사물인터넷융복합논문지 Vol. 10, No. 2, pp. 77-84, 2024 https://doi.org/10.20465/KIOTS.2024.10.2.077

블록체인 기반의 보안 위협을 예방할 수 있는 IoT 엣지 아키텍처 모델

정윤수*
목원대학교 게임소프트웨어공학과 교수

IoT Edge Architecture Model to Prevent Blockchain-Based Security Threats

Yoon-Su Jeong*
Professor, Game Software Enginnering, Mokwon University

요 약 지난 몇 년 동안 5G와 같은 새로운 저 지연 통신 프로토콜을 기반으로 IoT 엣지가 등장하기 시작했다. 그러나, IoT 엣지는 막대한 이점에도 불구하고, 새로운 보완 위협을 초래하여 이를 해결하기 위한 새로운 보안 솔루션이 필요하다. 본 논문에서는 IoT 시스템을 보완하는 클라우드 환경기반의 IoT 엣지 아키텍처 모델을 제안한다. 제안 모델은 IoT 엣지 장치에서 추출한 네트워크 트래픽 데이터를 기계 학습에 작용하여 사전에 보안 위협을 예방한다. 또한, 제안 모델은 로컬 노드에서 보안 데이터 일부를 할당함으로써 액세스 네트워크(엣지)에서의 부하 및 보안을 보장한다. 제안 모델은 IoT 엣지 환경 중 로컬 노드에 데이터 처리 및 관리의 일부 기능을 할당함으로써 액세스 네트워크(엣지)의 부하를 더욱 줄이는 동시에 취약 부분을 안전하게 보호한다. 제안 모델은 다양한 IoT 기능을 네임 서비스로 가상화하고, 필요에 따라 하드웨어 기능과 충분한 계산 리소스를 로컬 노드에 배포한다.

주제어 : 사물인터넷, 엣지 네트워크, 블록체인, 보안 위협, 기계 학습

Abstract Over the past few years, IoT edges have begun to emerge based on new low-latency communication protocols such as 5G. However, IoT edges, despite their enormous advantages, pose new complementary threats, requiring new security solutions to address them. In this paper, we propose a cloud environment-based IoT edge architecture model that complements IoT systems. The proposed model acts on machine learning to prevent security threats in advance with network traffic data extracted from IoT edge devices. In addition, the proposed model ensures load and security in the access network (edge) by allocating some of the security data at the local node. The proposed model further reduces the load on the access network (edge) and secures the vulnerable part by allocating some functions of data processing and management to the local node among IoT edge environments. The proposed model virtualizes various IoT functions as a name service, and deploys hardware functions and sufficient computational resources to local nodes as needed.

Key Words : IoT; Edge Network; Blockchain; Security Threat; Machine Learning

*교신저자 : 정윤수(bukmunro@mokwon.ac.kr)
접수일 2024년 02월 27일 수정일 2024년 03월 12일 심사완료일 2024년 03월 27일

1. 서론

사물인터넷(IoT)은 다양한 분야에서 빠르게 확대 사용되고 있으며, IoT와 관련된 보안 문제는 점점 더 중요시되고 있다. IoT 장치가 일상생활에서 점점 더 널리 보급되면서 해커가 민감한 데이터를 훔치거나 수정할 수 있으므로 IoT 장치와 CSP(Cloud Service Provider)의 적절한 보안은 데이터 전반의 기술과 보안을 지속하는 데 매우 중요하다[1-3].

IoT 시스템은 취약성과 더 많은 실시간 데이터 계산 및 통신에 대한 요구 증가로 인해 많은 로컬 엣지 장치에 연결되고 있다.

IoT 엣지 장치의 보안 공격은 일반적인 공격 중 서비스 거부(DoS)/분산 서비스 거부(DDoS) 공격, 정보 수집 공격, MITM(manin-the-middle) 공격, 주입 공격 및 멀웨어 공격 등이다[4]. 이러한 IoT 엣지 기반 생태계의 보안을 지원하기 위해 공격 탐지 및 분류를 사용하고 배치하여 공격이 발생하는 시기와 수행되는 특정 유형의 사이버 공격을 식별해야 한다. 또한, 머신 러닝(ML) 및 신경망 기술을 사용하여 다양한 유형의 공격을 인식하고 분류할 수 있도록 모델을 훈련할 수 있으며, 이를 통해 엣지에서 증가하는 사이버 공격을 보다 정확하고 시의적절하게 예방하고 대응할 수 있다[5,6].

