Smart Media Journal / Vol.14, No.12 / ISSN:2287-1322
https://dx.doi.org/10.30693/SMJ.2025.14.12.164

# OneM2M 기반 엣지 AI 시스템을 위한 보안 연결성 프레임워크

## (A Security Connectivity Framework for OneM2M-Based Edge AI Systems)

박기철*, 권용진**, 안재훈*, 김영환*

(Kicheol Park, Yongjin Kwon, Jaehoon An, Younghwan Kim)

**요 약**

사물인터넷(IoT) 기술의 확산으로 개인 환경에 설치되는 엣지 디바이스 수가 증가하고, 이들로부터 생성되는 실시간 데이터는 지능형 서비스를 위한 핵심 자원으로 활용된다. 특히 엣지 AI 시스템에서는 민감한 개인정보 기반의 데이터가 연산에 포함되는 경우가 많아, 보안 위협에 대한 대응이 필수적이다. ARM TrustZone과 같은 하드웨어 기반 신뢰 실행 환경(TEE)을 적용한 기존 보안 연구는 데이터 보호에 유효하지만, 모든 데이터에 일괄 적용할 경우 성능 저하와 시스템 병목 현상이 발생할 수 있다.

본 논문에서는 OneM2M 기반 엣지 AI 시스템에서 데이터의 민감도를 기반으로 하드웨어 보안 기능을 선택적으로 적용하는 보안 연결성 프레임워크를 제안한다. 제안 기법은 IoT 데이터의 흐름을 실시간 분석하여 보호가 필요한 민감 데이터를 선별하고, 해당 데이터에만 TrustZone 기반 암호화 및 무결성 검증을 수행한다. 이를 통해 성능 저하를 최소화하면서도 데이터 보안성을 유지할 수 있다. 실제 엣지 게이트웨이 환경에서 제안 프레임워크를 구현하고 성능 평가를 수행한 결과, 보안 적용의 실효성과 함께 처리 지연 완화 효과를 확인하였다.

■ 중심어 : 엣지 AI ; OneM2M ; 신뢰 실행 환경 ; 보안 연결 프레임워크

**Abstract**

With the proliferation of IoT technologies and the deployment of edge AI systems, sensitive data are being collected and processed in real time. However, such data are exposed to security threats during transmission and storage, and applying security functions in resource-constrained gateways often leads to performance degradation. Previous studies have utilized hardware security features but have not sufficiently considered performance limitations. This paper proposes a security connectivity framework to ensure data confidentiality and integrity in OneM2M-based edge AI systems. The proposed approach analyzes data flows to classify protected and general data, and integrates a Trusted Execution Environment (TEE) to perform encryption and integrity verification, thereby achieving both security and efficiency. An implemented platform is used to measure the performance degradation caused by hardware security functions and to evaluate the performance improvements achieved with the proposed method.

■ keywords : Edge AI ; OneM2M ; Trusted Execution Environment ; Security Connectivity Framework

## Ⅰ. 서 론

엣지 컴퓨팅은 다수의 IoT 디바이스에서 발생하는 방대한 데이터를 현장에서 실시간으로 처리함으로써, 통신 지연을 줄이고 분산된 지능형 서비스를 가능하게 하는 핵심 기술로 자리 잡고 있다[2,9,11]. 특히 엣지 환경에서는 추론뿐 아니라 지속적인 학습 요구가 함께 대두되면서, 엣지 디바이스와 서버 간 연산 협력 구조가 필수화되고 있다[2,9]. 이러한 구조에서 데이터를 수집·전

* 정회원, 한국전자기술연구원 지능형 IDC 사업단
** 준회원, 한국전자기술연구원 지능형 IDC 사업단
이 논문은 2025년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구 결과임 (No. RS-2025-25441574, (2세부)엣지AI 학습 및 지능의 동시 제공이 가능한 시스템 SW 기술 개발)
접수일자 : 2025년 09월 29일
수정일자 : 2025년 10월 27일
게재확정일 : 2025년 11월 04일
교신저자 : 안재훈 e-mail : corehun@keti.re.kr

송·처리하는 과정 전반에 걸쳐 보안성과 연결성을 동시에 확보하는 것이 중요한 과제로 부상하고 있다[3,5,6].

엣지 AI 시스템은 개인의 위치, 행동 패턴, 생체 정보 등 민감한 데이터를 실시간으로 수집하고 처리하는 특성상, 기밀성 및 무결성 보장을 위한 보안 대책이 필수적이다. 기존 연구들은 ARM TrustZone과 같은 하드웨어 기반 신뢰 실행 환경(Trusted Execution Environment, TEE)을 활용하여 보안을 강화하는 방법을 제시해왔다. TEE는 물리적으로 분리된 실행 환경을 제공함으로써, 민감 정보와 보안 연산을 격리하여 보호하는 데 효과적이다.

