엣지 및 클라우드 컴퓨팅 패러다임에 대한 지속 가능한 연합 강화 학습 연구

우정현[1], 김성원[2], 서병석[3], 고광만[4]
[1,2,3,4]상지대학교 컴퓨터공학과
e-mail : 2023015102@sj.sangji.ac.kr, 2023015003@sj.sangji.ac.kr,
seobs@sangji.ac.kr, kkman@sangji.ac.kr

User A Study on Sustainable Edge and Cloud Computing Paradigm based on Federated Reinforcement Learning

Jung-Hyun Woo[1], Sung-Won Kim[2], Byung-seokSeo[3], Kwang-Man Ko[4]
[1,2,3,4]Dept. of Computer Engineering, Sang-Ji University

요 약

엣지-클라우드 통신네트워크에서의 지속 가능한 사이버 보안 솔루션을 개발하기 위한 연구는 중요성을 갖는다. 최근의 기술 발전으로 인해 엣지 디바이스와 클라우드 서비스 간의 통신이 활발해지면서 보안 위협이 증가하고 있다. 이에 따라 연합 강화 학습과 같은 첨단 기술을 활용하여 보안 취약점을 탐지하고 대응하는 것이 중요하다. 본 논문에서는 엣지-클라우드 환경에서의 보안 취약점을 식별하고 대응하기 위해 연합 강화 학습을 기반으로 한 솔루션을 제안한다. 이를 통해 네트워크의 안전성을 보장하고 사이버 공격에 대응할 수 있는 기술을 개발하기 위해, 엣지-클라우드 환경에서의 보안 취약점을 식별하고 대응하기 위해 연합 강화 학습 기반으로 한 솔루션을 소개한다.

1. 서론

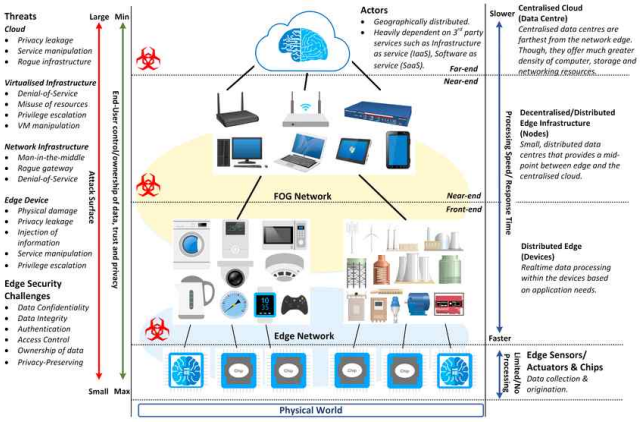
유·무선 통신 네트워크의 급속한 성장과 함께 정보 보안의 중요성이 더욱 높아지고 있다. 인터넷의 전반적인 보급과 빅데이터의 활용이 증가함에 따라, 유·무선 통신의 중요성이 한층 강조되고 있으며 이에 따라 보안 요구도 증가하고 있다. 이러한 상황에서 엣지 디바이스들과 엣지 서버의 등장으로 인해 데이터 처리와 학습을 현장에서 바로 수행할 수 있게 되었다. 이로써 유·무선 네트워크에서 보안 취약점을 효과적으로 탐지하고 공격에 대응하기 위한 인공지능 기반의 연구가 촉진되고 있다. 이러한 맥락에서 연합 학습 기술의 발전이 주목받고 있다. 연합 학습은 여러 기기가 협력하여 데이터를 공유하지 않고도 학습할 수 있도록 하여, 보안 위협을 최소화하면서 학습 효율과 성능을 극대화할 수 있는 기술로 자리매김하고 있다. 연합 학습과 같은 첨단 기술의 발전은 이러한 보안 요구를 충족시키는 데 중요한 기여를 하고 있다. 연합 학습은 분산된 데이터를 활용하여 학습 효율과 성능을 극대화하는 동시에, 각 참여 장치에서 데이터를 직접 공유하지 않고도 협력할 수 있게 한다. 이로 인해 데이터의 기밀성과 무결성을 유지하면서 보안 문제를 해결할 수 있다. 특히, 엣지-클라우드 통신 네트워크에서 다양한 데이터가 생성되고 처리되는 환경에서, 연합 학습은 보안성을 강화하는 데 필수적인 도구가 되고 있다. 데이터 보안의 중요성은 기업, 정부, 개인의 프라이버시와 신뢰성에 직접적인 영향을 미친다. 데이터 유출이나 변조가 발생하면 심각한 재정적 손실과 평판 손상을 초래할 수 있으므로, 인공지능과 관련된 데이터의 보안을 강화하는 기술이 절실히 필요하다. 연합 강화학습은 이러한 측면에서 중요한 기술로 부상하고 있으며, 사이버 보안과 인공지능의 융합을 통해 미래 디지털 인프라의 보안 패러다임을 성장시킬 수 있는 잠재력을 가지고 있다. 엣지-클라우드 통신 네트워크는 엣지 디바이스, 로컬 컴퓨팅 노드, 디바이스 간의 통신 등 다양한 데이터 소스를 포함하고 있어, 이들 각각에 적합한 보안 기술을 개발하고 적용하는 것이 중요하다. 시스템의 규모가 커짐에 따라 각 요소 및 요소 간의 보안 위협과 취약점을 일일이 검사하는 것은 점점 더 어려워지고 있다. 이에 자동으로 보안 위협을 검사할 수 있는 도구의