IoT 엣지는 보안, 개인 정보 보호 및 안전이 신중하게 대처해야 할 중요한 측면이며, 복원력, 견고성 및 일반적으로 이러한 시스템의 올바른 동작을 보장하는 것이 어느 때보다 시급한 요구 사항이다[7]. 특히, 이러한 필요성을 해결하기 위한 수단으로서 보안 보장이 두드러진다. 전통적인 분산 시스템(예: 서비스, 클라우드)에 지속해서 적용되는 보장 기술은 이제 확장성 및 동적이고 복잡하지만 리소스가 제한된 시스템에 적응하는 능력 측면에서 하이브리드 엣지 및 IoT 시스템에서 제기되는 새로운 과제에 직면할 때 부족하다. 기존의 보안 보장 기술은 대상 시스템을 전체적으로 평가하는 데 실패하고 5G와 같은 새로운 모바일 네트워크를 고려하지 않아 기존 관행에 대한 완전한 재고를 요구한다.

본 논문에서는 클라우드 환경기반의 보안 위협을 방지할 수 있는 IoT 엣지 아키텍처 모델을 제안한다. 제안 모델은 IoT 엣지 장치에서 추출한 네트워크 트래픽 데이터를 기계 학습에 적용하여 IoT 엣지 공격을 사전에 예방한다. 또한, 제안 모델은 로컬 노드에서 데이터 처리 및 관리의 일부를 할당받아 액세스 네트워크(엣지)에서의 부하 및 보안을 보장한다. 제안 모델은 시스템의 각 IoT 엣지 장치가 컴퓨팅 집약적인 태스크를 갖는 것으로 가정한다. 이를 통해 제안 모델은 블록체인 기술을 기반으로 IoT 기기와 ECD(Edge Computing Devices) 간의 자원 정보 상호 작용을 수행한다. 제안 모델은 시스템 내 IoT 기기의 수가 ECD 보다 많다는 점을 고려하면, ECD가 IoT 기기를 서비스하는 과정은 여러 IoT 기기가 ECD에 컴퓨팅 자원을 요청하는 과정으로 단순화할 수 있다. 이는 제안 모델이 여러 컴퓨팅 집약적인 작업이 동시에 ECD에 오프로딩 요청을 발행하기 때문이다.

이 논문의 구성은 다음과 같다. 2장에서는 IoT 엣지 관련된 기존 연구를 분석한다. 3장에서는 클라우드 환경기반의 보안 위협을 방지할 수 있는 IoT 엣지 아키텍처 모델을 제안하고, 4장에서는 성과 평가를 수행한다. 마지막으로 5장은 결론을 맺는다.