하지만 엣지 디바이스는 연산 성능, 전력, 메모리 등 자원이 제한적인 특성을 가지며, 모든 데이터를 TEE에서 처리할 경우 연산 병목과 지연이 심화되는 문제가 발생한다. 특히 다수의 디바이스가 동시 연결되는 환경에서는, 일률적인 보안 처리로 인해 시스템 전체의 처리율이 급격히 저하될 수 있으며, 이는 지능형 서비스의 실시간성을 저해하는 주요 요인이 된다[5].

이러한 한계를 극복하기 위한 방안으로, 데이터의 보안 요구 수준을 정량화하고, 민감도에 따라 보안 처리 수준을 차등 적용하는 방식이 주목받고 있다[6]. 즉, 기밀성과 무결성이 요구되는 데이터에만 하드웨어 보안 기능을 선택적으로 적용함으로써, 보안성과 성능 간 균형을 확보할 수 있다. 이를 위해서는 데이터 흐름 상에서 각 데이터의 특성과 민감도를 평가하고, 처리 경로를 분기하여 효율적인 보안 정책을 적용할 수 있는 구조적 기반이 필요하다.

본 논문에서는 oneM2M 플랫폼 구조에 기반하여, 데이터 민감도 기반 보안 분류와 TrustZone 연계를 통해 실시간 보안 연결성을 확보하는 엣지 AI 시스템용 보안 연결성 프레임워크를 제안한다. 제안된 프레임워크는 IoT 데이터의 흐름을 실시간으로 분석하여 보호 대상과 일반 데이터를 구분하고, 신뢰 실행 환경을 선택적으로 연계함으로써 성능 저하 없이 보안 수준을 유지할 수 있도록 설계되었다. 또한, oneM2M 서비스 계층과의 통합을 통해, 엣지 디바이스에서 서버까지 이어지는 전송 경로 상의 일관된 보안 정책 적용을 가능하게 하여 보안성과 처리 성능 간의 균형 효과를 실증하였다.

## Ⅱ. 관련 연구

### 1. IoT 아키텍처 표준 및 플랫폼

사물인터넷(IoT)은 다양한 산업 분야에서 새로운 서비스를 창출하고 있으나, 보안성과 복원력 측면에서 여전히 도전 과제가 존재한다[1]. 이러한 문제를 해결하기 위하여 국제 표준화 기구들은 IoT 참조 아키텍처와 플랫폼 표준을 제시하였다. ISO/IEC는 IoT 시스템을 위한 표준 참조 아키텍처를 정의하여 공통 프레임워크와 용어 체계를 제공하며, IoT의 상호운용성과 보안 위험 완화를 목표로 하고 있다.

또한 글로벌 표준화 기구인 oneM2M은 상호운용성을 보장하기 위한 공통 IoT 서비스 계층을 개발하였다. 이를 기반으로 Mobius 및 &Cube와 같은 오픈소스 IoT 플랫폼을 구현하여 서버와 디바이스 측 서비스에 적용한 바 있다[7,9]. 한편 IoT 데이터 처리를 분산시켜 지연을 줄이기 위한 엣지 컴퓨팅(MEC) 기술도 활발히 연구되고 있으며, 이는 통신망 엣지에 클라우드 기능을 확장함으로써 실시간 서비스 제공을 가능하게 하고 있다[2, 9, 11]. 이와 같이 표준 아키텍처와 플랫폼 기술은 대규모 IoT 환경에서 상호운용성과 보안성을 확보하기 위한 기반을 제공한다.