개발이 필요하며, 효율적인 투자를 위해서는 보안 기술을 집중적으로 적용할 수 있는 분야를 신중하게 선택해야 한다. 이와 같은 연구와 개발을 통해 보안과 효율성을 동시에 향상시킬 수 있으며, 이는 현대 통신 환경에서의 안정성과 신뢰성을 높이는 데 중요한 역할을 할 것이라고 생각한다.

2. 관련 연구

엣지 컴퓨팅은 클라우드와 함께 다양한 인프라 기능을 제공하며, 데이터 처리와 서비스 제공을 지원한다. 그러나 엣지 컴퓨팅 환경에서는 보안 문제가 심각한 고려사항으로 대두되고 있는 상황이다. 클라우드에서 엣지 디바이스로의 데이터 이동 과정에서는 다양한 보안 위협이 발생할 수 있다. 이러한 위협은 데이터 유출, 악성 코드 삽입, 서비스 조작, 권한 확대 등의 형태로 나타날 수 있다.

특히 사생활 유출 문제는 엣지 디바이스에서 수집된 민감한 개인 정보가 불법적으로 노출되는 경우를 의미한다. 정보 주입은 악의적인 공격자가 엣지 디바이스에 가짜 정보를 삽입하여 시스템을 혼란시키는 것을 의미한다. 서비스 조작은 엣지 디바이스의 서비스가 악성 코드에 의해 조작되어 사용자에게 해로운 결과를 초래하는 것을 의미한다. 또한 권한 확대는 악의적인 공격자가 엣지 디바이스에서 비인가된 권한을 획득하여 시스템에 대한 접근 권한을 확대하는 것을 의미한다.

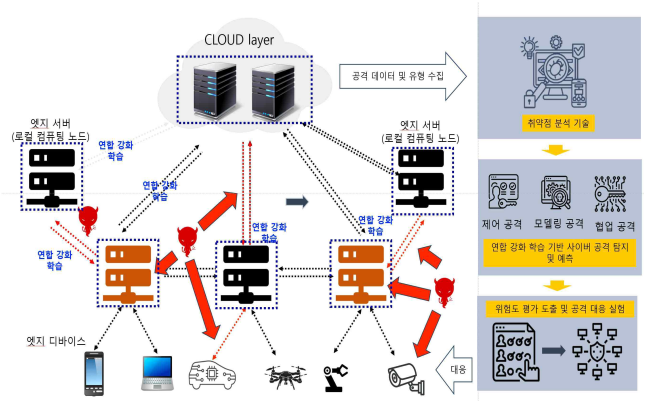


[그림 1. 엣지-클라우드 인프라 기능]

이에 따라 최근에는 엣지 보안에 대한 연구가 활발히 이루어지고 있으며, 다양한 보안 문제에 대한 연구와 관련된 다양한 과제들이 존재하고 있다. 이러한 연구들은 엣지 컴퓨팅 환경에서의 보안 위협에 대응하고, 안전하고 신뢰할 수 있는 서비스 제공을 지원하기 위한 것이다.