2. 관련 연구

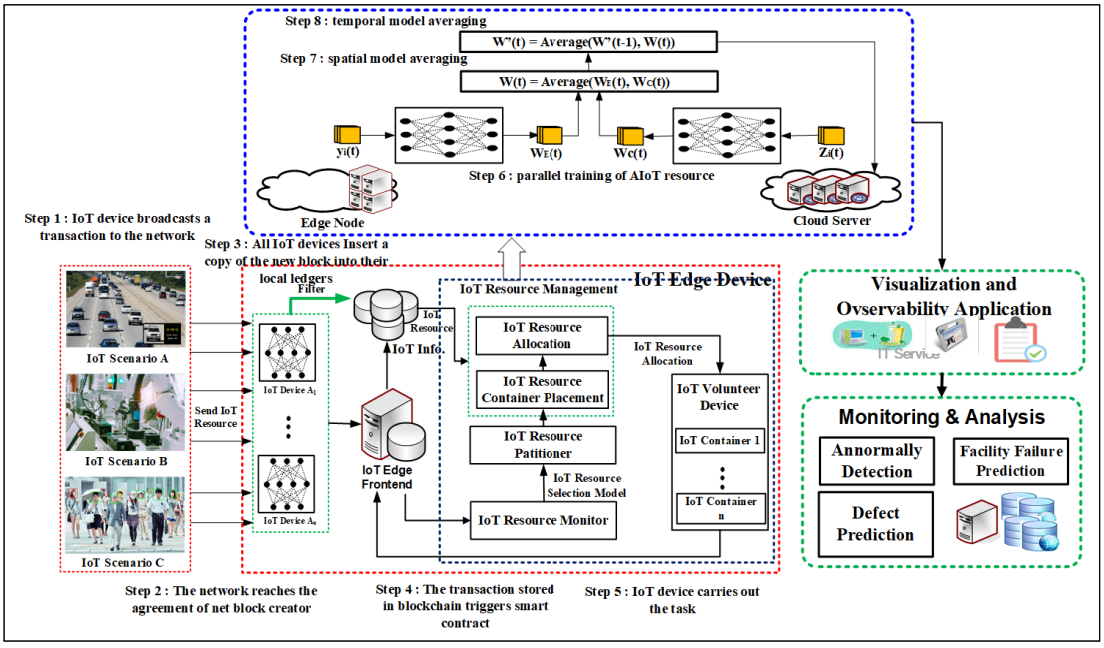
2.1 퍼블릭 블록체인 vs. 프라이빗 블록체인

퍼블릭 블록체인은 블록체인에서 누구나 참여하고, 읽고, 쓰고, 거래할 수 있는 탈중앙화된 네트워크입니다[8,9]. 누구나 네트워크에 참여하고, 합의 과정에 참여하고, 거래를 검증할 수 있는 허가를 받지 않는다. 퍼블릭 블록체인은 탈중앙화, 투명성, 무허가, 불변성 등의 특징이 있으며, 퍼블릭 블록체인의 대표적인 예로는 비트코인과 이더리움이 있다.

프라이빗 블록체인은 참여가 특정 개체 또는 개인으로 제한되는 중앙 집중식 네트워크이다[10]. 이는 참여자에게 네트워크에 가입하고 거래할 수 있는 권한이 부여되어야 한다. 액세스 제어 및 거버넌스는 중앙 기관 또는 신뢰할 수 있는 당사자의 컨소시엄에 의해 관리된다. 프라이빗 블록체인은 중앙 집중식 제어, 개인 정보 보호 및 기밀성, 확장성, 트랜잭션 처리 속도 향상 등의 특징이 있으며, 프라이빗 블록체인의 예로는 하이퍼레저 패브릭(Hyperledger Fabric)과 코르다(Corda)가 있다.

2.2 기존 연구

N. Almolhis et al. 은 마트 시티, 의료 및 스마트 홈을 포함하여 클라우드 IoT를 위한 솔루션이 개발된 여러 환경에 대해서 분석하였다[11]. 이 분석에서는 침입 탐지 시스템, 액세스 제어 모델 및 아키텍처, 보안 통신 프로토콜 사용, 다중 요소 인증, 사용자 활동 예측 분석 및 신원 기반 암호화가 포함된다.



[Fig. 1] Proposed Architecture for IoT Edge Security

I. Mohiuddin et al. 은 IoT 내 클라우드 기반 서비스를 위한 사용자 기반 개인 정보 보호 강화를 제안하였다[12]. 이 연구는 클라우드 서비스 자체 내에 개인 정보 보호를 통합하는 데 중점을 두며, 다양한 액세스 수준의 사용자는 요구 사항을 이해하고 투명한 생태계를 조성하기 위한 상호 작용을 제공받는다.

V. Hassija et al. 은 블록체인을 사용한 IoT에 암호화 해시 키를 사용하여 데이터 보안 기법을 제안하였다[13]. 이 기법은 IoT 장치에서 나오는 데이터는 블록체인에 안전하게 저장하여 스푸핑 공격과 데이터 손실을 방지하고 있다. 또한, 공개 키와 개인 키가 모두 사용되는 비대칭 암호화를 사용하여 무단 액세스를 방지할 수 있다.