### 2. IoT 디바이스 보안 기술

IoT 시스템에서 생성되는 데이터는 민감도에 따라 보호 수준을 달리 적용해야 할 필요성이 커지고 있다. AWS 같은 클라우드 모범 사례에서

는 IoT 장치에서 수집되는 데이터의 민감도를 식별·분류한 후 이를 기반으로 암호화 등 보안 통제를 적용할 것을 권고한다. 특히 AWS IoT 아키텍처 지침은 수집되는 모든 데이터를 민감도 수준에 따라 식별·분류하고, 민감도가 높은 데이터는 추가적인 암호화 또는 액세스 제어를 적용할 것을 명시함으로써 IoT 데이터 분류의 중요성을 강조하고 있다. 이처럼 데이터 분류는 클라우드 차원뿐만 아니라 리소스가 제한적인 IoT 엣지 환경에서도 필수로 고려되는 요소이다. 따라서 대규모 IoT 환경에서는 수많은 디바이스들이 민감 데이터를 생성·처리하므로, 디바이스 단의 보안 격리 기술이 중요하다. 이를위해 기존 연구로 스마트 단말 내에 가상화 기반의 도메인 분리 보안 플랫폼을 구현하여 일 영역과 보안 영역을 분리함으로써 단말 보안을 강화하였다[5, 7]. 또한 리소스가 제한된 게이트웨이 환경에서 ARM TrustZone의 성능 저하를 최소화하기 위해, 사용자 데이터 중 실제로 민감도가 높은 데이터만 신뢰 영역(secure world)에 저장하도록 플랫폼을 설계했다. 센서/사용자 정보 중 개인정보로 간주될 수 있는 데이터만을 분류하여 TEE에 보관·암호화 처리함으로써, 전체 시스템의 오버헤드를 줄이고자 하였다.

### 3. 데이터 민감도 분류 및 보안 기법

모든 IoT 데이터를 일괄 보호하면 성능 저하 및 비용이 크기 때문에, 중요한 민감 데이터만 선별하여 강력한 보안 조치를 적용하는 연구가 활발하다. 먼저, 일반적인 원칙으로 모든 데이터에 동일한 보안 수준을 적용하는 것은 비용 대비 효율적이지 않으며, 데이터의 민감도에 따라 보안 수준을 달리 설정해야 하고 IoT 데이터의 특성에 따라 보안 레벨을 차등 적용하는 아키텍처를 제안하며, 데이터 민감도 기반의 계층적 보안을 강조하였다[4]. 따라서 게이트웨이에서 수집된 데이터를 “사용자 민감 데이터”와 “일반 데이터”로 분류하고, 민감 데이터에만 TrustZone 기반 암호화를 적용하는 플랫폼에 대한 연구가 진행되었다[6]. 분류 과정에서 연결된 기기의 속성과 수집된 데이터 속성을 평가하여, 데이터 기밀성·무결성·신뢰성 각각에 가중치를 부여함으로써 총체적 민감도를 산정한다.

## Ⅲ. 시스템 구조 및 구현 개요

본 논문에서는 엣지 게이트웨이의 신뢰 실행 환경(TEE)을 활용하여 IoT 데이터의 중요도에 따라 선택적 보안 처리를 수행하는 플랫폼을 구현하였다. 시스템은 라즈베리파이5 위에 Rich OS와 신뢰할 수 있는 보안 OS(OP-TEE)로 구성된 TrustZone 환경을 갖추고 있다. 게이트웨이는 표준 IoT 플랫폼인 oneM2M과 연동되도록 Mobius 서버와 HTTP REST API로 통신하며, 이를 통해 수집 데이터를 클라우드에 연계한다. 그림1 은 일반 영역(노멀 월드)과 보안 영역(보호된 Secure 월드)으로 나뉘며, 데이터의 민감도를 평가해 필요한 경우에만 보안 영역의 기능을 사용하도록 설계되었음을 보여준다. 이러한 설계를 통해 모든 데이터를 무조건 TEE에서 처리할 때 발생하는 과도한 오버헤드를 피하면서도, 보호 우선도 높은 정보만 엄선하여 안전하게 처리할 수 있다. 자원이 제한된 IoT 게이트웨이에서 연결 기기와 데이터가 증가할 때 성능 저하 문제를 완화하고 구조적 확장성을 확보하기 위한 핵심 아이디어이다.

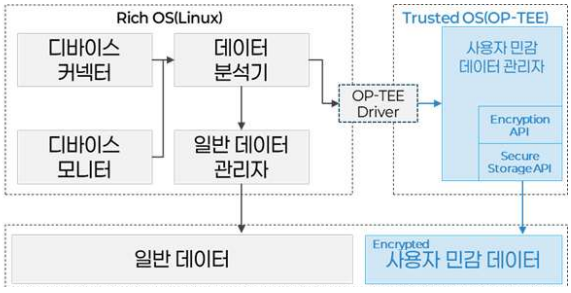



그림 1. TrustZone 기반 민감 데이터 분류 플랫폼

### 1. 시스템 구성 요소와 역할

게이트웨이 플랫폼의 주요 구성 모듈은 일반 실행 환경(Rich OS 상의 애플리케이션 모드)과 안전 실행 환경(Secure OS 상의 TEE 모드)에 분산되어 있다. 각 모듈의 역할은 다음과 같다.

