J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr


# 보안 공격에 강인한 사물인터넷 센서 기반 정보 시스템 개발☆

# Development of Internet of Things Sensor-based Information System Robust to Security Attack

윤 준 혁[1] 김 미 희*[1]
Junhyeok Yun Mihui Kim

**요 약**

사물인터넷 센서 장치와 빅데이터 처리 기법의 개발 및 보급으로 사물인터넷 센서를 활용한 정보 시스템이 여러 산업 분야에 적용되어 활용되고 있다. 정보 시스템이 적용된 산업 분야에 따라 정보 시스템이 도출하는 정보의 정확성이 산업의 효율, 안전에 영향을 미칠 수 있다. 따라서 외부 공격으로부터 센싱 데이터를 보호하고 정보 시스템이 정확한 정보를 도출할 수 있도록 하는 보안 기법이 필수적이다. 본 논문에서는 사물인터넷 센서 기반 정보 시스템의 각 처리 단계를 대상으로 하는 보안 위협을 살펴보고, 각 보안 위협에 대한 대응 기법을 제안한다. 나아가 제안하는 대응 기법을 통합하여 보안 공격에 강인한 사물인터넷 센서 기반 정보 시스템 구조를 제시한다. 제안 시스템에서는 경량 암호 알고리즘, 난독화 기반 데이터 유효성 검사 등 경량 보안 기법을 적용함으로써 저전력, 저성능의 사물인터넷 센서 장치에서도 최소한의 처리 지연만으로 보안성을 확보할 수 있도록 한다. 보편적으로 각 보안 기법을 실제로 구현하고 실험을 통해 성능을 보임으로써 제안 시스템의 실현 가능성을 보인다.

☞ 주제어 : 사물인터넷, 정보 시스템, 네트워크 보안, 빅데이터

**ABSTRACT**

With the rapid development of Internet of Things sensor devices and big data processing techniques, Internet of Things sensor-based information systems have been applied in various industries. Depending on the industry in which the information systems are applied, the accuracy of the information derived can affect the industry's efficiency and safety. Therefore, security techniques that protect sensing data from security attacks and enable information systems to derive accurate information are essential. In this paper, we examine security threats targeting each processing step of an Internet of Things sensor-based information system and propose security mechanisms for each security threat. Furthermore, we present an Internet of Things sensor-based information system structure that is robust to security attacks by integrating the proposed security mechanisms. In the proposed system, by applying lightweight security techniques such as a lightweight encryption algorithm and obfuscation-based data validation, security can be secured with minimal processing delay even in low-power and low-performance IoT sensor devices. Finally, we demonstrate the feasibility of the proposed system by implementing and performance evaluating each security mechanism.

☞ keyword : Internet of Things, Information System, Network Security, Big-data

## 1. 서 론

최근 빅데이터(Big Data) 처리 기술이 발전됨에 따라 다수의 사물인터넷(Internet of Things, IoT) 센서(Sensor) 장치로부터 방대한 양의 데이터(Data)를 수집하고 이를 분석, 처리하여 정보를 생성하는 다양한 정보 시스템(System)이 개발 및 보급되고 있다[1]. 정보 시스템이 적용된 산업 분야에 따라 사물인터넷 센서 기반 정보 시스템이 생성하는 정보의 정확도가 산업의 효율성부터 안전까지 넓은 범위에 영향을 미칠 수 있다. 예를 들어, 문화재 보호를 위해 설치한 사물인터넷 기반 위험 감시 시스템[2]의 경우, 감시 시스템의 오작동이 문화재 손실이라는 중대한 손해로 이어질 수 있다. 따라서 외부 공격으로 인해 정보 시스템이 잘못된 정보를 도출하지 않도록 보안 공격에 대한 적절한 대응 기법 적용이 필수적이다.

[1] School of Computer Engineering & Applied Mathematics, Computer System Institute, Hankyong National University, Jungang-ro, Anseong-si, Gyeonggi-do 17579, Korea.
* Corresponding author (mhkim@hknu.ac.kr)
[Received 1 July 2022, Reviewed 9 July 2022(R2 2 August 2022), Accepted 8 August 2022]
☆ This research was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No.2018R1A2B6009620).

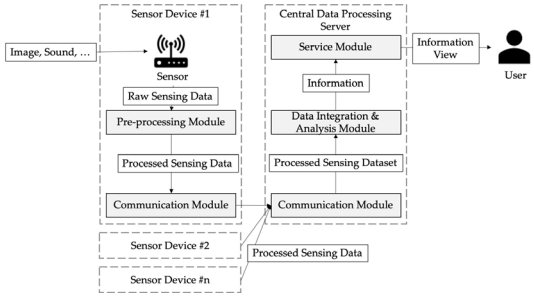
사물인터넷 센서 기반 정보 시스템은 일반적으로 데이터 센싱(Sensing), 데이터 전처리, 통신, 데이터 통합 및 분석의 단계를 거쳐 센싱 데이터로부터 정보를 도출하고 사용자에게 서비스를 제공한다[3, 4]. 공격자는 각 처리 단계의 취약점을 악용하여 데이터를 삽입, 변조함으로써 정보 시스템이 도출하는 정보의 정확도를 저하시킬 수 있다. 예를 들어, 공격자는 통신 단계에서 센싱 데이터를 중간 탈취하고 거짓 데이터를 대신 삽입할 수 있다[5]. 이미지(Image) 데이터를 수집하는 시스템은 일반적으로 통신 효율성을 위해 데이터 전처리 단계에서 보간 알고리즘(Algorithm)을 사용해 이미지의 크기를 줄인다[6]. 이 때, 보간 알고리즘의 취약점을 악용해 축소 전후의 이미지가 완전히 달라지도록 하는 이미지 스케일링(Image Scaling) 공격[7]을 수행할 수 있다. 이외에도 적대적 샘플 공격[8], 연결 탈취를 통한 거짓 데이터 삽입[9] 등 사물인터넷 센싱 데이터 기반 정보 시스템의 각 처리 단계에는 다양한 취약점이 존재하며, 정보 시스템이 정상적으로 활용되려면 이러한 취약점에 저항성을 가지는 시스템 구조와 보안 기법이 확보되어야 한다. 본 논문에서는 각 처리 단계에서 발생할 수 있는 보안 위협을 분석하고, 각 보안 위협에 대응하기 위한 보안 기법을 포함하는 보안 공격에 강인한 사물인터넷 센서 기반 정보 시스템 구조를 제안한다.

본 논문의 구성은 다음과 같다. 2장에서 사물인터넷 센서 기반 정보 시스템의 일반적인 구성과 기존 데이터 보안 기법 등 관련 연구를 소개하고, 3장에서 사물인터넷 센서 기반 정보 시스템의 각 처리 단계를 대상으로 하는 다양한 보안 위협과 대응 방안을 설명한다. 4장에서는 각 처리 단계에 대한 보안 기법을 통합하여 보안 공격에 강인한 사물인터넷 센서 기반 정보 시스템 구조를 제시한다. 5장에서 제안 시스템의 각 보안 기법 중 일부를 실제로 구현하고 성능을 평가한다. 6장에서 결론을 맺는다.

## 2. 관련 연구

### 2.1 사물인터넷 센서 기반 정보 시스템

그림 1은 일반적인 사물인터넷 센서 기반 정보 시스템의 구조를 도식화한 것이다. 사물인터넷 센서 기반 정보 시스템은 크게 센서 장치(Sensor Device)와 중앙 데이터 처리 서버(Central Data Processing Server)로 구성된다. 센서 장치는 센서(Sensor)와 전처리 모듈(Preprocessing Module), 통신 모듈(Communication Module)을 포함한다.