A. Rahman et al. 은 클라우드가 데이터 보호, 기밀성, 데이터 무결성과 같은 보안 문제를 포함하지만, 블록체인이 추가된 소프트웨어 정의 네트워킹(SDN)을 사용하여 이러한 문제를 해결하였다[14].

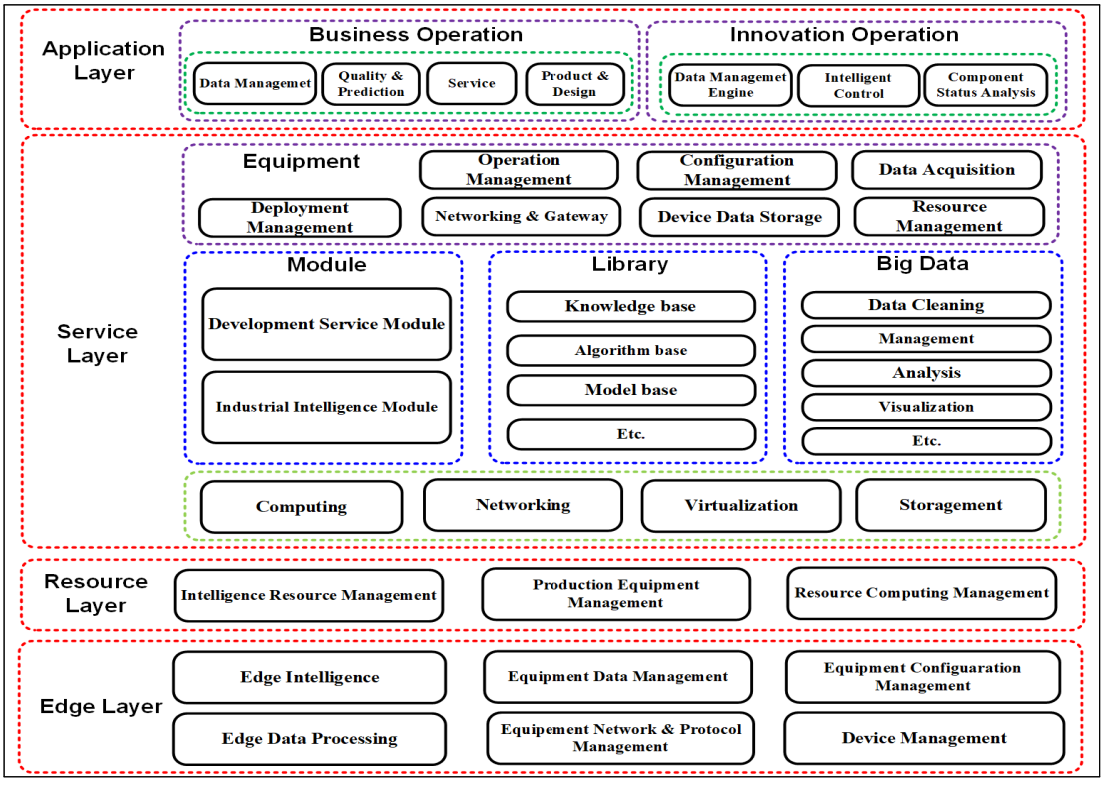
3. 안전성을 강화한 IoT 엣지 아키텍처 설계

3.1 개요

지난 몇 년 동안 5G와 같은 새로운 저 지연 통신 프로토콜을 기반으로 IoT 엣지가 등장했다. 그러나, IoT 엣지는 막대한 이점에도 불구하고, 새로운 보완 위협을 초래하여 이를 해결하기 위한 새로운 보안 솔루션이 필요한 상황이다. 제안 모델은 IoT 엣지 환경 중 로컬 노드에 데이터 처리 및 관리의 일부 기능을 할당함으로써 액세스 네트워크(엣지)에서의 부하를 더욱 줄이는 동시에 취약 부분을 안전하게 보안한다. 제안 모델은 다양한 IoT 기능을 네임 서비스로 가상화하고, 필요에 따라 하드웨어 기능과 충분한 계산 리소스를 갖춘 로컬 노드가 수행한다.

그림 1의 제안 모델은 엣지 컴퓨팅 및 5G 지원이 가능하며, 컴퓨팅 및 데이터 저장 프로세스를 수행하기 위해 데이터 처리의 구성 요소를 데이터 생성 소스에 가깝게 사용하는 분산 컴퓨팅 아키텍처를 기반으로 한다. 그림 1에서 IoT 엣지 환경은 주로 리소스가 제한되어 있어 IoT 엣지 중 일부 고성능 노드/장치 또는 게이트웨이를 통해 해당 엣지 노드(IoT-Edge 네트워크)와 결합한다. 또한, 그림 1은 일부 데이터 전처리, 분석 및 의사 결정을 로컬에서 수행하기 때문에 로컬 지연-중요 작업/단계에 대한 낮은 지연 시간 요건이 요구된다.

제안 모델은 그림 1과 같이 서로 다른 IoT 엣지 간에 필요한 정보를 안전하고 신뢰할 수 있는 공유를 허용하는 블록체인 기술을 사용한다.



[Fig. 2] Components for IoT Edge System

3.2 엣지 컴퓨팅 프레임워크

제안 모델은 그림 2를 사용하여 로컬 노드에서 데이터 처리 및 관리의 일부를 안전하게 할당함으로써 액세스 네트워크(엣지)에서의 부하 및 보안을 더욱 보장한다. 제안 모델의 계층 구조는 그림 2와 같이 엣지 계층, 자원 계층, 서비스 계층, 응용 계층을 포함한 전통적인 IoT 시스템과 일치한다.

3.2.1 엣지 계층

엣지 계층은 IoT 장치로부터 데이터를 수집하고, 대기 시간 및 대역폭 소비를 줄이기 위해 IoT 데이터가 중앙 플랫폼으로 전송되기 전에 엣지 계층에서 전처리 되고 필터링한다. 이를 통해 여러 데이터를 데이터베이스가 가공된 데이터와 가공되지 않은 데이터로 보관하고 추가적인 검토를 수행하다.