3. 연구 설계 방향

연구의 목표는 엣지-클라우드 통신네트워크에서 발생하는 다양한 보안 위협을 식별하고 대응하는 연합 강화 학습 기반의 사이버 보안 모델을 개발하는 것이다.



[그림 2. 연합강화학습 엣지-클라우드 통신네트워크]

3-1. 문제 정의: [그림2]와 같이 엣지-클라우드 통신네트워크에서의 보안 문제와 취약점을 식별하고, 연합 강화 학습을 적용하여 이에 대응하는 효과적인 모델을 개발한다. 이를 위해 다음과 같은 구체적인 목표를 설정한다. 엣지-클라우드 통신에서 발생하는 보안 위협의 종류와 특성을 분석하고 문제를 명확히 정의한다. 연합 강화 학습을 통해 식별된 보안 취약점에 대응할 수 있는 새로운 방법을 개발한다.

3-2. 변수 정의

(1) 독립 변수: 네트워크 구성 요소 (예: 엣지 디바이스, 클라우드 서버), [그림1]과 같이 보안 위협 유형을 살펴보면 (데이터 유출, 악성 코드 삽입), 데이터 특성(데이터 양, 속도) 등이 있다.

(2) 종속 변수: 보안 위협 탐지 및 대응의 성능 지표 (정확도, 탐지율, 거짓 양성률 등)를 평가한다.

연구 모델 설계: 연합 강화 학습을 기반으로 한 사이버 보안 모델을 설계하고, 이를 위한 구체적인 알고리즘 및 기술을 정의한다. 연구 모델 설계 단계에서는 다음과 같은 절차를 따른다.

엣지-클라우드 통신에서 발생하는 보안 위협의 특성을 고려하여 강화 학습 모델을 설계한다.

보안 취약점 탐지 및 대응을 위한 알고리즘을 개발하고 구현한다.

연합 학습을 통해 다양한 엣지 디바이스와 클라우드 서버 간의 협력을 강화한다.

이와 같은 연구 설계를 통해 보안 모델의 효율성과 신뢰성을 높일 수 있다.

4. 결론

본 연구에서는 엣지-클라우드 통신네트워크의 보안 강화를 위한 전략적인 솔루션을 제시하였다. 이를 통해 사이버 보안에 대응하기 위한 효과적인 방법을 제안한다.

먼저, 엣지-클라우드 통신네트워크에서의 보안 위협 관리와 사이버 공격 대응을 강화하기 위해 데이터 수집과 분석이 중요하다. 이를 위해 실시간으로 네트워크 트래픽을 모니터링하고 이상 징후를 탐지하는 AI 기반의 솔루션을 제안한다.

둘째, 연합 강화 학습을 활용한 데이터 무결성과 사이버 위협 탐지 및 예측 모델의 개발은 보안 수준을 향상시키는 데 유용하다. 네트워크에서의 패턴을 학습하고 실시간으로 이상 징후를 감지하여 보안 사고에 신속하게 대응할 수 있도록 한다.

셋째, 보안 평가를 위한 테스트베드 구축과 사이버 보안 모델의 고도화는 보다 효과적인 보안 전략의 구축을 도움을 준다. 실제 환경에서의 시뮬레이션을 통해 보안 취약점을 식별하고 향후 사이버 공격에 대비하는 데 도움이 된다. 이를 통해 엣지-클라우드 통신네트워크의 보안을 보다 효과적으로 강화할 수 있을것으로 기대가 된다.

6. 참고 문헌

[1] Matthew Hagan, Fahad Siddiqui, Sakir Sezer “Enhancing Security and Privacy of Next-GenerationEdge Computing Technologies” PST. Fredericton, NB, Canada. 2019, pp 2-3

[2] 한채림, 이선진, 이일구 “산업용 사물 인터넷을 위한 프라이버시 보존연합학습 기반 심층강화학습모델” 정보보호학회, 이화여자대학교, 2023, pp 2-3