(그림 1) 사물인터넷 센서 기반 정보 시스템 구조
(Figure 1) Internet of Things Sensor-based Information System Structure

중앙 데이터 처리 장치는 통신 모듈과 데이터 통합 및 분석 모듈(Data Integration & Analysis Module), 서비스 모듈(Service Module)을 포함한다. 센서 장치의 센서는 실제 주변 환경으로부터 데이터를 수집한다. 정보 시스템의 목적에 따라 카메라(Camera), 미세먼지 센서, 소음 센서 등 다양한 종류의 센서를 사용할 수 있다. 전처리 모듈은 센서가 수집한 데이터에 대한 전처리를 수행한다. 전처리는 데이터 오차 보정, 통신 효율성 향상, 처리 효율성 향상을 위한 형식 변환 등 다양한 목적, 방법으로 수행할 수 있다. 통신 모듈은 센싱 데이터를 중앙 데이터 처리 서버로 전송한다. 중앙 데이터 처리 서버의 통신 모듈은 센서 장치와 통신하여 센싱 데이터를 전송받는다. 데이터 통합 및 분석 모듈은 여러 센서 장치로부터 전송받은 데이터를 통합하고 분석한다. 통합 단계에서 이상치 제거, 중복 제거 등 후처리를 수행한다. 여러 센서 장치로부터 전송받은 대량의 데이터를 효율적으로 처리하기 위해 맵리듀스(Map Reduce) 알고리즘[10]을 지원하는 하둡(Hadoop)[11], 스파크(Spark)[12] 등 분산 처리 프레임워크(Framework)를 사용할 수 있다. 통합된 데이터를 분석하는 방법은 정보 시스템의 목적에 따라 달라질 수 있다. 예를 들어, 교통 정보 제공 시스템의 경우 수집된 교통량 데이터를 기반으로 정해진 기준에 따라 혼잡도를 계산할 수 있다[13]. 서비스 모듈은 생성된 정보를 사용자가 이해하기 쉬운 형태로 제공한다. 서비스 제공의 형태는 웹(Web) 서비스, 전용 클라이언트(Client) 응용프로그램을 이용한 서비스 등 다양한 형태로 나타날 수 있다.

### 2.2 기존 데이터 보안 기법

데이터 기반 정보 시스템은 오래전부터 개발, 보급되

어 사용됐고, 이를 대상으로 하는 다양한 보안 위협 역시 등장했다. 따라서 암호화 알고리즘[14, 15], 이상치 탐지 기법[16] 등 데이터 기반 정보 시스템의 보안성 확보를 위한 다양한 보안 기법들이 개발, 보급되어 다수의 정보 시스템에 적용되었다. 그러나 사물인터넷 센서를 기반으로 하는 정보 시스템은 기존의 정보 시스템과 다른 특성을 가진다. 사물인터넷 센서 장치는 일반적으로 작동을 멈추지 않기 때문에 저전력, 저성능의 처리 장치를 기반으로 설계한다[17]. 따라서, 사물인터넷 센서 기반 정보 시스템의 센서 장치을 위한 보안 기법은 저성능 환경에서도 정상적으로 작동할 수 있어야 한다. 중앙 데이터 처리 장치 역시 24시간 수집되는 방대한 양의 센싱 데이터를 처리해야하기 때문에 보안 기법 적용으로 인한 처리 부하를 최소화해야 한다[18]. 보안 기법 적용으로 인한 처리 부하가 큰 경우, 센싱 데이터 처리 성능에 악영향을 줄 수 있고, 결과적으로 정보 시스템의 실시간성을 잃을 수 있다. 표 1은 기존에 널리 사용되는 보안 기법이 사물인터넷 센서 기반 정보 시스템에 적용하기 어려운 이유와 대안을 정리한 것이다.

(표 1) 기존 보안 기법의 한계와 대안
(Table 1) Limitation of Existing Security Mechanisms and Alternatives

| Security Mechanism | Limitation | Alternatives |
|---|---|---|
| Block Encryption Algorithm | High Processing Overhead | CSPRNG-based Lightweight Encryption Algorithm |
| Statistic-based Data Validation | Can Conduct After All Data Collected | Obfuscation-based Data Validation |

정보 시스템의 통신 단계에서 공격자는 센싱 데이터를 중간에서 탈취하고 이를 변조 후 재전송하여 정보 시스템이 정상적인 데이터를 수집하지 못하도록 하고, 나아가 정상적인 정보를 생성하지 못하게 할 수 있다. 이러한 공격을 막기 위해 RSA(Rivest Shamir Adlema), AES (Advanced Encryption, Standard)와 같은 블록 암호 알고리즘을 사용해 센싱 데이터를 암호화할 수 있다. 그러나 블록 암호 알고리즘은 암호화 처리 과정에서 발생하는 처리 부하가 크기 때문에 저전력, 저성능 처리 장치를 포함하는 사물인터넷 센서 장치에 적용하기에는 부적절하다[19]. 본 논문에서 제안하는 시스템은 암호학적으로 안전한 의사 난수 생성기(Crypto Secure Pseudo Random Number Generator, CSPRNG)를 기반으로 하는 대치 암호 알고리즘을 적용해 저성능 환경인 센서 장치에서도 데이터를 빠르게 암호화하여 안전하게 전송할 수 있도록 한다.

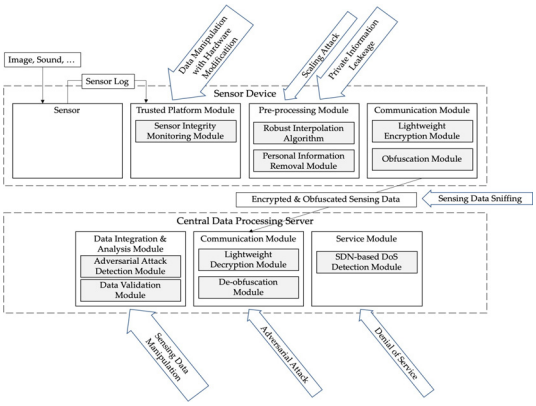
센싱 데이터의 유효성을 검증하기 위해 수집된 데이터의 분포를 분석하고, 이를 기반으로 이상치를 제거할 수 있다. 그러나 분포 분석을 통한 이상치 제거 기법은 센싱 데이터 수집이 완료된 시점에 사용할 수 있다. 또한, 분석해야 하는 센싱 데이터의 수량이 많은 경우 처리 부하가 급격히 증가할 수 있다. 따라서 다수의 센서 장치로부터 실시간 센싱 데이터를 수집해 처리하는 사물인터넷 센서 기반 정보시스템에 적용하기에 부적절하다. 본 논문에서 제안하는 시스템은 센서 장치와 중앙 데이터 처리 장치가 미리 합의한 난독화 함수를 적용하여 공격자가 임의로 삽입한 데이터가 정상 데이터와 완전히 다른 범위에서 나타나도록 한다. 이러한 방법을 적용함으로써 사물인터넷 센서 기반 정보 시스템의 실시간성을 유지하면서 동시에 센싱 데이터의 유효성을 빠르게 검증할 수 있다.

본 논문에서 제안하는 시스템은 이처럼 저성능 환경, 실시간성 등 사물인터넷 센서 기반 정보 시스템의 특성을 고려하여 설계한 보안 기법을 적용함으로써 사물인터넷 센서 기반 정보 시스템에서 낮은 처리 부하만으로 보안성을 확보하는 방법을 제시한다. 나아가 통신 단계뿐만 아니라 데이터 전처리, 데이터 통합 및 분석, 서비스 제공 단계에서 발생할 수 있는 다양한 보안 취약점을 분석하고 각 보안 취약점에 대한 대응 보안 기법을 포함하는 정보 시스템 구조를 제안한다.