3.2.2 자원 계층

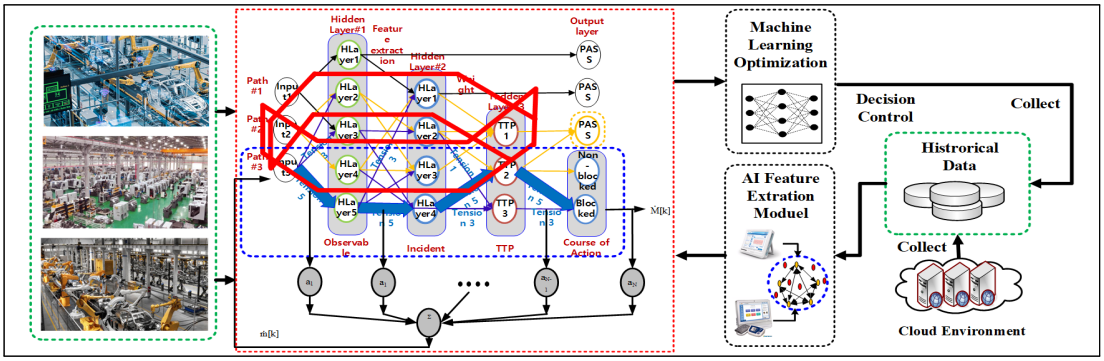
자원 계층은 계산 용량이 강하고 계산 자원이 충분하며 보다 복잡한 계산 작업을 처리할 수 있다. 계산 작업 전송에서 계산 효율을 향상시키고 에너지 소비를 줄이기 위해 시스템은 컨트롤러의 계산 능력에 따라 마스터 컨트롤러를 선택하고, 마스터 컨트롤러를 통해 IoT 장치가 선택한 계산 작업을 처리한 다음 작업 데이터를 블록체인에 패키징하여 업로드하게 된다.

3.2.3 서비스 계층

서비스 계층 빅데이터, 인공지능 등의 기술을 활용하여 방대한 감각 데이터를 융합, 분석, 저장함으로써 정보 파편화 문제를 해결한다. 데이터의 일관된 관리와 업데이트를 통해 정보 공격을 피하고, 상위 계층의 애플리케이션에 통일된 공유 데이터를 제공함으로써 단말의 일관된 관리를 실현하고, 허브, 플랫폼, 공유 데이터 관리의 기반을 마련한다.

3.2.4 애플리케이션 계층

애플리케이션 계층은 그리드 데이터 정보를 위한 비즈니스 응용 플랫폼이다. 응용 계층은 IoT 클라우드 플랫폼에 접속할 수 있도록 하여 최종 사용자에게 그리드 운영 비즈니스 사용자 에너지 소비 비즈니스를 위한 지능화를 제공하고 통합 에너지 시스템 운영 비즈니스 포저



[Fig. 3] AI based IoT Edge processing

응용 서비스를 제공하여 전체 네트워크 시스템, 사용자 및 기타 에너지 시스템의 인식과 상호 작용을 한다.

4. AI 블록체인 기반 분산 처리

그림 3은 AI 블록체인 기반의 블록체인 처리 과정을 나타내고 있다. 그림 3에 사용된 AI 블록체인은 AI를 적용한 블록체인 대상 시스템을 의미한다.. 그림 3에서 제안 모델은 여러 가상 머신(VM)을 활용하고 머신러닝(Machine Learning) 모델을 호스팅하기 위해 확장 가능한 컴퓨팅 리소스를 지원한다. 제안 모델은 IoT 장치에서 생성된 로컬 업데이트 세트(즉, 로컬 ML 모델의 그라디언트)를 얻고 업데이트에 대한 사전 처리 및 계산 작업을 수행한다. 오브젝트 검출, 예측과 같은 다양한 빅데이터 분석 작업을 수행하기 위해서 IoT 장치는 ML 모델을 얻기 위해 인터넷을 통해 ML 모델과 필요한 자원(즉, 블록체인 및 ML 작업 실행) 요청을 전송한다.

서버는 자원이 풍부한 컴퓨팅 기능을 갖추고 있으며, 정확한 ML 모델(즉, 글로벌 업데이트)을 준비하는 서비스에서 자원과 컴퓨팅 기능을 제공한다. 또한, 정확한 ML 모델을 제공하는 것에 대한 응답으로 블록체인의 정보를 얻는다.

블록체인 네트워크는 서버 간에 분산되고 안전한 방식으로 트랜잭션(즉, 로컬 및 글로벌 업데이트)을 기록하고 전송할 수 있는 분산 원장을 제공한다. 제안 모델은 블록체인을 통해 IoT 엣지 정보를 제어하고 퍼블릭 블록체인과 달리 순수한 피어투피어 제어를 피함으로써 더 높은 처리량(즉, IoT의 ML 작업에 상당히 필요함)으로 낮은 지연 시간을 제공하는 프라이빗 블록체인이 사용된다.

