

# 사물인터넷(IoT) 기기 분류 체계 기반 공공분야 점유율 분석

이형우\*

한신대학교 컴퓨터공학부 교수

## Analysis of Public Sector Sharing Rate based on the IoT Device Classification Methodology

Hyung-Woo Lee\*

Professor, Division of Computer Engineering, Hanshin University

**요약** 사물인터넷(IoT)은 데이터의 융합과 공유 기능을 제공하며, 다양한 첨단 기술이 함께 융복합되어 새로운 서비스를 창출하는 데 있어서 가장 근간이 되는 핵심 기술 분야이다. 하지만, 사물인터넷에 대한 분류 체계가 제각각이며 국내 공공분야를 대상으로 한정 지었을 경우 실제로 어느 정도의 점유율로 어떤 기기 등이 설치되어 운영되고 있는지에 대한 현황을 제대로 파악하기가 어려울 정도로 체계화된 자료나 연구 결과를 발견하기가 매우 어렵다. 따라서 본 연구에서는 사물인터넷 기기에 대한 분류 체계를 매출액과 출하량 및 성장률에 근거하여 현실에 맞게 관련성을 분석한 후 이를 토대로 국내 공공기관을 대상으로 실제 IoT 기기의 점유율 등을 상세 분석하였다. 도출된 분석 결과는 앞으로 IoT 기기에 대한 악성코드 공격 대응, 침해사고 분석 및 보안 취약성 강화 등 정보보호 기술 고도화를 위한 연구 분석용 IoT 기기를 선정하는 과정에서 효율적으로 활용 될 수 있을 것으로 기대된다.

**주제어** : 사물인터넷, 분류 체계, 공공분야, 국내외 점유율, IoT 기기 분류 및 현황 파악

**Abstract** The Internet of Things (IoT) provides data convergence and sharing functions, and IoT technology is the most fundamental core technology in creating new services by convergence of various cutting-edge technologies. However, there are different classification systems for the Internet of Things, and when it is limited to the domestic public sector, it is difficult to properly grasp the current status of which devices are installed and operated with what share, and systematic data or research The results are very difficult to find. Therefore, in this study, the relevance of the classification system for IoT devices was analyzed according to reality based on sales, shipments, and growth rate, and based on this, the actual share of IoT devices among domestic public institutions was analyzed in detail. The derived detailed analysis results are expected to be efficiently utilized in the process of selecting IoT devices for research and analysis to advance information protection technology such as responding to malicious code attacks on IoT devices, analyzing incidents, and strengthening security vulnerabilities.

**Key Words** : Internet of Things, classification system, public sector, domestic and overseas market share, IoT device classification and status identification

## 1. 서론

사물인터넷(IoT, Internet of Things)의 개념은 케빈 애쉬톤(Kevin Ashton)이 처음으로 사용한 이후 초기에는 RFID 태그를 활용한 근거리 통신 시스템을 의미 했지만, 지금은 유무선 네트워크로 연결된 모든 사물들의 통신 시스템으로 범주가 급격히 넓어지고 있다. 일반적으로 사물인터넷은 사물이 연결되어 정보 공유로 인해 다양한 서비스가 제공되는 것으로 정의하고 있으며 센서 계층, 네트워크 계층, 미들웨어 계층 및 응용 계층 등으로 구성된다[1-3]. 따라서 사물인터넷의 시작은 각종 센서들이 포함된 센싱 계층에서부터 시작하여 각종 센서들은 네트워크 계층에서 제공하는 각종 통신 기술로 연결되어 서로 상호작용하며, 데이터를 생성하여 미들웨어 계층에 있는 플랫폼 서버에 전달된다. 그리고 서버는 센서로부터 수집한 데이터를 취합, 분류, 분석하여 의미 있는 정보를 생성하고 이를 공유하기 위한 API를 제공한다. 이렇게 가공되어 제공되는 정보들은 우리의 삶을 더욱 편리하게 만들어주는 수많은 사물인터넷 서비스들로 이어진다. 특히 4차 산업혁명 시대를 맞이하고 있는 현재, 사물인터넷은 데이터의 융합과 공유 기능을 제공하며, 다양한 첨단 기술이 함께 융·복합되어 새로운 서비스를 창출하는 데 있어서 가장 근간이 되는 핵심 기술 분야이다.