## 3. 제안 시스템

### 3.1 제안 시스템 구조

그림 2는 본 논문에서 제안하는 보안 공격에 강인한 사물인터넷 센서 기반 정보 시스템의 구조를 도식화한 것이다. 제안 시스템은 일반적인 사물인터넷 센서 기반 정보 시스템과 동일하게 센서 장치(Sensor Device)와 데이터 처리 서버(Data Processing Server)로 구성된다. 센서 장치는 센서(Sensor), 전처리 모듈(Pre-processing Module), 통신 모듈(Communication Module), 신뢰 플랫폼 모듈(Trusted Platform Module)이 포함된다. 중앙 데이터 처리 서버에는 통신 모듈(Communication Module), 데이터 통합 및 분석 모듈(Data Integration & Analysis Module), 서비스 모듈(Service Module)이 포함된다. 각 모듈 방향으로 향하는 화살표는 해당 처리 단계를 대상으로 하는 보안 공격을 의미한다. 서비스를 대상으로 하는 서비스 거부 공격에 대응하기 위해 중앙 데이터 처리 서버는 소프트웨어




(그림 2) 제안 시스템 구조
(Figure 2) Proposed System Structure

정의 네트워크(Software Defined Network, SDN)을 통해 서비스를 사용자에게 제공한다. 제안 시스템의 각 모듈에 포함된 보안 기법은 정보 시스템의 응용 분야에 상관없이 공통적으로 포함되는 모듈에 대한 보안 공격을 막을 수 있도록 구성했다. 정보 시스템의 응용 분야에 따라 데이터의 특성, 전처리 방법 등이 달라질 수 있으며 이로 인해 발생하는 보안 위협은 본 연구에서 다루지 않는다. 각 보안 기법은 사물인터넷 센서 기반 정보 시스템의 저성능 환경과 실시간성을 고려하여 처리 부하 및 통신 부하를 최소화할 수 있는 위치에 배치한다. 센서 장치의 전처리 모듈에는 보간 알고리즘 공격에 저항성을 가지는 보간 알고리즘과 개인정보 제거 모듈이 포함된다. 보간 알고리즘은 이미지 데이터를 수집하는 시스템에 적용하여 이미지 크기 조정으로 발생할 수 있는 보간 알고리즘 공격에 대응한다. 개인정보 제거 모듈은 응용에 따라 다르게 구현한다. 센싱 데이터에 개인정보가 포함될 가능성이 없는 경우 구현하지 않을 수 있다. 이러한 보안 기법들은 처리해야하는 데이터의 양이 크지 않고, 외부에서 처리하는 경우 높은 통신 부하를 유발할 수 있기 때문에 센서 장치에 배치한다. 통신 모듈에는 경량 암호화 알고리즘과 난독화 모듈이 포함된다. 경량 암호화 알고리즘은 센서 장치와 중앙 데이터 처리 서버가 사전에 합의된 동일한 시드(Seed)를 공유하는 의사 난수 생성기를 기반으로 대칭 암호화를 수행한다. 시드의 안전한 보관을 위해 센서 장치의 신뢰 플랫폼 모듈에 시드를 저장한다. 난독화 모듈은 센싱 데이터의 범위를 확장하여 이상치를 더 효율적으로 찾을 수 있도록 한다. 예를 들어, 온도 데이터를 수집하는 정보 시스템에서 온도 값은 특정 범위 안에서 나타난다. 공격자는 이러한 특성을 이해하고 시스템이 이상치로 처리하지 않는 범위 안에서 거짓 데이터를 생성하고 삽입할 수 있다. 난독화가 적용된 경우 난독화 이후의 센싱 데이터 값의 범위가 확장되기 때문에, 공격자가 적절한 거짓 데이터를 생성하기 어렵다. 신뢰 플랫폼 모듈은 센서 로그를 기록하고, 통신 모듈을 통해 센서 로그를 중앙 데이터 처리 서버로 전송한다. 중앙 데이터 처리 서버는 센서 로그를 검토하여 센서 하드웨어에 변조가 확인되거나 로그가 유효하지 않은 것으로 판단되면 해당 센싱 데이터를 유효하지 않은 데이터로 판단하고 제거한다.

데이터 처리 서버의 통신 모듈에는 경량 암호화 알고리즘과 난독화 모듈이 포함된다. 경량 암호화 알고리즘은 센서 장치가 전송한 암호화된 센싱 데이터를 복호화한다. 난독화 모듈은 난독화 함수의 역을 적용하여 원래의 센싱 데이터 값을 복원한다. 전처리 및 분석 모듈에는 유효성 검증 모듈이 포함된다. 유효성 검증 모듈은 난독화가 해제된 센싱 데이터에 대해 정상 범위를 벗어난, 즉 이상치로 판단되는 값을 가지는 센싱 데이터를 제거한다. 난독화를 통해 공격자가 삽입한 거짓 데이터의 범위가 정상 데이터와 다르게 나타나도록 했기 때문에, 전체 센싱 데이터에 대한 분석 이전에 이상치를 탐지하고 제거할 수 있다. 이상치 제거는 센서 장치에서도 수행할 수 있다. 그러나 통신 단계에서의 악의적 데이터 삽입에 대응하기 위해서는 데이터 처리 서버에서 이중 탐지를 해야 하며, 센서 장치에서 이상치 제거를 수행하는 경우 데이터의 실시간성을 해치기 때문에 제안 시스템에서는 유효성 검증 모듈을 데이터 처리 서버에 배치한다. 서비스 모듈에는 소프트웨어 정의 네트워크 기반 서비스 거부 공격 탐지 모듈이 포함된다. 서비스를 위한 패킷은 [20]의 연구에서 제시한 소프트웨어 정의 네트워크로 포워딩되며, 허니팟에 수집된 공격 패킷 정보는 소프트웨어 정의 네트워크 기반 서비스 거부 공격 탐지 모듈로 전달받아 서비스 거부 공격 발생 여부를 감시한다.

## 3.2 제안 시스템 적용 보안 기법

표 2는 사물인터넷 센서 기반 정보 시스템의 각 처리 단계를 대상으로 하는 보안 취약점을 나타낸 표이다. 사물인터넷 센서 기반 정보시스템의 각 처리 단계를 대상으로 하는 보안 위협과 각 보안 위협에 대한 대응 방안을 정리했다. 본 절에서는 각 처리 단계에서의 보안 위협과 대응 방안에 대해 자세히 설명한다.

(표 2) 사물인터넷 센서 기반 정보 시스템 대상 보안 공격 및 대응 방안

(Table 2) Security Thread and Countermeasures for Internet of Things Sensor Based Information System

| Process | Security Threat | Countermeasure |
|---|---|---|
| Data Sensing | Data Manipulation with Hardware Modification | Trusted Platform Module |
| | Private Information Leak | Personal Information Masking Model |
| Data Analysis | Adversarial Attack | Image Feature-based Adversarial Example Detection Model |
| Data Preprocessing | Scaling Attack | Resistance Interpolation Algorithm |
| Communication | Sensing Data Manipulation | Lightweight Obfuscation Algorithm-based Sensing Data Validation |
| | Sensing Data Sniffing | CSPRNG-based Lightweight Encryption |
| Service | Denial of Service | SDN-based Denial of Service Detection |

### 3.2.1 데이터 센싱 보안 위협

데이터 센싱 단계는 센서 장치에 포함된 센서를 사용해 실제로 주변 환경으로부터 데이터를 수집하는 단계로, 중앙 데이터 처리 장치와 달리 공격자가 센서 장치에 물리적으로 쉽게 접근할 수 있으므로 물리적 공격이 주로 발생한다.

하드웨어 조작을 통한 센싱 데이터 변조 공격은 공격자가 센서 장치에 직접 접근하여 센서 장치에 포함된 외부 입출력 장치 등을 통해 악성 코드를 삽입하거나 센서를 조작하여 센싱 데이터의 값을 변조하는 보안 공격이다. 센서 장치에 대한 물리적 보안을 강화하더라도 현실적으로 모든 센서 장치를 계속해서 감시할 수 없으므로 물리적 공격을 완전히 차단하는 것은 어렵다. 제안 시스템에서는 센서 장치에 신뢰 플랫폼 모듈을 적용함으로써 센서 장치의 조작 여부를 중앙에서 탐지할 수 있도록 한다. 신뢰 플랫폼 모듈은 센서 장치의 중앙 처리 장치, 메모리(Memory)와 완전히 격리된 상태로 시스템을 감시할 수 있도록 설계된 보안 칩셋(Chipset)이다. 신뢰 플랫폼 모듈은 시스템 장치의 작동 로그를 내부에 저장하고, 이를 주기적으로 중앙 데이터 처리 장치로 전송한다. 하드웨어 조작을 통한 센싱 데이터 변조 공격이 발생한 경우, 서비스 관리자는 장치 작동 로그를 통해 하드웨어 조작이 발생한 사실을 확인하고 해당 센서 장치로부터 전송된 센싱 데이터를 유효하지 않은 데이터로 처리할 수 있다. 신뢰 플랫폼 모듈은 하드웨어(Hardware) 암호화를 사용하기 때문에 현실적으로 신뢰 플랫폼 모듈에 저장된 장치 작동 로그를 변조하는 것은 불가능에 가깝다. 또한, 공격자가 신뢰 플랫폼 모듈을 물리적으로 제거한 경우에도 서비스 관리자는 해당 센싱 데이터가 신뢰 플랫폼 모듈에 의해 검증되지 않았기 때문에 유효하지 않은 데이터로 처리한다. 제안 시스템에서는 센서 장치에 TPM을 적용하여 센서 로그를 기록하고 이를 통해 하드웨어 조작을 통한 센싱 데이터 변조 공격에 대응한다.

