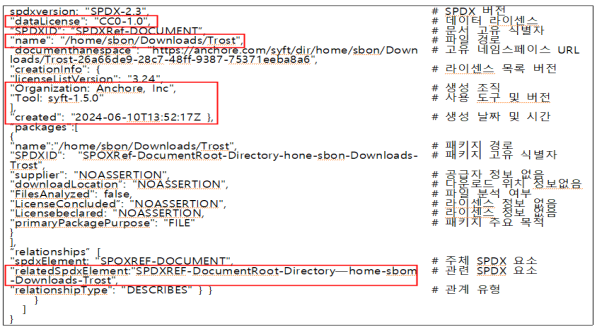
[그림 1] 실험 구성도

[그림 1]은 디지털 의료기기의 안전성을 강화하기 위한 효과적인 SBOM의 필요성에 대한 실험 구성도를 제시한다.

본 연구에서는 직접 SBOM을 구현하고, 이를 통해 도출된 개선점 및 제안사항을 바탕으로 디지털 의료기기에 SBOM 구현이 필수적임을 제시하고자 한다.

4. 디지털 의료기기 SBOM 구현

사용자의 정신 건강 관리를 위한 다양한 기능과 치료를 제공하는 디지털 의료기기인 전문 심리상담 앱 'Trost', 'Mindcafe', 'Ollacare'를 대상으로 SBOM 구현을 진행하였다.



[그림 2] trost digital medical device SBOM implementation

생성된 SBOM에는 "/home/sbom/Downloads/trost" 디렉터리에 대한 정보가 포함되어 있었다. 해당 SBOM에서는 다양한 정보를 확인할 수 있지만, 저자가 재구성한 SBOM 항목에 대해서는 여섯 가지 정도만 확인할 수 있었고, 나머지 항목에 대한 데이터는 명시되어 있지 않았다. 이러한 한계점은 향후 SBOM 생성 및 관리 프로세스를 개선하는 데 있어 고려해야 할 사항으로 확인되었다.

5. 제안 평가

본 연구에서는 TTA[5]에서 제시한 15가지 SBOM 필수 항목 중 저자가 재구성하여 열 가지 항목을 선정하여, AI 기반 디지털 의료기기에 대한 SBOM 구현과 평가를 진행하였다. 선정된 열 가지 SBOM 항목은 "SBOM Validation Tool Name", "Supplier Name", "Author Name", "Component Name", "Version String", "License Name", "Unique Identifier", "Component Hash", "Timestamp", "Relationship"이다. 이를 통해 의료기기 SBOM의 구축 현황과 개선 방향을 확인하고자 하였다. 연구 결과, 일부 SBOM 항목에 대한 정보 누락이 확인되어, 의료기기 SBOM 구축의 완전성 제고가 필요함을 시사하였다. 이는 의료기기 보안 관리와 지속적인 유지보수를 위한 SBOM 정보의 체계적인 관리의 중요성을 보여준다.

[표 4] Evaluation of Software Component Information for Digital Medical Devices

Category	Trost	Mindcafe	Ollacare
SBOM Validation Tool Name	O	O	O
Supplier Name	X	X	X
Author Name	O	O	O
Component Name	O	O	O
Version String	X	X	X
License Name	O	O	O
Unique Identifier	O	O	O
Component Hash	X	X	X
Timestamp	O	O	O
Relationship	X	X	X

세 가지 AI 기반 디지털 의료기기에 대한 SBOM 구현 결과를 분석하였다. SBOM 정보 항목 중 "SBOM Validation Tool Name"과 "Author Name", "Component Name", "License Name", "Unique Identifier", "Timestamp" 항목에 대한 데이터는 모든 의료기기에서 확인되었으나, "Supplier Name", "Version String", "Component Hash", "Relationship" 항목에 대해서는 정보가 누락되어 있었다. 의료기기의 보안 관리와 지속적인 유지보수를 위해서는 SBOM 정보의 완전한 확보가 필요하다.

6. 결론

본 연구에서는 디지털 의료기기의 사이버 보안 강화를 위해 SBOM 구현 및 분석을 수행하였다. 의료기기 산업의 디지털화와 함께 증가하는 사이버 보안 위험에 대응하기 위해 SBOM은 중요한 역할을 할 수 있다.

분석 결과, 세 가지 AI 기반 디지털 의료기기의 SBOM을 구현하고 주요 항목을 분석한 결과, SBOM 정보 항목 중 "SBOM Validation Tool Name"과 "Author Name",

“Component Name”, “License Name”, “Unique Identifier”, “Timestamp” 항목에 대한 데이터는 모든 의료기기에서 확인되었으나, “Supplier Name”, “Version String”, “Component Hash”, “Relationship” 항목에 대해서는 정보가 누락되어 있었다. 이는 SBOM 구축의 완전성이 부족함을 보여준다.

SBOM 정보의 확보는 의료기기 보안 강화를 위해 필수적이다. SBOM 정보의 체계적인 관리 및 활용 방안을 심도 있게 탐구할 필요가 있다.

따라서, 향후 디지털 의료기기 제조업체와 관련 정책 당국은 SBOM 구축과 관리에 중점을 두어야 할 것이다. 이를 통해 의료기기의 사이버 보안 수준을 높이고, 안전하고 신뢰할 수 있는 디지털 의료기기를 제공할 수 있을 것으로 기대된다.

참고문헌

[1] 식품의약품안전처 의료기기안전국. “의료기기 사이버보안을 위한 소프트웨어 자재명세서 원칙 및 실무“. 2023.

[2] 김희연. ″디지털 헬스케어 기기의 딥러닝 기반 SBOM 결함 탐지 기법.” 국내석사학위논문 아주대학교 일반대학원, 2024.

[3] 이형동. ″사이버보안을 위한 소프트웨어 자재명세서(SBOM)의 도입의도에 영향을 미치는 요인에 관한 연구.″ 국내박사학위논문 숭실대학교 일반대학원. 2023.

[4] 김진민, 위성승, 김낙일, 신용태. ”국내 S/W 공급망 보안을 위한 사이버안보 정책방안 연구“. 한국전자거래학회지, 28(1), 2023, 29-53.

[5] 한국정보통신기술협회. ”공개 소프트웨어 공급망 관리를 위한 소프트웨어 목록 구성속성 (SBOM) 규격.“ 2022.