하지만, 사물인터넷에 대한 분류 체계가 제각각이며 국내 공공분야를 대상으로 한정 지었을 경우 실제로 어느 정도의 점유율로 어떤 기기 등이 설치되어 운영되고 있는지에 대한 현황을 파악하기가 어려울 정도로 체계화된 자료나 연구 결과를 파악하기가 매우 어렵다. 따라서 본 연구에서는 사물인터넷 기기에 대한 분류 체계를 현실에 맞게 재정립하고 이를 토대로 국내 공공기관을 대상으로 실제 IoT 기기의 점유율 등을 분석하였다. 상세 분석 결과는 앞으로 IoT 기기에 대한 악성코드 공격 대응, 침해사고 분석 및 보안 취약성 강화 등 정보보호 기술 고도화를 위한 연구 분석용 IoT 기기를 선정하는 등의 과정에서 효율적으로 활용 될 수 있을 것으로 기대된다.

## 2. 기존 연구의 문제점

### 2.1 기존의 IoT 분류 체계 및 현황

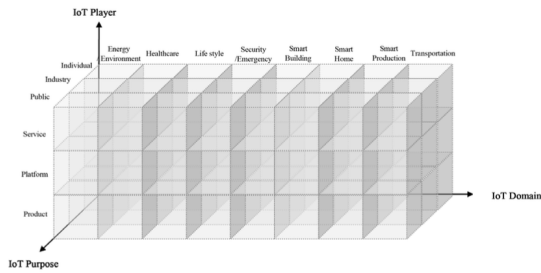
사물인터넷 서비스 관련 시장 활성화와 IoT 관련 기

술에 대한 연구개발 및 객관적인 측면에서의 통계 자료 수집, 관리 등을 위해서는 IoT 기기에 대한 분류 체계를 수정/보완하거나 현실에 맞도록 변경해야 한다. IoT 기기 분류 체계에 관련된 기존의 연구로는 2015년도에 진행된 연구가 있다. 해당 연구에서는 사물인터넷 서비스 산업을 포괄적으로 분석하기 위해 제품 및 서비스의 목적과 제공자 특성, 사업 영역 등에 대한 관점의 분류체계를 제시함으로써 사물인터넷 서비스에 대한 객관적이고 체계적인 현황 분석을 지원하고, 전략적인 사물인터넷 서비스 촉진을 도모하는 통계 기반을 제공하고자 하였다. 해당 시점에서 사물인터넷에 대한 개념, 현황 등에 대한 고찰을 통해 정부에서는 2014년도 현재 정부, 시장 조사기관, 산업계 별로 분류 목적을 중심으로 사물인터넷 기술을 활용한 서비스 제공 목적과 대상에 따라 개인, 산업, 공공 사물인터넷으로 분류하였다[3].

이때 개인 IoT는 사용자 중심의 편리하고 쾌적한 삶 제공을 목적으로 차량, 건강관리, 일상생활 등의 비즈니스 영역을 포함하였으며, 산업 IoT는 생산성/효율성 향상 및 신규 부가가치 창출 목적으로 주로 공장 및 농장의 생산물 관리에서부터 관련 기술을 활용한 전반적인 산업 분야를 포함하였다. 마지막으로 공공 IoT는 살기 좋고 안전한 사회를 실현하고자 주로 대단위의 도시 계획이나 국민 안전/보안, 환경 등의 영역에서 제공되는 서비스를 포함하도록 분류하였다.