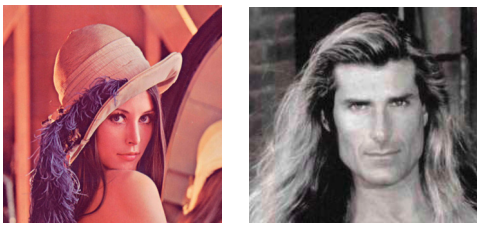
센싱 데이터에 개인정보가 포함된 경우, 센서 장치에서 중앙 데이터 처리 장치로 센싱 데이터를 전송하는 과정에서 외부 공격자에 의해 개인정보 유출 문제가 발생할 수 있다. 따라서 센싱 데이터를 중앙 데이터 처리 장치로 전송하기 전 센서 장치에서 센싱 데이터에 포함된 개인정보를 제거해야 한다. 예를 들어, 카메라를 사용한 주차장 폐쇄도 정보 시스템의 경우 차량 번호판과 같은 정보가 포함될 수 있다. 이러한 경우 Haar 알고리즘 등 객체 검출 알고리즘을 사용해 이미지에 포함된 차량 번호판을 탐지하고, 해당 부분을 제거하여 개인 정보 유출 문제에 대응할 수 있다[21, 22]. 정보 시스템의 목적에 따라 센싱 데이터 개인정보 포함 여부나 형태가 달라지기 때문에 각 응용에 따라 적절한 개인정보 제거 모듈이 센서 장치에 포함되어야 한다. 제안 시스템에서는 센서 장치의 전처리 모듈에 응용에 따라 적절한 개인정보 제거 모듈을 적용하여 개인정보 유출 문제에 대응한다.

### 3.2.2 데이터 전처리 보안 위협

데이터 전처리 단계에서는 처리 효율성, 통신 효율성 향상을 목적으로 센서로부터 수집된 센싱 데이터를 다양한 방법으로 처리한다. 센싱 데이터가 이미지인 경우, 통신 부하를 줄이기 위해 이미지 크기를 축소할 수 있다. 센

싱 데이터에 포함된 값 중 일부가 정보 도출에 불필요하거나 원본 값이 아닌 통계치가 필요한 경우에도 중앙 데이터 처리 서버에서의 처리 효율성 향상을 위해 센서 장치에서 전처리를 수행할 수 있다.

보간 알고리즘 공격은 카메라와 같은 이미지 센서를 사용하는 센서 장치를 대상으로 하는 보안 공격이다. 이미지 크기 축소 과정에서 사용되는 보간 알고리즘의 취약점을 이용한 공격으로, 카메라로 촬영한 이미지와 보간 알고리즘을 사용해 축소한 이미지가 완전히 다르게 보이도록 하는 특수 이미지를 생성하여 공격한다. 그림 3은 실제로 보간 알고리즘 공격에 사용되는 특수 이미지로, 그림 3-(a)의 이미지를 보간 알고리즘을 사용해 축소하면 그림 3-(b)의 이미지로 변환된다. 이는 보간 알고리즘이 특정 픽셀(Pixel) 주위의 평균값 등을 기반으로 새로운 픽셀을 형성하는 특성을 이용한 것으로, 큰 가중치를 곱한 목표 이미지를 일부 픽셀에 삽입하여 보간 알고리즘 적용 시 최종 픽셀이 목표 이미지의 것으로 결정되도록 한다. 제안 시스템에서는 센서 장치의 전처리 모듈에 보간 알고리즘 공격에 저항성이 있는 수정된 보간 알고리즘을 적용하여 보간 알고리즘 공격에 대응한다. [23, 24] 등의 연구에서는 보간 알고리즘 공격에 저항성을 가지는 보간 알고리즘을 제시했다.



(a) (b)

(그림 3) 보간 알고리즘 공격 이미지 (a) 공격 이미지 예시 (b) 보간 후 이미지

(Figure 3) Interpolation Algorithm Attack Image (a) Attack Image Example (b) Image After Interpolation

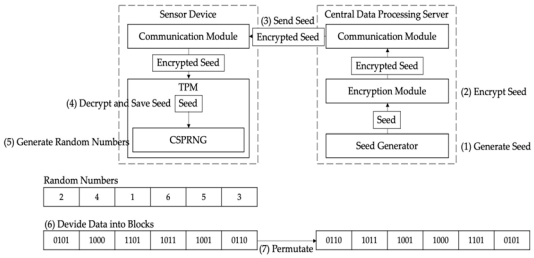
### 3.2.3 통신 보안 위협

통신 단계에서는 센서 장치에서 수집한 센싱 데이터를 중앙 데이터 처리 서버로 전송한다. 통신 단계에서는 외부 공격자가 센서 장치와 중앙 데이터 처리 서버의 연결을 탈취할 가능성이 높다. 따라서 외부 공격자가 연결을 탈취하더라도 센싱 데이터의 내용을 확인할 수 없도록 하고, 센싱 데이터의 유효성을 확보하는 것이 중요하다.

센싱 데이터 변조 공격은 외부 공격자가 연결을 탈취하고 실제 센싱 데이터와 다른 거짓 데이터를 중앙 데이터 처리 서버로 전송하여 정보 시스템이 올바른 판단을 내리지 못하도록 하는 보안 공격이다. 센싱 데이터 변조 공격은 센싱 데이터 수집 후 분포도 분석을 통해 이상치를 제거함으로써 대응할 수 있다. 그러나 이상치 제거를 통한 대응은 모든 센서 장치로부터 센싱 데이터를 모두 수집한 이후에만 수행할 수 있기 때문에 정보 시스템의 실시간성을 만족시킬 수 없다. 제안 시스템에서는 난독화 함수를 사용해 센싱 데이터의 범위를 확장한다. 공격자는 센서 장치가 수집하는 센싱 데이터의 종류를 파악하더라도 난독화 함수를 알 수 없기 때문에 정상 범위 내의 거짓 데이터를 생성할 수 없다. 제안 시스템에서는 센서 장치의 통신 모듈과 중앙 데이터 처리 서버의 통신 모듈에 난독화 함수를 적용하여 센싱 데이터 유효성을 빠르게 검사할 수 있도록 한다.

센싱 데이터 탈취 공격은 센싱 데이터에 대한 접근 권한이 없는 외부 공격자가 연결을 탈취하여 센싱 데이터의 내용을 확인하는 보안 공격이다. 센싱 데이터 탈취 공격은 데이터 암호화를 통해 대응할 수 있다. 그러나 저전력, 저성능 처리 장치를 포함하는 센서 장치의 특성으로 인해 암호화 과정에서의 처리 부하가 높은 블록 암호 알고리즘을 적용하는 것은 부적절하다. 따라서 저성능 환경에서도 정상 적으로 암호화를 수행할 수 있는 경량 암호화 알고리즘이 필요하다. 제안 시스템 에서는 암호학적으로 안전한 의사 난수 생성기(Crypto Secure Pseudo Random Number Generator, CSPRNG)를 사용해 저성능 환경에서도 데이터를 빠르게 암호화할 수 있는 방법을 제시한다. 센서 장치와 중앙 데이터 처리 서버는 의사 난수 생성기에서 사용할 동일한 시드(Seed)를 공유한다. 그림 4는 암호학적으로 안전한 의사 난수 생성기를 활용해 데이터를 암호화하는 과정을 도식화한 것이다. (1)중앙 데이터 처리 서버는 임의의 시드를 생성하고, (2)블록 암호를 사용해 암 호화하여 이를 (3)센서 장치로 안전하게 전송한다. 시드 교환은 전체 암호화 과 정 중 최초 1회만 수행되기 때문에 블록 암호를 사용했을 때의 처리 부하는 고려하지 않는다. (4)전송받은 시드는 복호화하여 신뢰 플랫폼 모듈에 저장한다. (5) 동일한 시드를 공유하는 중앙 데이터 처리 서버와 센서 장치는 암호학적으로 안 전한 의사 난수 생성기를 사용해 동일한 난수열을 생성한다. 암호학적으로 안전한 의사 난수 생성기는 난수열 일부를 통해 전체 난수열을 추론할 수 없음이 수학적으로 검증되었기 때문

에 시드를 탈취하지 않는 이상 외부 공격자는 난수열을 추론할 수 없다. (6)데이터를 여러 개의 블록으로 나누고 (7)난수열에 따라 대치를 수행한다. 이 때, 블록의 크기가 작고 블록의 개수가 많을수록 더 안전한 암호화 가 가능하다. 암호화된 데이터의 원문은 동일한 난수열을 사용해 역순으로 대치를 수행하여 얻을 수 있다.