디바이스 커넥터(Device Connector): 게이트웨이에 연결되는 IoT 센서/디바이스들과의 통신 연결을 관리한다. 새로운 IoT 기기가 등록되면 해당 디바이스의 ID, 타입 등의 정보를 초기 수집하고 게이트웨이에 등록 절차를 진행한다. 디바이스별 데이터 송수신 채널을 열어주고 유지하는 역할을 한다.

디바이스 모니터(Device Monitor): 연결된 IoT 기기의 상태를 지속적으로 모니터링하고 메타데이터를 관리한다. 예를 들어 기기의 동작 여부, 오류 발생, 데이터 전달 주기 등을 추적하여, 장기간의 동작 신뢰도나 데이터 전달 무결성 지표를 평가한다. 이 모듈은 수집 경로 상의 보안 수준(예: 디바이스의 자체 암호화 지원 여부, 통신 프로토콜의 안전성)을 파악하여 데이터 무결성 점수 계산에 활용된다. 또한 각 기기의 가동 시간 및 고장 기록을 수집하여 신뢰성 평가에도 기여한다.

데이터 분석기(Data Analyzer): 게이트웨이의 핵심 모듈로, 수집된 원시 데이터를 입력받아 데이터의 중요도(민감도)를 판정한다. 디바이스 커넥터/모니터로부터 전달된 기기 정보와 데이터 속성을 바탕으로 세 가지 평가 기준을 계산한다:

데이터 기밀성 - 해당 데이터가 개인 프라이버시나 민감 정보를 포함하는 정도를 평가한다. 이는 데이터 내용이 사용자에게 미치는 영향(예: 위치정보, 건강정보, 금융정보 등 노출 시 피해 심각도)에 따라 산정된다.

데이터 무결성 - 데이터가 전송 경로에서 위변조 없이 신뢰성 있게 전달되었는지를 평가한다. 디바이스 및 게이트웨이 간 통신에 보안 프로토콜 적용 여부, 경로 중간 기기들의 하드웨어 보안 기능 활용 여부 등을 고려하여 산출한다.

데이터 신뢰성 - 데이터를 생성하는 디바이스의 신뢰도를 평가한다. 기기의 평균 무고장시간(MTTF)이나 과거 오류 빈도 등을 기반으로 산출된 장치 신뢰성 지표를 사용하며, 시간이 지남에 따라 기기의 신뢰도가 저하되는 특성을 반영한다.

이러한 세 가지 값에 가중치를 적용하여 최종 데이터 중요도 점수를 계산한다. 가중치는 서비스 환경에 따라 조정 가능하며, 예를 들어 개인정보 위주의 서비스에서는 기밀성 가중치를 높게 두는 방식으로 유연하게 민감도 기준을 설정할 수 있다. 데이터 분석기는 설정된 임계치를 넘는 중요도 점수를 갖는 데이터를 “우선 보호 대상 데이터”로 분류하고, 이하인 경우 일반 데이터로 취급한다.

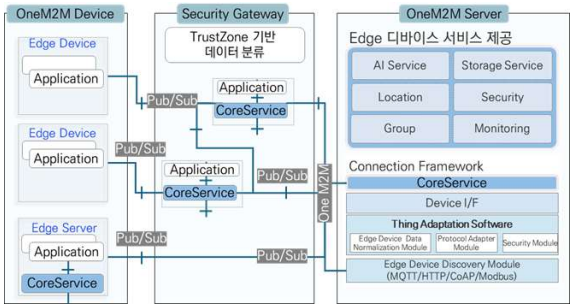



그림 2. oneM2M Mobius 기반 데이터 흐름도

일반 데이터 관리자(Normal Data Manager): 민감도로 분류되지 않은 일반 데이터를 일반 실행 공간에서 저장 및 관리한다. 이 모듈은 수집된 데이터를 로컬 게이트웨이의 데이터베이스나 파일 시스템에서 저장한다. 그림 2는 필요 시 원격 oneM2M Mobius 플랫폼으로 연계 전송되는 과정을 보여준다. 일반 데이터는 게이트웨이에서 실시간 처리하거나 요약 정보만 업로드 하는 등 성능 우선의 방식으로 다루어지며, 보안 부하를 최소화한다.

Sensitive Data Manager: 신뢰 실행 환경 내에서 동작하는 보안 모듈로서, 보호 우선도 높은 정보로 판정된 데이터를 안전하게 처리한다[2]. 데이터 분석기의 요청에 따라 TrustZone Secure World 상에서 호출되며, 전달된 데이터를 암호화하여 저장하거나 보안 처리를 적용한다. 민감 데이터 관리자는 OP-TEE 기반의 신뢰 애플리

케이션(TA) 형태로 구현되었고, 암호화 키와 같은 민감한 보안 자재를 TrustZone 내 Secure Storage API를 통해 안전하게 관리한다. 이를 통해 암호 키 등이 노출되지 않도록 하드웨어 보안 영역에서 격리하며, 데이터의 기밀성과 무결성을 보장한다.