5. 성능평가

5.1 환경설정

표 1은 제안 모델의 IoT 엣지 환경을 구성하는 요소(클라우드 네트워크, 에지 네트워크, IoT 디바이스)의 성능평가에 필요한 매개 변수를 모델별로 분류하여 IoT 엣지 아키텍처를 최적화할 수 있도록 IoT 엣지 간에 필요한 정보를 평가하기 위한 매개변수 설정값을 정의하였다. 제안 모델은 각 IoT 엣지 구성이 애플리케이션별로 다르며 특정 IoT 애플리케이션의 요구 사항에 따라 달라진다. IoT 엣지 장치 간 지연 시간 매개 변수는 추적 경로(trace route)를 사용하여 시뮬레이션을 위해 설정되었으며, 토폴로지의 루트, 즉 로컬에서 클라우드로 이동함에 따라 장치의 전력 소비는 점차 증가한다. 또한, IoT 엣지 관련 사례에 정의된 요구 사항을 고려하여 다양한 매개 변수가 설정하였다.

〈Table 1〉 Simulation parameters

Parameters	Upstream bandwidth (MBps)	Downstream bandwidth (MBps)	Storage capabilities / RAM (GB)	Processing capabilities / CPU (MIPS)	Communication latency (ms)	Blockchain Instructions (M)	Blockchain Processing Power(Idle-Max)(W)
Cloud Networks	60	36	16	15000-20000	20	12	20-40
Edge Networks	30	18	8	4000-10000	10	6	10-20
IoT Devices	15	9	4	500-2000	2	-	-

〈Table 2〉 Model Hyperparameters

Model	Hyperparameters	Model	Hyperparameters
RF	num-trees =10 num_attr_each_split = sqrt(70)	KNN	num_neighbors = 5, metric = Euclidean, weight = Uniform
SVM	C = 1.0, kernel = RBF, g = auto, num_tolerance = 0.001, iter_limit = 100		
ANN	neurons_per_hidden_layer = 100, activation = ReLU, solver = Adam, regularization = 0.0001, max_iter = 400, replicable_training = true		
DT	induce_binary_tree = true, min_num_instances_in_leaves = 2, smallest_subset_split = 5, max_tree_depth = 100, stop_when_maj_reaches (%) = 95		

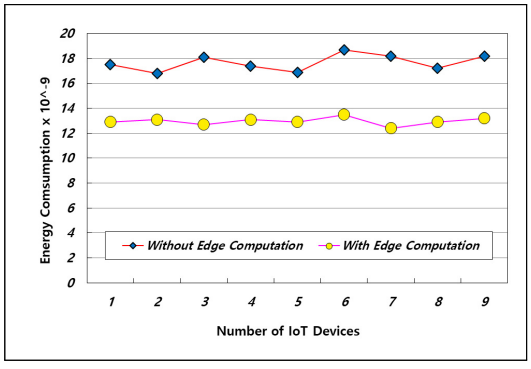
표 2은 제안 모델의 성능평가에 필요한 매개 변수를 모델별로 분류하여 IoT 엣지 아키텍처를 최적화할 수 있도록 IoT 엣지 간에 필요한 정보를 평가하기 위한 매개변수 설정값을 정의하였다.

제안 모델의 AI 기반 엣지 프로세싱의 성능을 분석하기 위해서 사이버 보안 데이터셋을 실험에 사용하였으며, 데이터셋은 일반 및 공격 IoT 네트워크 트래픽 데이터를 모두 포함하고 있다. 또한, 표 2는 모델별 하이퍼파라미터의 설정값을 Google Colab 지원 개발 언어 및 라이브러리를 사용한다.

5.2 성능 평가

5.2.1 총 에너지 소비

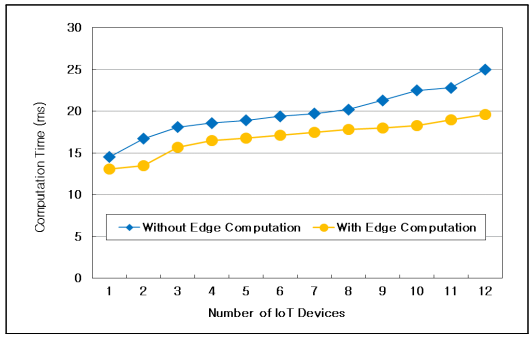
그림 4는 제안 모델과 엣지 컴퓨팅 프레임워크가 없는 전통적인 IoT 네트워크의 에너지 소비를 비교한 것이다. 제안 모델은 엣지 컴퓨팅 프레임워크가 없는 전통적인 IoT 네트워크보다 에너지 소비가 평균 34% 낮은 것으로 평가되었다. 적은 것을 관찰할 수 있다. 또한, 제안 모델에서 노드 수가 증가함에 따라 에너지 소비가 안정적임을 알 수 있다.