(그림 4) 암호학적으로 안전한 의사 난수 생성기 기반 데이터 암호화

(Figure 4) Data Encryption Using Crypto Secure Pseudo Random Number Generator

### 3.2.4 데이터 분석 보안 위협

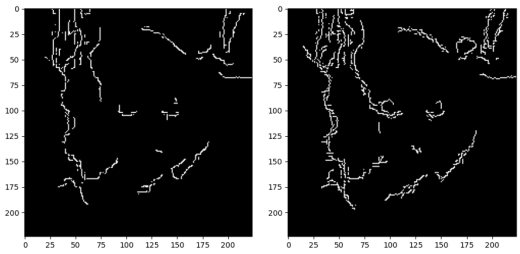
적대적 샘플 공격은 카메라와 같은 이미지 센서를 사용하는 센서 장치를 대상으로 하는 보안 공격이다. 카메라가 촬영 중인 물체에 페인트나 스티커 등을 이용해 노이즈를 삽입한다. 이렇게 변조된 센싱 데이터는 중앙 데이터 처리 장치로 전송되어 분석 단계에서 분석 모듈이 정상적으로 정보를 생성하지 못하게 한다. 페인트나 스티커 등을 이용하는 적대적 공격은 센싱 데이터 모니터링을 통해 공격 여부를 쉽게 판단할 수 있다. 그러나 최근의 적대적 샘플 공격 기법은 육안으로 확인하기 어려울 정도로 아주 작은 수준의 노이즈(Noise)만으로 수행할 수 있도록 발전했다. 그림 5는 최소한의 노이즈로 생성한 적대적 샘플의 예시이다. 그림 5-(a)와 5-(b)는 육안으로 구분이 어려울 정도로 유사하다. 그러나 그림 5-(a)는 이미지 분석 모델이 '비행기'로 분류하고 그림 5-(b)는 '고래'로 분류한다. 따라서 센싱 데이터가 변조된 적대적 샘플인지 확인하기 위한 보안 기법을 필요로 한다. 제안 시스템에서는 적대적 샘플에서 공통적으로 나타나는 엣지(Edge) 성분 주변 노이즈(Noise), 이산 코사인 변환(Discrete Cosine Transform, DCT) 계수 편향성 등 이미지 특성을 기반으로 센싱 데이터의 적대적 샘플 여부 탐지 모델을 적용한다.

(a) (b)

(그림 5) 최소한의 노이즈를 포함하는 적대적 샘플 예시 (a) 정상 이미지 (b) 적대적 샘플

(Figure 5) Example of the Adversarial Noise with Minimal Noise (a) Normal Image (b) Adversarial Sample

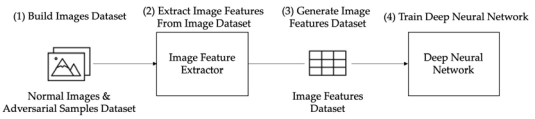
그림 6은 적대적 샘플에서 공통적으로 나타나는 엣지 성분 주변 노이즈 현상을 시각화한 것이다. 그림 6-(a)는 정상 이미지에서 추출한 엣지 성분, 그림 6-(b)는 적대적 샘플에서 추출한 엣지 성분으로, 적대적 샘플에서 추출한 엣지 성분의 경우, 정상 이미지에서 추출한 것과 달리 엣지 성분이 선형으로 나타나지 않고 엣지 성분 주변으로 노이즈가 발생하는 것을 확인할 수 있다. 제안 시스템에서는 이러한 특성을 기반으로 적대적 샘플 여부를 판단한다.




(a) (b)

(그림 6) 엣지 노이즈 비교 예시 (a) 정상 이미지의 엣지 노이즈 시각화 (b) 적대적 샘플의 엣지 노이즈 시각화

(Figure 6) An Example of the Edge Noise Comparison (a) Edge Noise Visualization of Normal Image (b) Edge Noise Visualization of Adversarial Sample




(그림 7) 적대적 샘플 탐지 모델 학습 처리 흐름
(Figure 7) Adversarial Sample Detection Model Training Flow

그림 7은 이미지로부터 다양한 특성을 추출하고, 이를 기반으로 적대적 샘플 탐지 모델을 학습하는 방법을 도식화한 것이다. 탐지 모델은 딥러닝 모델(Deep Learning Model)의 일종인 깊은 인공 신경망(Deep Neural Network, DNN)을 기반으로 한다. 탐지 모델을 학습하기 위해 (1) 다수의 정상 이미지 및 적대적 샘플을 포함하는 데이터셋(Dataset)을 구성한다. (2)데이터셋에 포함된 이미지로부터 엣지 성분 노이즈 비율, 이산 코사인 변환 계수 등 다양한 이미지 특성을 추출하여 (3)이미지 특성과 적대적 샘플 여부로 구성된 데이터셋을 생성한다. (4)해당 데이터셋을 학습 데이터로 하여 인공 신경망을 학습한다. 이렇게 학습된 인공 신경망을 이용해 적대적 샘플이 가지는 이미지 특성을 기반으로 입력 데이터의 적대적 샘플 여부를 탐지할 수 있다.

### 3.2.5 서비스 보안 위협

서비스 단계에서는 데이터 통합 및 분석 모듈에서 생성한 정보를 사용자에게 제공하기 위해 웹서비스, 전용 클라이언트 애플리케이션 등 다양한 형태로 서비스를 운영한다. 공격자는 서비스 가용성을 저해하여 정상적인 운영과 사용이 불가능하도록 서비스 거부 공격을 수행할 수 있다. 따라서 정보 시스템 서비스는 서비스 거부 공격에 대한 저항성을 확보해야 한다. [20]의 연구에서는 소프트웨어 정의 네트워크 구조와 허니팟을 활용해 다양한 종류의 지능형 서비스 거부 공격에 대응할 수 있는 방법을 제시했다. 제안 시스템에서는 서비스 모듈이 제공하는 서비스 패킷이 허니팟을 포함하는 소프트웨어 정의 네트워크를 거치게 함으로써 지능형 서비스 거부 공격에 대응한다.

## 4. 성능 평가

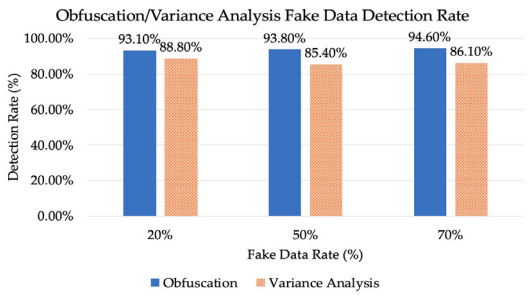
제안 시스템에 적용된 보안 기법의 공격 차단 성능과 처리 부하를 확인하기 위해 보안 기법 일부를 실제로 구현하고 실험을 수행했다. 난독화 알고리즘 적용을 통한 데이터 삽입 공격 대응 성능을 보이기 위해 난독화 이전과 이후의 유효 데이터 범위 변화와 처리 성능을 실험을 통해 비교한다. 이미지 특성 기반 탐지 모델을 통한 적대적 샘플 탐지 성능을 보이기 위해 적대적 샘플 탐지 모델을 학습하고 탐지 성능을 확인한다. 데이터 탈취 공격에 대한 대응 성능을 보이기 위해 의사난수생성기 기반 경량 암호 알고리즘의 처리 부하와 브루트포스(Bruteforce) 공격 가능성을 실험을 통해 확인한다. 표 3은 실험을 수행한 시스템 환경을 정리한 것이다. 센서 장치의 저전력, 저성능 환경을 재현하기 위해 센서 장치에서 작동하는 보안 기법은 암(Advanced RISC Machine, ARM) 아키텍처(Architecture) 환경에서 실험을 수행했다. 이러한 실험 환경은 사물 인터넷 환경을 위해 개발되어 널리 사용되고 있는 라즈베리 파이(Raspberry Pi) 및 호환 제품의 컴퓨팅 환경을 재현한 것이다.