보안 연결성을 위해 게이트웨이와 Mobius 간 통신에는 TLS 적용 등 암호화된 채널(HTTPS)을 사용하고, 민감 데이터의 경우 전송 전에 추가로 페이로드 암호화를 적용함으로써 이중 보호한다. 또한 Mobius 플랫폼의 접근제어 정책을 활용하여 민감 데이터 리소스에는 인증된 클라이언트만 접근하도록 설정하였다. 이러한 플랫폼 연동을 통해 제안 시스템은 표준 IoT 프레임워크와의 호환성을 갖추면서도 종단 간 보안을 강화한다.

## 2. 데이터 중요도 분류 알고리즘

다음은 데이터 중요도 평가 및 선택적 보안 처리 알고리즘으로 그림3의 표현된 슈도코드에서는 새로운 디바이스가 등록될 때의 초기 설정과 수집 데이터에 대한 중요도 평가 및 처리 분기를 보여준다.

**Require:** Device info $D$ (with fields: type, securitySupport, MTTF, etc.), New data $x$
**function** OnDeviceRegister($D$)
  Initialize $D.integrity \leftarrow$ EvaluateIntegrity($D.securitySupport$)
  Initialize $D.confidentiality \leftarrow$ EvaluateConfidentiality($D.type$)
  Initialize $D.reliability \leftarrow 1.0$ ▷ start with max reliability
  $D.startTime \leftarrow$ now() ▷ for reliability decay
**end function**
**function** OnDataReceived($x$ from device $D$)
  $t \leftarrow$ hoursSince($D.startTime$)
  $D.reliability \leftarrow e^{-\lambda \cdot t}$ ▷ update reliability (MTTF-based)
  $I \leftarrow D.integrity$
  $C \leftarrow D.confidentiality$
  $R \leftarrow D.reliability$
  $S \leftarrow w_i \cdot I + w_c \cdot C + w_r \cdot R$ ▷ calculate sensitivity score
  **if** $S \geq threshold$ **then**
    SecureStore.EncryptAndSave($x$) ▷ invoke TEE for sensitive data
    SendToCloud($x$, encrypted=True)
  **else**
    LocalDB.Save($x$) ▷ store in normal world
    SendToCloud($x$, encrypted=False)
  **end if**
**end function**

그림 3. 민감 데이터 분류 알고리즘

위 알고리즘에서, 새로운 디바이스가 게이트웨이에 등록되면 (OnDeviceRegister) 해당 디바이스의 초기 기밀성 점수와 무결성 지원 여부를 평가하여 기록하고, 신뢰성 평가를 위한 초기값을 설정한다. λ는 MTTF 기반의 고장률 파라미터이다. OnDataReceived 루틴에서는 수집된 새로운 데이터 x에 대해, 미리 기록된 해당 디바이스 D의 기밀성(C)·무결성(I) 값과 최신 신뢰성(R) 값을 불러와 민감도 점수 S를 계산한다. 계산된 S가 사전에 정한 임계값 이상인 경우 x를 중요 데이터로 간주하여, TrustZone의 Secure World 기능을 통해 EncryptAndSave()를 호출한다. 이 과정에서 TEE의 중요 데이터 관리자가 호출되어 데이터 x를 암호화 처리한 뒤 안전하게 저장하며, 필요하면 즉시 oneM2M 서버로 암호화된 채로 전송한다. 한편 S가 임계값 미만인 일반 데이터로 분류되면, x를 로컬 게이트웨이 저장소에 원문으로 저장하고 Mobius 서버로도 전송한다. 이와 같이 중요도에 따라 처리 경로를 분기함으로써 보안이 특히 요구되는 항목은 하드웨어 보안의 보호를 받고, 그렇지 않은 데이터는 게이트웨이가 효율적으로 처리하도록 한다.

