D²IP 인증 및 암호화 기법 연구 : DDS 기반 데이터베이스 통합 플랫폼 인증 및 암호화 기법 연구

김 용 성, 최 영°, 송 병 권*, 강 선 미**

서경대학교

wiz@skuniv.ac.kr, °cy@skuniv.ac.kr, *bksong@skuniv.ac.kr, **smkang@skuniv.ac.kr

A DDS based Database Integration Platform authentication and encryption

Yongseong Kim, Young Choi°, Byungkwen Song*, Sunmee Kang**

SeoKyeong Univ

요 약

OMG에서 제안한 통신 미들웨어 표준인 DDS(Data Distribution Service)는 중앙서버 없이 단순 발간, 구독 방식의 정보 교환을 제공하는 국제 표준 통신 규격이며 사물인터넷을 위한 최적의 실시간 통신 미들웨어이다. Open DDS를 이용하여 DDS 기반 데이터베이스 통합 플랫폼 D²IP(A DDS based Database Integration Platform)을 구현하였으며, 사물인터넷 및 다양한 단말로부터 데이터를 수집하여 저장하는데 활용하고 있다. 본 논문은 DDS에서 데이터를 수집하고 이를 시계열 데이터베이스(Time Series Database)에 저장하는 서비스에서 DDS 발간/구독을 위해 인증 처리와 메시지의 암복호화를 통해 보다 안정적이고, 강화된 보안 서비스를 위한 방안을 제시한다.

Ⅰ. 서 론

정보통신기술의 발달로 인하여 사물인터넷(Internet of Things, IIoT) 및 산업용 사물 인터넷(Industrial Internet of Things, IIoT) 기술도 많은 발전을 이루고 있으며, 다양한 환경에 맞추어 사물인터넷 기기도 최적화되어 제작되고 있다.

OMG(Object Management Group)에서 제안한 통신미들웨어인 DDS(Open Data Distribution Service)는 발간/구독(Publish/Subscribe) 방식의 실시간 데이터 통신이 필요한 고성능, 고확장성의 사물인터넷 환경에 적합하다.[1]

본 연구에서는 OpenDDS(Open Data Distribution Service) 기반으로 만들어진 D²IP(A DDS based Database Integration Platform)를 이용하여 사물인터넷 기기에서 데이터 수집하여, 시계열 데이터베이스인 InfluxDB에 저장하는 시스템에서 데이터 전송 구간의 데이터 보호를 위하여 발간/구독을 위한 인증과 메시지 데이터의 암복호화에 대한 방안을 제시한다.

Ⅱ. D²IP를 이용한 IoT 데이터 수집 시스템 설계

2.1 D²IP 서비스

본 연구에서는 실내 유기필름을 이용한 제품 사용조건별 생활환경 중 유해물질 노출량을 수집하는 환경에 D²IP를 적용하여 실험해 보았다.

D²IP는 DDS기반 데이터베이스 통합 플랫폼이다. D²IP는 데이터베이스에서 발행(Publisher)/구독(Subscriber)을 관리할 수 있고, 데이터베이스의 변경 사항을 발간/구독 할 수도 있으며, 구독된 정보의 저장이 가능하다. 발행/구독의 데이터베이스가 처리되는 부분이 함수로 구성되어 있으며, 원격함수호출 클라이언트를 작성하여 서버의 함수를 호출할 수 있게 구성되어 있으며, 클라이언트를 DDS 발행/구독에서 선언하여 원하는 기능을 호출하여 사용하도록 구현되어 있다. 그림 1 D²IP 데이터베이스 서비스 구성은 DCPS모델에서 데이터베이스 서비스를 구성하였다.[2][3]