### 2.2 기존 분류 체계의 문제점

하지만 기존의 사물인터넷 분류 체계는 실제로 급변하는 산업계 현황과는 상당 부분 차이가 있으며, 분석 기관 별로 사물인터넷을 바라보는 관점에 따라 많은 사물인터넷 산업의 현실을 제대로 반영하지 못하고 있다는 한계점이 존재하여 개선이 필요하다. 특히 정부에서 제공한 분류 체계는 서비스 제공 목적과 대상에 따라 분류하고 있어 실제 사물인터넷 기기의 적용 사례 및 점유율 등을 반영하지 못하고 있으며, 사물인터넷 기기의 공급자 측면에 대한 기술적 분류 특성을 반영하지 못하고 있어서 향후 체계적인 정책 분석과 기술적 연구개발 과정을 수행하는데 어려움이 많다는 단점이 있다. 일부 거시적 관점에서 시장 전망을 수립하는 데 있어서는 다소 도움이 될 수 있을지 모르겠으나, 산업계/학계를 중심으로 한 기술개발 및 분석 과정에서 기존의 분류 체계를 활용하기에는 많은 문제점이 있음을 부인할 수 없다.



[Fig. 1] Existing 3-D based IoT classification system

결국 사물인터넷을 서비스 대상, 공급자, 영역으로 분류하던 기존 방식을 일부 개선하여 서비스가 제공하는 가치와 목적(IoT Purpose), 응용된 산업 분야(IoT Domain) 및 해당 응용 산업에서 활동하는 서비스 공급자(IoT Player) 등으로 분류하여 다차원적인 분류 체계를 제시[2]하기도 하였으나, 실제로 특정 사물인터넷 기기를 대상으로 분류 체계에 적용해 볼 경우 구분이 모호하고 명확하게 분류되지 않는 경우가 다수이기에 이 역시도 실세계에 적용하기가 어려우며 구분이 각종 IoT 기기에 대한 분류 시 구분이 모호하다는 등 많은 문제점을 야기하고 있다. 따라서 본 연구에서는 이론적인 분류 체계가 아니라 사물인터넷 시장 동향 분석을 토대로 실제 사물인터넷 관련 산업체 매출액과 기기 생산 규모 등 현실적인 측면에서의 사물인터넷 분류 체계를 새롭게 제시하고, 국내 공공기관에서 보급/설치된 기기에 대한 점유율 현황을 분석하였다.

### 3. IoT 시장 동향 중심 분석

#### 3.1 매출액 중심 IoT 시장 동향 분석

시장조사 기관 IDC(International Data Corporation)에서 발표한 자료에 따르면 사물인터넷(IoT, Internet of Things)에 대한 지출액이 2022년 1조 달러를 돌파하고, 2023년에는 1조 1,000억 달러까지 증가한다고 전망하고 있다. 또한 2020 GIP 품목별 보고서 등에 따르면 2019년 전 세계적으로 IoT 관련 매출액은 7,260억 달러를 기록할 것으로 추산되었으며 이후 2023년까지 연평균 12.6%의 성장률을 달성할 것으로 예측되고 있다. 또한 시장조사 기관 Statista의 조사에 따르면, 2020년 스마트 홈 시장 전체 매출은 927억 달러를 기록할 것으로 예측되며 2021년에는 1,155억 달러를 달성하며 1,000억 달러를 넘는 매출을 낼 것으로 나타났다. 특히

많은 기업에서 IoT로의 전환이 신속하게 이루어짐에 따라 IoT 관련 소프트웨어 및 플랫폼 시장은 꾸준히 성장하고 있는 것으로 나타났다. 사물인터넷 전문 조사기관 IoT Analytics의 조사에 따르면, IoT 플랫폼 시장은 2018년부터 2023년까지 연평균 39%씩 성장하여 223억 달러 규모를 기록할 것으로 전망하고 있다. 특히 인터넷 보급의 확대에 따라 네트워크 보안 시장은 점점 커지고 있는 것으로 나타나고 있다. 시장조사 기관 인사이트 파트너(Insight Partners)에 따르면, IoT 보안 서비스 시장은 2017년 84억 달러를 기록하였으며 2019년에는 115억 달러를 기록한 것으로 추산하고 있다. 아울러 2017년부터 2025년까지 연평균 17.6%씩 성장하여 2025년에는 309억 달러를 기록할 것으로 전망되며, 블록체인의 상용화로 IoT 보안 시장은 더욱 커질 것으로 예상하고 있다[4-9].