[Fig. 4] Total Energy Consumption

5.2.2 계산 시간

그림 5는 제안 모델을 엣지 IoT 프레임워크 유·무에 따라 네트워크의 계산 시간을 비교하였다. 제안 모델의 IoT 엣지 프레임워크는 안전한 데이터 전송을 수행하는데 더 적은 시간을 사용하고 노드 수가 증가함에 따라 계산 시간이 선형적으로 증가하였다. 그러나 IoT 엣지 프레임워크가 없는 네트워크에서는 계산 시간에 급격한 변화가 있었다.



[Fig. 5] Total Energy Consumption

5.2.3 AI 모델별 성능평가

제안 모델에서는 SVM이 이상치(outlier)에 대해 민감하지 않은 특성이 있어, 데이터의 이상치가 많이 포함된 경우에도 좋은 성능을 발휘할 수 있어 다른 모델에 비해 정확도가 99.7%로 가장 정확도가 높게 나타났다.

이러한 특성은 SVM이 다양한 분야에서 활용될 수 있도록 만들어주는 중요한 장점 중 하나이다. SVM은 고차원 데이터셋에서도 잘 작동한다. 표 3에서 RF(98.7%)보다 ANN 모델이 더 높은 정확도(99.2%)를 나타내지만, 훈련 및 예측 시간은 RF가 더 높게 나타났다. 그러나, RF는 ANN보다 상대적으로 낮은 재현율(93%)을 가지고 있다. 그 이유는 이 모델이 False Negative 예측이 상대적으로 높기 때문인데, 이는 공격을 양성으로 잘못 탐지하였기 때문이다.

RF는 KNN보다 낮은 정확도를 나타내지만, RF는 예측 시간이 낮게 나타났다. SVM 모델은 RF 및 KNN 모델보다 더 높은 정확도(99.7%)를 나타내지만, 훈련 시간

〈Table 3〉 Model Performance

Model	Accuracy	Precision	Recall	F1 score	Training time(sec)	Prediction time(sec)
RF	0.987	0.97	0.93	0.97	150.86	6.67
KNN	0.991	0.96	0.97	0.96	7.23	1151.89
SVM	0.997	0.97	0.98	0.98	4.89	1.41
ANN	0.992	0.97	0.97	0.97	200.04	2.54
DT	0.989	0.96	0.95	0.96	5.15	0.09

(4.89초)과 예측 시간(1.41초)이 훨씬 적게 나타났다. SVM 모델에서는 작은 데이터 셋에 적합한 커널 함수를 사용하기 때문에 RF보다 훈련 시간이 훨씬 짧아 제안 모델의 IoT 시스템에 적합하다. 그러나 하나의 모델을 가장 적합한 모델로 선택하는 것은 제안 모델이 IoT 장치에서 사용하거나 IoT 엣지에서 사용되는지에 따라 다르다.

5.3 보안 평가

블록체인 기반 IoT 엣지 환경에서 발생할 수 있는 보안 공격 중 제안 모델이 안정성을 보안할 수 있는 보안 공격 대응 방안은 다음과 같다. 첫째, 제안 모델은 AI를 활용하여 IoT 에지 장치에서 추출된 네트워크 트래픽 데이터를 분석하고 네트워크 토폴러지를 동적으로 조정하여 악성 하드웨어 삽입 또는 민감한 정보 추출과 같은 공격자의 물리적 변조 위험을 줄여준다. 둘째, 제안 모델은 IoT 에지 장치에 권한 및 액세스 데이터를 쿼리하여 민감한 블록체인 정보를 추출함으로써 정보 침해 및 데이터 도난에 대한 안전성을 향상시킨다. 셋째, 제안 모델은 블록체인 검증 결과를 권한 및 액세스 수준과 일치시켜 우선순위 기반의 블록체인 액세스 제어를 사용하여 IoT 에지 장치에 대한 무단 액세스로 인한 서비스 거부 공격을 효과적으로 방지한다. 넷째, 제안 모델은 블록체인 헤더 및 본문의 ID 및 타임스탬프 정보를 검증 프로세스에 통합하여 스푸핑 공격에 대한 복원력을 향상시키고 있다. 다섯째, IoT 에지 장치에는 취약성이나 결함이 있을 수 있지만, 제안 모델은 IoT 리소스 손상을 예방하기 위해서 블록체인에 대한 무단 액세스를 요구하여 보안 및 기능과 관련된 위험을 줄여주고 있다.

6. 결론

IoT 엣지 환경은 다양한 IoT 장치들이 활용되면서 다양한 연구가 진행되고 있다. 그러나, IoT 엣지는 보안과 관련된 문제들이 나타나면서 이에 대한 보안 보장이 요구되고 있다.