(표 3) 실험 환경
(Table 3) Experimental Environment

| Data Processing Server | |
|---|---|
| CPU | Intel i7 Quad-core Processor |
| GPU | AMD Radeon Pro 555 |
| RAM | 16GB DDR4 |
| Network | GIgabit Ethernet |
| Sensor Device | |
| CPU | ARMv8 64bit 1.4GHz |
| RAM | 1GB LPDDR2 |
| Network | Gigabit Ethernet |

### 4.1 난독화를 위한 데이터 변조 공격 대응 성능

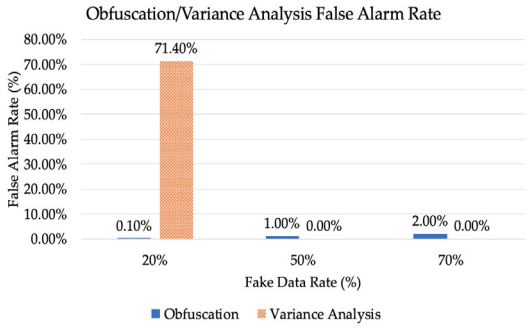
제안 시스템에서 난독화 알고리즘을 통한 데이터 변조 공격 대응 성능을 보이기 위해 데이터 수집이 완료된 후 분포도 분석을 통해 이상치를 제거하는 방법과 난독화를 통해 이상치를 제거하는 방법을 비교했다. 난독화 알고리즘은 제안 시스템에서 제안하는 기법으로 파이썬(Python) 언어를 사용해 구현했다. 분포도 분석을 통한 이상치 제거 기법은 [25]의 연구에서 제시한 클러스터링(Clustering) 기반 이상치 제거 기법을 동일하게 파이썬을 사용해 구현했다. 거짓 데이터 삽입은 전체 데이터 중 거짓 데이터가 차지하는 비율을 각각 20%, 50%, 70%로 하여 랜덤 값을 삽입하는 방법으로 수행했다.




(그림 8) 난독화/분포도 분석 기반 거짓 데이터 탐지 기법 탐지율 비교

(Figure 8) Obfuscation/Variance Analysis Fake Data Detection Rate Comparison

그림 8은 제안 시스템에 적용된 난독화 기반 거짓 데이터 탐지 기법과 분포도 분석 기반 거짓 데이터 탐지 기법의 탐지율을 비교한 것이다. 탐지율은 삽입된 거짓 데이터 중 탐지 기법에 의해 탐지된 데이터의 비율을 의미한다. 전체 데이터 중 거짓 데이터가 차지하는 비율이 증가함에 따라 탐지율이 저하되는 분포도 분석 기반 기법과 달리 난독화 기반 기법은 전체 데이터 중 거짓 데이터의 비율에 상관없이 비교적 높은 정확도를 유지하는 것을 확인할 수 있다. 분포도 분석 기반 기법의 경우 전체 데이터 중 거짓 데이터 비율이 늘어날수록 거짓 데이터를 중심 분포에서 떨어진 이상치가 아닌 또 다른 군집을 이루는 정상 데이터로 판단하는 것으로 추측할 수 있다. 그러나 난독화 기반 기법은 각 거짓 데이터의 분포를 확산시키기 때문에 이러한 현상이 쉽게 발생하지 않는다.




(그림 9) 난독화/분포도 분석 기반 거짓 데이터 탐지 기법 오탐지율 비교

(Figure 9) Obfuscation/Variance Analysis False Alarm Rate Comparison

그림 9는 난독화 기반 기법과 분포도 분석 기반 기법의 오탐지율을 비교한 것이다. 오탐지율은 탐지 기법이 거짓 데이터로 탐지한 데이터 중 실제로 거짓 데이터가 아닌 것의 비율을 의미한다. 분포도 분석 기반 기법의 경우 전체 데이터 중 거짓 데이터 비율이 낮을 때 71.4%로 매우 높은 오탐지율을 보였다. 이러한 특성은 거짓 데이터를 군집화 하는 과정에서 군집 최소 크기를 만족하기 위해 정상 데이터를 군집에 포함시키면서 발생하는 문제로 추측할 수 있다. 난독화 기반 기법의 경우 거짓 데이터 비율이 50% 이상일 때 1~2% 수준으로 분포도 분석 기반 기법 대비 높은 오탐지율을 보이지만, 낮은 수치이며 방대한 양의 데이터를 수집하는 사물인터넷 센서 기반 정보 시스템의 정보 도출에 영향을 미치지 않는 수준이다.

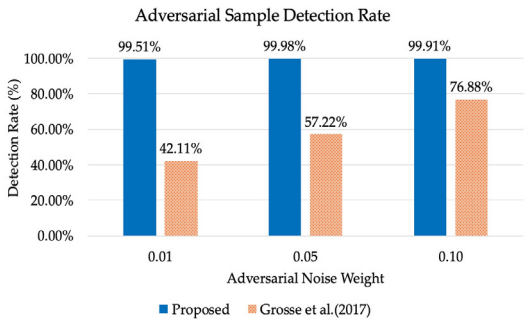
## 4.2 적대적 샘플 공격 탐지 성능

제안 시스템에서 이미지 특성 기반 적대적 샘플 탐지 모델을 통한 적대적 샘플 공격 탐지 성능을 확인하기 위해 이미지 특성 기반 적대적 샘플 탐지 모델과 [26]의 연구에서 제시한 통계 기반 적대적 샘플 탐지 기법의 성능을 비교했다. 각 기법은 파이썬으로 구현했으며, 이미지 특성 기반 적대적 샘플 탐지 모델 학습 을 위해 오픈 소스(Open Source) 이미지 데이터셋인 CIFAR[27]을 사용했다. 적대적 샘플은 [28]의 연구에서 제시한 JSMA(Jacobian Saliency Map Attacks) 기법을 사용해 생성했으며, 각각 0.01, 0.05, 0.1의 노이즈 가중치로 생성했다.


(그림 10) 적대적 샘플 탐지 예시

(Figure 10) An Example of Adversarial Sample Detection

그림 10은 제안 시스템의 적대적 샘플 탐지 모델을 실제로 구현하여 적대적 샘플을 탐지하는 화면이다. 실험에 사용한 이미지는 육안으로 보기에 '비행기'로 보이지만 적대적 노이즈가 삽입되어 인공지능 이미지 인식 모델은 '쾌속정'로 분류하는 적대적 샘플 이미지이다. 육안으로 원본 이미지와 구분하기 어려울 정도로 작은 노이즈만을 삽입했음에도 불구하고 적대적 샘플을 정상적으로 탐지해내



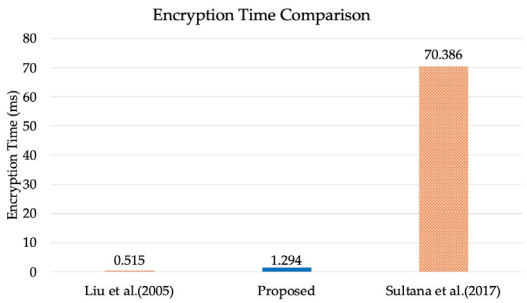

(그림 11) 적대적 샘플 탐지 성능
(Figure 11) Adversarial Sample Detection Performance

는 것을 확인할 수 있다. 그림 11은 제안 시스템에 적용된 이미지 특성 기반 적대적 샘플 탐지 모델과 통계 기반 적대적 샘플 탐지 모델[26]의 적대적 노이즈 삽입 수준에 따른 탐지율을 나타낸 것이다. 적대적 노이즈 가중치가 낮을수록 육안으로 적대적 샘플 여부를 확인하기 어려운 이미지이다. 가중치 0.01 수준의 노이즈가 삽입된 적대적 샘플에서 42.11%의 낮음 탐지율을 보인 통계 기반 적대적 샘플 탐지 모델과 달리 이미지 특성 기반 탐지 모델은 적대적 노이즈 가중치 0.01~0.1까지 다양한 적대적 샘플에 대해 모두 99% 이상의 높은 탐지율을 보임을 확인할 수 있다.