#### 3.2 출하량 중심 IoT 시장 동향 분석

IDC의 전 세계 분기별 스마트 홈 단말기 추적 조사(Worldwide Quarterly Smart Home Device Tracker)에 따르면, 2020년도 비디오 엔터테인먼트 관련 스마트 홈 단말기 출하량은 3억 5,390만 대를 기록할 것으로 예상되며 이는 전체 단말기 중 41.4%를 차지할 것으로 전망하며, 2위는 홈 모니터링 및 보안 단말기로 1억 6,630만 대, 3위는 스마트 스피커가 1억 3,370만 대 판매될 것으로 추산하고 있다[8,9].

전반적인 단말기 출하량은 5년 간 연 평균 성장률 14.0%를 기록하며 크게 증가할 것으로 보이며, 따라서 2024년에는 전체 출하량이 14억 대에 달할 것으로 전망하고 있다. 또한 단말기 분야별 점유율 순위는 변동이 없을 것으로 예상하는 가운데 비디오 엔터테인먼트 단말기 출하량은 연평균 6.3%씩 성장하여 4억 5,120만 대를 기록하고, 홈 모니터링 및 보안 단말기는 3억 350만 대, 스마트 스피커는 2억 390만 대를 기록할 것으로 전망하고 있다.

IoT 애널리틱스의 조사에 따르면, 2020년 기준 시장에 출시된 IoT 플랫폼 수는 620개로 2017년 450개에 비해 약 170개 증가한 것으로 나타났다. IoT 애널리틱스는 2016년 상위 10곳의 기업이 2019년에는 58%의 시장 점유율을 기록했다고 분석하였고, IoT 시장은 인수합병을 통해 통합되는 경향을 보이지 않고 있으며, 세부 분야가 다양해 소규모 업체의 운영이 지속적으로 증가함에 따라 플랫폼 수도 증가하고 있는 것으로 나타났다.

### 3.3 성장률 중심 IoT 시장 동향 분석

IoT 애널리틱스의 조사에 따르면, 2019년 기준 IoT 플랫폼의 50%가 산업 및 제조용 IoT 플랫폼으로 나타났으며, 제조업체는 IoT 플랫폼 도입을 통해 비용을 도입하고 새로운 수익원을 창출하고자 노력하고 있음을 알 수 있다. 에너지 분야에서의 도입이 34%로 2위를 차지했으며, 모빌리티 분야는 32%, 스마트 시티 31%, 헬스케어와 생산 체인, 유통, 스마트 홈 분야가 각각 23%, 21%, 19%, 18%로 나타났다.

시장조사 기관 BIS리서치(BIS Research)에 따르면, 소비자 및 기업의 안전한 통신에 대한 요구가 증가하면서 IoT 보안 시장은 크게 성장하고 있는 것으로 나타났다. 아울러 보안 및 스토리지 목적의 클라우드 서비스 플랫폼 출시가 증가하면서 보안 솔루션에 대한 수요는 더욱 증가할 것으로 보인다. 2018년 기준 IoT 보안 서비스 중 이용 비율이 가장 높은 서비스는 전체의 37%를 차지한 컨설팅 서비스로 37%, 2위는 25.7%의 유지 및 보수 서비스, 3위는 21.9%를 기록한 관리 서비스로 나타났다. 2023년에도 보안 서비스 이용 비율 순위는 유지될 것으로 예상되며, 컨설팅 서비스는 40.6%로 이용 비율이 증가하며 유지 및 보수 서비스는 23.5%로 다소 줄어들 것으로 예측됨. 관리 서비스는 22.5%, 기타 서비스는 13.4%를 기록할 전망이다. 그러나, 위 내용과 같이 각기 분리되어 있는 시장 동향 분석 자료를 토대로 다양한 형태의 IoT 기기가 공공분야에 실제로 어느 정도의 점유율로 설치되어 있는지에 대한 정보를 확인하기가 어려우며 실제 활용 현황을 파악하기도 쉽지 않기에 매출액, 출하량 및 성장률 정보를 종합하여 분석이 가능하도록 새로운 방법론 개발이 필요하다.