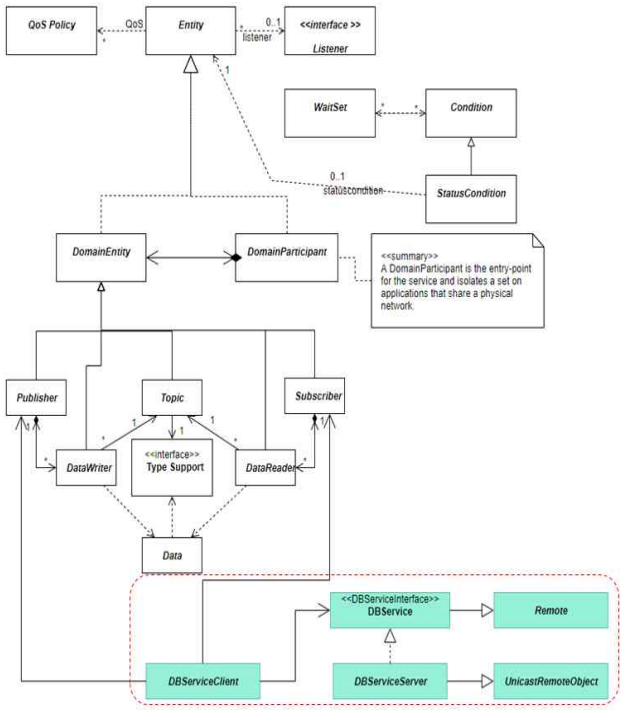

그림 1 D²IP 데이터베이스 서비스 구성

2.2 D²IP IoT 데이터 수집

IoT 장치에 식별번호(id) 값을 부여하고, 수집되는 데이터는 속성-값

(attribute-value) 쌍으로 이루어진 JSON(JavaScript Object Notation) 형태로 만들어서, 이를 장비식별번호와 메시지로 구성된 DDS IDL(Interface Description Language)을 생성하여 전송하도록 한다.

시계열 데이터베이스 InfluxDB는 tag keys-values, field keys-values의 구조로 저장 되므로 JSON 형태로 전송하고 저장하는 것이 효율적이다.

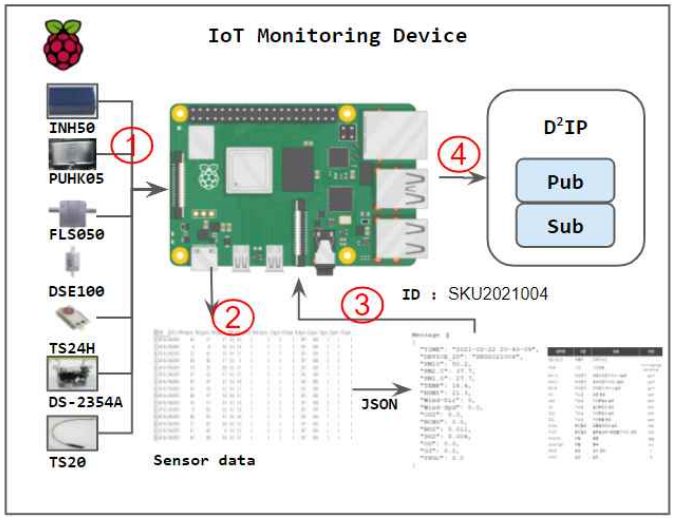

그림 2 IoT Monitoring Device

그림 2. IoT Monitoring Device의 ①의 다양한 센서를 통해서 데이터를 수집하여 ②와 같은 형태로 수집을 하여 ③과 같이 JSON 형태로 변환을 하여 D²IP를 통하여 DDS 토픽으로 서버에 저장이 된다.

Ⅲ. D²IP를 위한 인증과 전송 암복호화 설계 및 구현

3.1 D²IP 인증 및 암복호화 전송 설계

D²IP에서 메시지 전송을 위하여 아이디와 암호를 통하여 서버에서 인증을 통하여 암복호화에 사용할 공개키(Public key)를 발급 받고, 이를 이용하여 전송할 JSON 데이터를 암호화하여 전송하고, 서버에서는 개인키(Private Key)를 이용하여 복호화하여 데이터베이스에 저장한다.