## 4.3 의사 난수 생성기 기반 경량 암호화 성능

제안 시스템에 적용된 의사 난수 생성기 기반 경량 암호화 기법의 성능을 확인하기 위해 암호화 알고리즘과 기존에 제안된 경량 암호 기법[29, 30]을 실제로 구현하고 처리 성능을 비교했다. 의사 난수 생성기 기반 경량 암호화 알고리즘은 보안성이 검증된 의사 난수 생성기를 사용하며, 신뢰 플랫폼 모듈을 사용해 시드를 안전하게 보관하도록 설계되었기 때문에 높은 보안성을 만족한다. 또한, 무차별 대입 공격의 경우 데이터를 200만개의 블록으로 나누었을 때 이론적으로 총 4,700경개의 데이터가 생성될 수 있기 때문에 사실상 불가능하다.

그림 12는 기존 경량 암호 알고리즘과 제안 기법의 암호화 시간을 비교한 것이다. [29]의 알고리즘이 0.515ms, 제안 알고리즘이 1.295ms, [30]의 알고리즘이 70.386ms의 암호화 시간을 보였다. [29]의 알고리즘이 가장 빠르게 암호화를 수행했으나, 해당 알고리즘은 동일한 대치 수열을 모든 데이터에 대해 사용하기 때문에 공격자가 암호문과 평문 쌍을 하나만 탈취하더라도 모든 데이터를 복호화할 수 있다. 제안 알고리즘의 경우, [29]의 알고리즘 대비 암호화 시간이 길지만, 이는 의사 난수 생성기를 사용해 대치 수열을 갱신하는 과정에서 발생하는 것으로, 이러한 과정을 통해 공격자가 암호문과 평문 쌍을 가지고 있더라도 다른 데이터를 복호화하지 못하도록 한다. 따라서 제안 알고리즘은 기존 기법 대비 빠르게 암호화를 수행할 수 있으면서 동시에 높은 보안성을 만족했다고 볼 수 있다.




(그림 12) 경량 암호 알고리즘 암호화 소요 시간 비교
(Figure 12) Lightweight Encryption Algorithms Encryption Time Comparison

## 4.4 전체 보안 기법 적용 시 처리 부하

표 4는 제안 시스템의 각 처리 단계에 적용된 보안 기법으로 인해 발생하는 처리 시간 증가를 나타낸 것이다. 모든 처리 시간은 1000개의 센싱 데이터를 처리했을 때, 그 중 한 개의 센싱 데이터를 처리하는데 걸린 평균 시간을 계산한 것이다. 데이터 처리 외에 통신 지연 등으로 인한 처리 시간 증가는 고려하지 않았다. 데이터 센싱 단계에서는 신뢰 플랫폼 모듈 적용으로 인한 처리 부하가 발생한다. 그러나 신뢰 플랫폼 모듈의 경우 하드웨어 칩(Hardware Chip)으로 처리 속도가 매우 빠르기 때문에 처리 시간에 큰 영향을 주지 못한 것을 확인할 수 있다. 데이터 전처리 단계에서는 저항성 보간 알고리즘 적용, 개인정보 제거 모델 적용으로 인한 처리 부하가 발생한다. 이 과정에서 센싱 데이터 당 평균 0.3ms 수준의 처리 시간 지연이 발생했다. 통신 단계에서는 난독화 알고리즘, 경량 암호 알고리즘 적용으로 인해 센싱 데이터 당 평균 1.3ms 수준의 처리 시간 지연이 발생했다. 데이터 통합 및 분석 단계에서는 적대적 샘플 탐지 모델 적용으로 인해 센싱 데이터 당 평균 47.6ms 수준의 처리 시간

지연이 발생했다. 데이터 통합 및 분석 단계에서의 센싱 지연은 중앙 처리 서버의 성능 향상, 병렬 연산 프로세서 추가 등의 방법으로 지연을 최소화할 수 있다. 서비스 단계에서는 다양한 서비스 거부 공격 탐지 및 차단 기법 적용으로 인해 센싱 데이터 당 평균 0.1ms 수준의 처리 시간 지연이 발생했다. 결과적으로, 제안 시스템은 보안 기법이 적용되지 않은 시스템 대비 센싱 데이터 당 평균 49.3ms 수준의 처리 시간 지연이 발생했다. 그러나 처리 시간 지연 중 대부분은 데이터 통합 및 분석 단계에서 발생한 것이고, 이는 중앙 처리 서버의 성능에 따라 감축시킬 수 있다. 따라서, 제안 시스템은 용납할 수 있는 수준의 처리 시간 증가만으로 높은 보안성을 만족시켰다고 볼 수 있다.

(표 4) 보안 기법 적용으로 인한 처리 시간 증가
(Table 4) Processing Time Increment due to Security Mechanisms Application

| Process | without Security Mechanisms (ms) | Proposed System (ms) | Increment |
|---|---|---|---|
| Data Sensing | 0.2 | 0.2 | 0ms (0.00%) |
| Data Preprocess-ing | 4.1 | 4.4 | 0.3ms (7.31%) |
| Communi-cation | 0 | 1.3 | 1.3ms ( %) |
| Data Integration & Analysis | 52.2 | 99.8 | 46.6ms (91.18%) |
| Service | 12.1 | 12.2 | 0.1ms (0.82%) |

## 5. 결론 및 향후 연구과제

본 논문에서는 사물인터넷 센서 기반 정보 시스템을 대상으로 하는 다양한 보안 위협과 각 보안 위협에 대한 대응 방안을 소개했다. 하드웨어 조작을 통한 데이터 조작, 적대적 이미지 공격, 보간 알고리즘 공격, 데이터 탈취, 서비스 거부 공격 등의 보안 공격을 공격의 목표가 되는 처리 단계에 따라 분류하고, 각 처리 단계의 처리 위치 및 특성에 따라 보안 알고리즘을 배치함으로써 보안 공격에 강인한 사물인터넷 센서 기반 정보 시스템 구조를 제안했다. 사물인터넷 센서 기반 정보 시스템은 다수의 저전력, 저성능 처리 장치 기반 센서 장치를 사용해 센싱 데이터를 수집하는 특성으로 인해 기존에 제안되고 사용하던 보안 기법을 그대로 적용하기 어렵다. 제안 시스템에서는 경량 암호화 알고리즘, 난독화 기반 유효성 검증 등 경량 보안 알고리즘을 적용하고 비교적 높은 처리 성능을 요구하는 보안 알고리즘은 중앙 처리 서버에 배치함으로써 최소한의 처리 부하만으로 보안 공격에 강인한 사물인터넷 센서 기반 정보 시스템을 구성했다. 또한, 제안 시스템에 적용한 각 보안 기법의 일부를 실제로 구현하고 그 성능을 분석하여 실현 가능성을 보였다.

향후 연구에서는 최근 보급이 확대되고 있는 영상 데이터 기반의 정보 시스템을 대상으로 하는 다양한 고수준 보안 공격과 이에 효과적으로 대응하기 위한 보안 기법을 연구하고자 한다. 이를 통해 제안하는 사물인터넷 센서 기반 정보시스템의 응용 범위를 확장할 수 있다.