## 3. TrustZone 기반 보안 처리 흐름

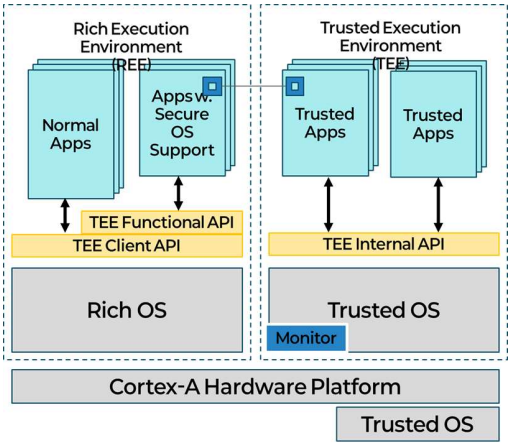



그림 4. TrustZone S/W 계층 구조

그림4는 TrustZone의 S/W 계층 구조를 보여준다. 이에 따라 본 논문에서 제안하는 플랫폼은 데이터 중요도 분류 결과에 따라 다음과 같은 보

안 처리 절차가 수행된다:

일반 데이터 처리 경로: 게이트웨이의 데이터 분석기가 새 데이터를 보안 요구 수준이 높지 않은 데이터로 판단하면, 해당 데이터를 일반 모드에서 처리한다. 일반 데이터 관리자는 디바이스 모니터로부터 전달받은 원시 데이터를 즉시 로컬에 저장하거나 필터링한다. 그런 다음 Mobius 서버의 해당 리소스 경로로 HTTP REST 요청을 보내어 데이터를 업로드한다. 이때 전송은 일반 네트워크 소켓에서 이뤄지지만, 전송 계층 보안(TLS)을 적용하여 데이터의 전송 중 기밀성을 확보한다. 일반 경로에서는 암호화나 TEE 호출로 인한 부하가 없기 때문에 지연 시간이 최소화되고, 게이트웨이가 다중 IoT 기기로부터 들어오는 대량 데이터도 실시간으로 처리할 수 있다.

## Ⅳ. 실 험

본 논문에서 제안한 보안 연결성 프레임워크의 효과를 검증하기 위하여 라즈베리파이 5 기반 IoT 게이트웨이를 대상으로 성능 평가 환경을 설계하였다. 실험 시나리오는 게이트웨이에 다수의 가상 IoT 장치가 연결되어 주기적으로 센서 데이터를 생성하고, 이를 게이트웨이가 처리한 후 oneM2M 서버에 전달하는 과정으로 설정하였다. 각 장치는 128바이트 크기의 데이터를 일정 주기로 전송한다고 가정하였으며, 동시 접속 장치 수(N)는 1, 5, 10으로 변화시켜 확장 시의 성능 변화를 관찰하였다. 데이터 크기는 고정하여, 처리 부하 변화가 발생하는 주요 요인은 동시 접속 수와 데이터 발생 빈도로 한정하였다.

성능 평가는 세 가지 처리 모드를 정의하여 비교하였다.

일반 처리 모드: 모든 데이터를 Rich OS에서 원문으로 처리 및 전송하는 방식으로, 보안 기능을 적용하지 않는다. 이 모드는 성능 비교의 기준점으로 사용된다.

전체 보안 모드: 유입되는 모든 데이터를 Trusted OS(OP-TEE)의 Secure World에서 암호화한 후 전송하는 방식이다. 가장 강력한 보안을 제공하지만, 암호화 연산과 컨텍스트 전환으로 인한 성능 오버헤드가 발생한다.

선택적 보안 모드(제안 기법): 데이터 분석기를 통해 중요도가 높은 정보만 Secure World에서 암호화하고, 중요도가 낮은 데이터는 일반 처리 경로를 따른다. 본 실험에서는 약 절반 정도의 데이터가 보안 처리 대상으로 분류되도록 임계값을 설정하였다.

측정 지표는 다음과 같다. 첫째, 평균 지연 시간(latency)은 데이터가 게이트웨이에 입력된 시점부터 Mobius 서버로 전송 완료되기까지 소요된 시간을 의미한다. 이 값에는 분류 알고리즘 실행, 보안 영역 전환 및 암호화, 네트워크 전송 시간이 모두 포함된다. 둘째, 처리량(throughput)은 단위 시간당 서버로 전달된 데이터 건수를 나타내며, 게이트웨이 처리 성능을 보여준다. 셋째, 자원 오버헤드는 보안 적용에 따른 CPU 사용률 및 메모리 점유율 증가를 의미한다.

모든 실험은 동일 조건에서 30회 이상 반복 수행하여 신뢰도를 확보하였으며, 결과는 평균값을 사용하였다. 게이트웨이와 Mobius 서버는 동일한 LAN 환경에 배치하여 네트워크 지연 요인을 최소화하였고, 서버 측은 충분한 사양의 별도 장비를 사용하여 병목 현상이 발생하지 않도록 하였다.