본 논문에서는 IoT 시스템의 보안 위협을 방지할 수 있는 IoT 엣지 아키텍처 모델을 제안하였다. 제안 모델은 로컬 노드에서 데이터 처리 및 관리의 일부를 할당함으로써 액세스 네트워크(엣지) 부하 및 보안을 보장한다. 제안 모델은 시스템 내 IoT 기기의 수가 ECD보다 많다는 점을 고려하여 IoT 기기가 ECD에 컴퓨팅 자원을 요청하는 과정으로 단순화하였다. 제안 모델은 IoT 애지 장치에서 추출한 네트워크 트래픽 데이터를 사용하여 안전성을 평가하였다. 평가 결과, 제안 모델은 SVM 모델이 가장 적합한 것으로 나타났다. 그러나, 하나의 모델을 가장 적합한 모델로 선택하는 것은 환경에 따라 달라지기 때문에 SVM이 IoT 엣지 환경에 모두 적합하지는 못하다. 향후 연구에서는 본 연구에서 얻은 결과를 바탕으로 다양한 클라우드 환경에 적용하여 제안 모델의 성능을 평가할 예정이다.

REFERENCES

[1] I.Yen, F.Bastani, N.Solanki, Y.Huang and S.Hwang, "Trustworthy Computing in the Dynamic IoT Cloud," 2018 IEEE International Conference on information Reuse and Integration (IRI), pp.411-418, 2018.

[2] S.M.Ali, A.S.Elameer and M.M.Jaber, "IoT network security using autoencoder deep neural network and channel access algorithm," Journal of Intelligent Systems, Vol.31, No.1, pp.95-103, 2022.

[3] M.A.Ferrag, O.Friha, D.Hamouda, L.Maglaras and H.Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," IEEE Access, Vol.10, pp.40281-40306, 2022.

[4] S.Sachdeva and A.Ali, "Machine learning with digital forensics for attack classification in cloud network environment," International Journal of System Assurance Engineering and Management, Vol.13, No.1, pp.156-165, 2022.

[5] K.Sha, R.Errabelly, W.Wei, T.A.Yang and Z.Wang, "EdgeSec: Design of an Edge Layer Security Service to Enhance IoT Security," 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC),

pp.81-88, 2017.

[6] R.Sachdev, "Towards Security and Privacy for Edge AI in IoT/IoE based Digital Marketing Environments," 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), pp.341-346, 2020.

[7] P.M.Shakeel, S.Baskar, H.Fouad, G.Manogaran, V.Saravanan, and C.E.Montenegro-Marin, "Internet of things forensic data analyтsis using machine learning to identify roots of data scavenging," Fuтture Generation Computer Systems, Vol.115, pp.756-768, 2021.

[8] J.Wang, S.Wang, L.Wang, W.Shao, S.Xu and S.Zhang, "A Blockchain and Edge Computing Based Public Audit Scheme for Cloud Storage," 2022 41st Chinese Control Conference (CCC), pp.7466-7470, 2022.

[9] L.Liu and K.Omote, "Efficient Authentication System Based On Blockchain Using eID card," 2023 IEEE International Conference on Blockchain (Blockchain), pp.166-171, 2023.

[10] Y.C.Chang, Y.S.Lin, A.K.Sangaiahc and H.T.Wu, "A Private Blockchain System based on Zero Trust Architecture," 2024 26th International Conference on Advanced Communications Technology (ICACT), pp.143-146, 2024.

[11] N.Almolhis, A.M.Alashjaee, S.Duraibi, F.Alqahtani and A.N.Moussa, "The Security Issues in IoT - Cloud: A Review," 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA), pp.191-196, 2020.

[12] I.Mohiuddin and A.Almogren, "Security Challenges and Strategies for the IoT in Cloud Computing," 2020 11th International Conference on Information and Communication Systems (ICICS), pp.367-372, 2020.

[13] V.Hassija, V.Chamola, V.Saxena, D.Jain, P.Goyal and B.Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," IEEE Access, Vol.7, pp.82721-82743, 2019.

[14] A.Rahman, M.J.Islam, M.S.I. Khan, S.Kabir, A.I.Pritom and M.R.Karim, "Block-SDoTCloud: Enhancing Security of Cloud Storage through Blockchain-based SDN in IoT Network," 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), pp.1-6, 2020.

정 윤 수(Yoon-Su Jeong) [정회원]

- 1998년 2월 : 청주대학교 전자계산학과(공학사)
- 2000년 2월 : 충북대학교 전자계산학과(이학석사)
- 2008년 2월 : 충북대학교 전자계산학과(이학박사)
- 2012년 2월 ~ 현재 : 목원대학교 게임소프트웨어공학과 교수

〈관심분야〉

IoT/IIoT, 네트워크, 정보보안, 빅데이터, 암호학, 스마트팜, 헬스케어