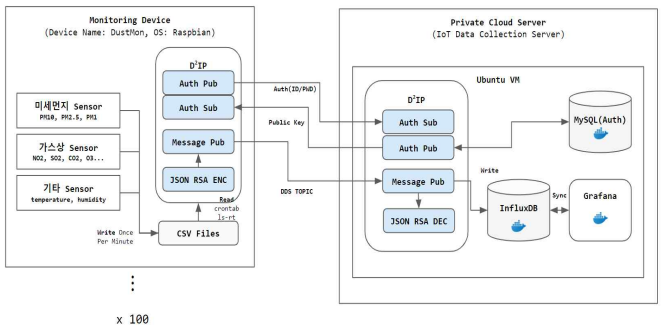

그림 3 D²IP 메시지 전송의 인증 및 암복호화 구조

D²IP의 암복호화 시스템은 RSA 암호화를 사용하였다. RSA는 두 개의 키를 사용하며, 키란 메시지를 열고 잠그는 상수(constant)를 의미한다. 공개키는 모두에게 알려져 있으며 메시지를 암호화하며, 암호화된 메시지는 개인키를 이용하여 복호화하는 방식으로 구현이 쉽고, 널리 사용되는 방식이다. TLS(Transport Layer Security), SSL(Secure Socket Layer)에도 사용되는 방식이다.

3.2 D²IP 암복호화 구현

D²IP는 OpenSSL(Secure Socket Layer)를 사용하여 RSA 키를 생성하였으며, 암호화 강도를 증가시키기 위해 2048비트의 키를 사용하지 않고 4096비트의 키를 사용하였다.[4]

RSA 키 크기가 클수록 연산 속도가 증가하여 속도가 느려질 수 있으며, CPU 사용량이 증가할 수 있다. 메시지를 암호화하게 되면 키 크기에 따라 항상 동일한 크기의 메시지를 전송할 수 있다.

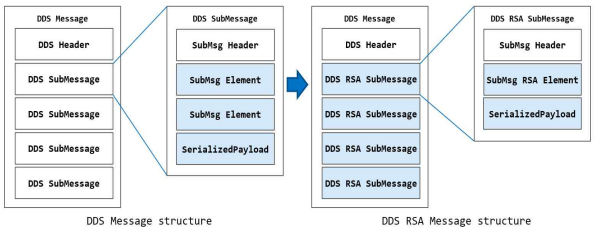

그림 4 D²IP DDS RSA message structure

그림 4. D²IP DDS RSA message structure와 같이 message를 RSA로 암호화하여 Payload를 일정하게 할 수 있다.

Ⅳ. 결 론

IoT 장치의 사용이 증가하고 비정형 데이터의 저장과 시계열 데이터베이스의 사용이 급증하고 있으며, 이에 따른 데이터의 보안에 대한 이슈가 증가하고 있다. 향후에는 DDS Security와 D²IP RSA를 적용한 것의 성능 분석과 키의 길이 512비트, 1024비트, 2048비트, 4096비트에 따른 성능분석 및 속도 향상을 위한 방법을 연구할 예정이다.

ACKNOWLEDGMENT

본 논문은 (재)한국화학융합시험연구원에서 시행한 “실내 유기필름을 이용한 제품 사용조건별 생활환경 중 유해물질 노출량 측정 기술” 과제 지원으로 작성되었습니다.

참 고 문 헌

[1] DDS Foundation "Why Choose DDS?" Object Management Group, Inc.(1997-2019), Retrieved Apr., 14, 2019, from https://www.dds-foundation.org.

[2] Y.S. Kim, Y. Choi, B.K. Song, S.M. Kang "OpenDDS based Database integrated service platform", Proceedings of Symposium of the Korean Institute of communications and Information Sciences / Pages.1044-1045, Korea, Feb, 2020.

[3] Introduction to OpenDDS, Don Busch, Principal Software Engineer and Partner Object Computing, Inc.(OCI)(2006-2019), Retrieved Oct., 22, 2019, from https://opendds.org/about/articles/Article-Intro.html.

[4] OpenSSL Strategic Architecture, Copyright © 1999-2018, OpenSSL Software Foundation., Retrieved Feb., 10, 2021, from https://www.openssl.org/