## 참고문헌(Reference)

[1] Abbasi, A., Sarker, S. and Chiang, R. H., “Big data research in information systems: Toward an inclusive research agenda”, Journal of the association for information systems, Vol.17, No.2, pp.3, 2016. http://dx.doi.org/10.17705/1jais.00423

[2] Moo-kyung Jung, Chang-yong Choi, Ho-cheol Lee and Dong-myung Lee, “A Design of Platform of Portable Cultural Asset Surveilance System”, In Proceedings of Korea Institute of Information and Communication Engineering Conference, pp.599-600, 2013. https://koreascience.kr/article/CFKO201331751950292.page

[3] Dziak, D., Jachimczyk, B. and Kulesza, W. J. “IoT-based information system for healthcare application: design methodology approach”, Applied Sciences, Vol.7, No.6, pp.596, 2017. https://doi.org/10.3390/app7060596

[4] Guo, Y. and Qu, J. “Study on intelligent logistics management information system based on IOT and cloud computation in big data era”, The Open Cybernetics & Systemics Journal, Vol.9, No.1, 2015. http://dx.doi.org/10.2174/1874110X01509010934

[5] Tharayil, K. S., Farshteindiker, B., Eyal, S., Hasidim, N., Hershkovitz, R., Houri, S. and Oren, Y. “Sensor defense in-software (SDI): Practical software based detection of spoofing attacks on position sensors”,

Engineering Applications of Artificial Intelligence, Vol.95, pp.103904, 2020. https://doi.org/10.1016/j.engappai.2020.103904

[6] Kuemper, D., Iggena, T., Toenjes, R. and Pulvermueller, E. “Valid. IoT: a framework for sensor data quality analysis and interpolation”, In Proceedings of the 9th ACM Multimedia Systems Conference, 2018, pp.294-303. https://doi.org/10.1145/3204949.3204972

[7] Xiao, Q., Chen, Y., Shen, C., Chen, Y. and Li, K. “Seeing is not believing: Camouflage attacks on image scaling algorithms”, In 28th {USENIX} Security Symposium ({USENIX} Security 19), pp.443-460, 2019. https://www.usenix.org/conference/usenixsecurity19/presentation/xiao

[8] Chakraborty, A., Alam, M., Dey, V., Chattopadhyay, A. and Mukhopadhyay, D. “Adversarial attacks and defences: A survey”, arXiv preprint, arXiv:1810.00069, 2018. https://doi.org/10.48550/arXiv.1810.00069

[9] Mo, Y. and Sinopoli, B. “False data injection attacks in control systems”, In Preprints of the 1st workshop on Secure Control Systems, pp.1-6, 2010. https://ptolemy.berkeley.edu/projects/truststc/conferences/10/CPSWeek/papers/scs1_paper_7.pdf

[10] Dean, J. and Ghemawat, S. “MapReduce: simplified data processing on large clusters”, Communications of the ACM, Vol.51, No.1, pp.107-113, 2008. https://doi.org/10.1145/1327452.1327492

[11] Apache, “Apache Hadoop”, https://hadoop.apache.org

[12] Apache, “Apache Spark”, https://spark.apache.org

[13] Tcheumadjeu, L. C. T., Luber, A., Brockfeld, E., Gurczik, G., Sohr, A. and Sauerländer, A. “Integration of mobile wireless RF sensors into a traffic information system”, Transportation research procedia, Vol.25, pp.1865-1883, 2017. https://doi.org/10.1016/j.trpro.2017.05.168

[14] Kapalova, N., Khompysh, A., Arici, M. and Algazy, K. “A block encryption algorithm based on exponentiation transform”, Cogent Engineering, Vol.7 No.1, pp.1788292, 2020. https://doi.org/10.1080/23311916.2020.1788292

[15] Ma, Y., Li, C. and Ou, B. “Cryptanalysis of an image block encryption algorithm based on chaotic maps”, Journal of Information Security and Applications, Vol.54, pp.102566, 2020. https://doi.org/10.1016/j.jisa.2020.102566

[16] Boukerche, A., Zheng, L. and Alfandi, O. “Outlier detection: Methods, models, and classification”, ACM Computing Surveys (CSUR), Vol.53, No.3, pp.1-37, 2020. https://doi.org/10.1145/3381028

[17] Yoon, C., Huh, M., Kang, S. G., Park, J. and Lee, C. “Implement smart farm with IoT technology”, In 2018 20th International Conference on Advanced Communication Technology (ICACT), pp.749-752, 2018. https://doi.org/10.23919/ICACT.2018.8323908

[18] Chatterjee, S., Kar, A. K. and Mustafa, S. Z. “Securing IoT devices in smart cities of India: from ethical and enterprise information system management perspective”, Enterprise Information Systems, Vol.15, No.4, pp.585-615, 2021. https://doi.org/10.1080/17517575.2019.1654617

[19] Anaya, E., Patel, J., Shah, P., Shah, V. and Cheng, Y. “A Performance Study on Cryptographic Algorithms for IoT Devices”, In Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy, pp.159-161. 2020. https://doi.org/10.1145/3374664.3379531

[20] Sung-sik Mun, Mi-hui Kim, “Dos Attack Defense Using SDN and Honeypot”, In Proceedings of Korea Information Processing Society Conference, pp.397-400. 2020. https://doi.org/10.3745/PKIPS.y2020m11a.397

[21] Joon-hyuk Yoon, Mi-hui Kim, “Smart parking system using mobile crowdsensing: focus on removing privacy information”, In Proceedings of the Korea Information Processing Society Conference, pp.32-35, 2018. https://doi.org/10.3745/PKIPS.y2018m05a.32

[22] Sharma, P. S., Roy, P. K., Ahmad, N., Ahuja, J. and Kumar, N., “Localisation of License Plate and Character Recognition Using Haar Cascade”, In 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), pp.971-974, 2019. https://ieeexplore.ieee.org/abstract/document/8991267

[23] Kim, B., Abuadbba, A., Gao, Y., Zheng, Y., Ahmed, M. E., Kim, H. and Nepal, S. “Decamouflage: A Framework to Detect Image-Scaling Attacks on Convolutional Neural Networks”, arXiv preprint, arXiv:2010.03735, 2020. https://doi.org/10.48550/arXiv.2010.03735

[24] Quiring, E., Klein, D., Arp, D., Johns, M. and Rieck, K. “Adversarial preprocessing: Understanding and preventing image-scaling attacks in machine learning”, In 29th {USENIX} Security Symposium ({USENIX} Security 20), pp.1363-1380, 2020. https://www.usenix.org/conference/usenixsecurity20/presentation/quiring

[25] Angelin, B. and Geethe, A., “Outlier Detection using Clustering Techniques-K-means and K-median”, In 2020 4th International Conference on Intelligent Computing and Control Systems, pp.373-378, 2020. https://doi.org/10.1109/ICICCS48265.2020.9120990

[26] Grosse, K., Manoharan, P., Papernot, N., Backes, M. and McDaniel, P., “On the (statistical) detection of adversarial examples”, arXiv preprint, arXiv: 1702.06280, 2017. https://doi.org/10.48550/arXiv.1702.06280

[27] Giuste, F. O. and Vizcarra, J. C., “CIFAR-10 Image Classification Using Feature Ensembles”, arXiv preprint, arXiv:2002.03846, 2020. https://doi.org/10.48550/arXiv.2002.03846

[28] Qureshi, A. U. H., Larijani, H., Yousefi, M., Adeel, A. and Mtetwa, N. “An adversarial approach for intrusion detection systems using Jacobian Saliency Map Attacks (JSMA)”, Algorithm. Computers, Vol.9, No.3, p. 58, 2020. https://doi.org/10.3390/computers9030058

[29] Liu, H. and Wang, X. “Image encryption using DNA complementary rule and chaotic maps”, Applied Soft Computing, Vol.12, No.5, pp.1457-1466, 2012. https://doi.org/10.1016/j.asoc.2012.01.016

[30] Sultana, S. F. and Shubhangi, D. C. “Video encryption algorithm and key management using perfect shuffle”, International Journal of Engineering Research and Applications, Vol.7, No.2, pp.1-5, 2017. http://dx.doi.org/10.9790/9622-0707030105

## ◐ 저 자 소 개 ◑

**윤 준 혁 (Junhyeok Yun)**
2020년 한경대학교 컴퓨터공학과 (공학사)
2021년 한경대학교 대학원 컴퓨터응용수학부 (공학석사)
관심분야 : 네트워크 보안, 데이터 과학, 머신 러닝, 사물 인터넷
E-mail : junhyeok2723@hknu.ac.kr

**김 미 희 (Mihui Kim)**
1997년 이화여대 전자계산학과 (공학사)
1999년 이화여대 컴퓨터학과 (공학석사)
1999년~2003년 한국전자통신연구원 연구원
2007년 이화여대 컴퓨터학과 (공학박사)
2007년~2009년 이화여대 컴퓨터학과 전임강사
2009년~2010년 노스캐롤라이나주립대학교 연구원
2011년~현재: 한경대학교 컴퓨터응용수학부 교수
관심분야: 네트워크 성능 분석 및 보안, 무선네트워크 보안, 침입대응, 크라우드센싱, 블록체인, 머신 러닝
E-mail : mhkim@hknu.ac.kr