표 1은 동시 기기 수(N)의 변화에 따라 세 가지 처리 모드별 평균 지연 시간을 비교한 결과를 나타낸다. 일반 처리 모드의 경우 보안 연산이 적용되지 않으므로 기기 수가 증가하더라도 지연 시간이 거의 변하지 않았다. 예를 들어 N=1에서는 약 10 ms, N=10에서도 약 11 ms 수준으로 안정적인 결과를 보였다. 반면 전체 보안 모드는 모든 데이터에 암호화를 적용하기 때문에 기기 수가 늘어날수록 지연 시간이 크게 증가하였다. 1개 기기일 때 약 12 ms였으나, 10개 기기일 경우 약 20 ms에 달하여 기준 대비 두 배 가까운 지연이 발생하였다. 이는 다수의 IoT 기기가 동

시에 데이터를 전송할 경우, Secure World의 암호화 연산이 성능 병목으로 작용함을 의미한다.

표 1. 처리 기기에 따른 평균 지연 시간 비교 (단위: ms)

| 동시 IoT 기기 수 (N) | 일반 처리 | 전체 보안 | 제안 기법 |
|---|---|---|---|
| 1 | 10 | 12 (+20%) | 11 (+10%) |
| 5 | 10 | 15 (+50%) | 12 (+20%) |
| 10 | 11 | 20 (+82%) | 13 (+18%) |

제안한 선택적 보안 모드는 초기에는 전체 보안과 유사한 지연을 보였으나, 기기 수가 증가할수록 지연 증가 폭이 훨씬 완만하였다. 예를 들어 N=10 환경에서 평균 지연은 약 13 ms로 측정되어, 전체 보안 모드 대비 약 35% 개선되었으며, 일반 처리와 비교해도 약 2 ms(18%)의 증가에 그쳐 비교적 양호한 성능을 유지하였다. 이러한 결과는 중요도가 낮은 데이터에 대해 불필요한 암호화를 수행하지 않음으로써 전환 오버헤드가 줄어든 효과를 반영한다. 처리량 측면에서도 동일한 경향이 관찰되었는데, N=10 환경에서 전체 보안 모드의 처리량은 기준 대비 약 60% 수준으로 하락한 반면, 제안 기법은 약 85% 수준을 유지하여 성능 저하를 효과적으로 완화하였다.

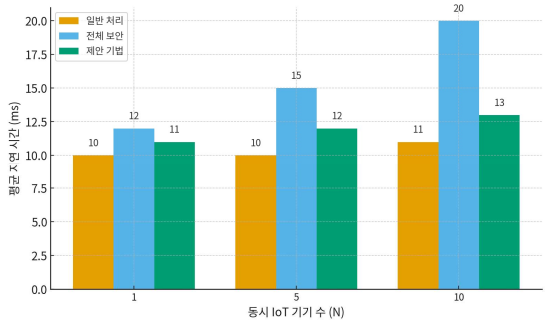



그림 5. 제안한 기법을 적용한 플랫폼 성능 비교

암호화 연산 자체의 소요 시간도 측정하였다. AES-128 알고리즘으로 128바이트 데이터를 암호화하는 데 약 0.2 ms, HMAC-SHA256을 생성하는 데 약 0.15 ms가 소요되었다. TrustZone 세계 전환 시간은 호출당 약 20~30 µs 수준으로 암호화 연산에 비해 상대적으로 작은 비중을 차지하였다.

실제로 데이터 크기를 256바이트, 512바이트로 확장하여 실험한 결과, 전체 보안 모드에서는 데이터 크기에 비례하여 지연 시간이 거의 선형적으로 증가한 반면, 제안 기법은 증가 폭이 절반 이하로 줄어들어 데이터 규모가 커져도 성능 저하가 상대적으로 완만하게 나타났다. 종합하면, 본 논문에서 제안한 프레임워크는 다수의 IoT 기기가 연결된 확장 환경에서도 TrustZone 기반 보안을 적용하면서 과도한 성능 저하를 방지할 수 있음을 실험적으로 확인하였다.

## V. 결 론

본 논문에서는 IoT 게이트웨이에 TrustZone 기술을 적용하고 oneM2M 플랫폼과 연동하여 선택적 데이터 보안 프레임워크를 구현하였다. 제안한 기법은 자원 제한적인 엣지 환경에서 하드웨어 보안 기능 사용에 따른 성능 저하를 최소화하기 위해 고안되었다. 구체적으로, 모든 데이터를 무조건 암호화하는 대신 사용자에게 중요도가 높은 정보만 선별적으로 보호함으로써 보안과 효율성의 균형을 달성하였다. Secure World에서는 중요도가 높은 데이터의 기밀성과 무결성을 보장하고, Normal World에서는 중요도가 낮은 데이터의 신속한 처리를 병행하는 이원화된 처리 구조를 갖는다. 실험 결과, 모든 데이터를 보안 처리할 경우 발생하는 심각한 성능 저하가 확인된 반면, 제안한 선택적 보안 프레임워크는 TrustZone으로 전달해야 하는 데이터양을 효과적으로 줄여 시스템의 확장성을 크게 높일 수 있었다. IoT 기기 수나 데이터량이 증가해도 본 프레임워크 적용 시 성능 저하가 완화되어 구조적 확장성과 성능 효율을 동시에 확보함을 종합적으로 확인하였다. 또한 oneM2M 표준 플랫폼과의 통합을 통해 본 솔루션이 실제 IoT 서비스 환경에 쉽게 적용 가능하고 이기종 시스템과의 상호운용성을 갖추었음을 보여주었다. 끝으로, 제안한 프레임워크는 경량 하드웨어 보안의 효과적인 활용 방안을 제시함으로써 향후 스

마트 홈, 스마트 헬스케어 등 다양한 분야의 IoT 데이터 보호에 기여할 수 있을 것으로 기대된다.

## REFERENCES


[1] Da Xu, Li, Wu He, and Shancang Li, "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233 - 2243, 2014.

[2] Cao, Keyan, et al., "An Overview on Edge Computing Research," *IEEE Access*, vol. 8, pp. 85714 - 85728, 2020.

[3] 김정녀, "안전한 스마트 단말을 위한 가상화 기반 도메인 분리 보안 플랫폼 구현," *스마트미디어저널*, 제5권, 제4호, pp. 116 - 123, 2016년 12월

[4] Lu, Xiaofeng, et al., "Privacy Information Security Classification for Internet of Things Based on Internet Data," *International Journal of Distributed Sensor Networks*, vol. 11, no. 8, pp. 932941, 2015.

[5] H. Kim and Y. Kim, "Securing IoT Devices with ARM TrustZone," in Proceedings of *IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1 - 2, Jan. 2017.

[6] 허만우, 박기철, 홍지만, "사물인터넷 게이트웨이 보안을 위한 사용자 민감 데이터 분류," *스마트미디어저널*, 제8권, 제4호, 17 - 24쪽, 2019년

[7] Kim, Jaeho, et al., "Towards the oneM2M Standards for Building IoT Ecosystem: Analysis, Implementation and Lessons," *Peer-to-Peer Networking and Applications*, vol. 11, no. 1, pp. 139 - 151, 2018.

[8] ISO/IEC 30141:2018, Internet of Things (IoT) - *Reference Architecture, International Organization for Standardization*, 2018.

[9] ETSI, Multi-Access Edge Computing (MEC); *Framework and Reference Architecture*, ETSI GS MEC 003, 2019.

[10] 이지호, 최성찬, 정승명, 박종홍, 김재호, "모비우스 플랫폼을 활용한 지능 서비스 기술 개발 사례," *지능정보통신 (The Magazine of KIICE)*, 제19권, 제1호, pp. 11 - 30, 2018년 6월

[11] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on Multi-Access Edge Computing for Internet of Things Realization," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2961 - 2991, 2018.


## 저 자 소 개


**박기철(정회원)**

2019년 선문대학교 전자공학과 학사 졸업.
2021년 숭실대학교 컴퓨터 학과 석사 졸업.

<주관심분야 : 시스템 소프트웨어, 운영체제>

**권용진(준회원)**

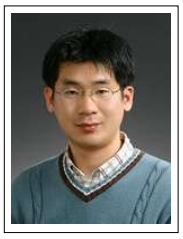
2023년 한국외국어대학교 컴퓨터전자시스템공학부 학사 졸업
2025년 성균관대학교 전자전기컴퓨터공학과 석사 재학

<주관심분야 : 클라우드컴퓨팅, 시스템소프트웨어>

**안재훈(정회원)**

2007년 광운대학교 컴퓨터공학과 학사 졸업.
2009년 숭실대학교 컴퓨터공학과 석사 졸업.
2014년 숭실대학교 컴퓨터공학과 박사 졸업.

<주관심분야 : 시스템 소프트웨어, 운영체제>



**김영환(정회원)**

2000년 부경대학교 컴퓨터공학과 학사 졸업.
2003년 성균관대학교 컴퓨터공학과 석사 졸업.
2011년 숭실대학교 컴퓨터공학과 박사 졸업.

<주관심분야 : 시스템 소프트웨어, 운영체제>