## 4. IoT 기기 분류 체계 기반 공공분야

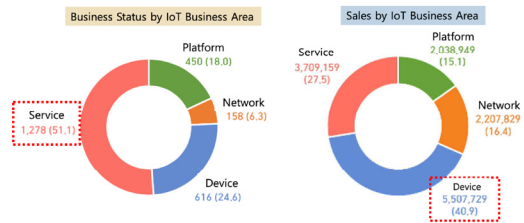
### 점유율 분석

#### 4.1 IoT 기기 공공분야 점유율 분석 방법론

현실 세계에 적용 가능한 IoT 분류 체계를 제시하기 위해서는 실제 세계에 적용/배포된 IoT 기기를 중심으로 분류 체계를 새롭게 구성해야 한다. 현재까지 정부 또는 공공기관에서 일반적으로 사용하고 있는 분류 체계를 종합적으로 분석해 보면 아래 그림과 같이 2021년 현재 IoT 분류 체계는 일반적으로 “플랫폼, 네트워크, 제품기기 및

서비스” 등과 같은 4가지 영역으로 분류하여 조사/분석 [4,5]하고 있는 것을 확인할 수 있다. 2021년 현재 국내 IoT 관련 사업체는 서비스 분야가 전체 사업체의 51.1%를 차지하고 있었으며, 매출액을 기준으로 분석하였을 경우 제품기기 분야가 전체 매출의 40.9%를 차지하고 있는 것으로 나타났다.

여기에 추가적으로 관련 자료를 조사 분석해 보면 국내 서비스 분야를 중심으로 해당 사업체 수 현황을 파악할 수 있는 자료를 확보할 수 있다. 그러나 각각의 자료 등이 조금씩 다른 관점과 분류 기준을 설정하고 있으므로 공공분야 IoT 기기에 대한 점유율 파악시에도 일정 정도의 자료 보정 과정이 필요하다.



[Fig. 2] How to analyze IoT device market share

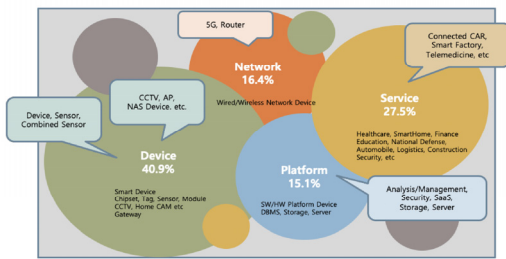
따라서 본 연구에서는 공공분야를 중심으로 IoT 분야 시장 점유율을 조사하기 위해 아래와 같이 4단계에 걸쳐서 분석 과정을 수행하였다. (1단계) IoT 분류 체계 및 현황 관련 논문과 자료 등을 조사 하였으며, (2단계) 정부, 공공기관 및 주요 관련 협회 자료를 조사하였다. 각종 보고서 및 관련 자료를 검색/취합하였고, (3단계) 실증 데이터를 수집하기 위해 조달청 등을 통해 최근 1년간 실제로 집행된 IoT 관련 제품 및 서비스 현황을 분석하였다. 이를 통해서 (4단계) 데이터 보정 과정을 수행하여 최종적으로 IoT 기기(제품)에 대한 시장 점유율 분석 결과를 도출할 수 있었다.



[Fig. 3] Stages of market share research by IoT sector

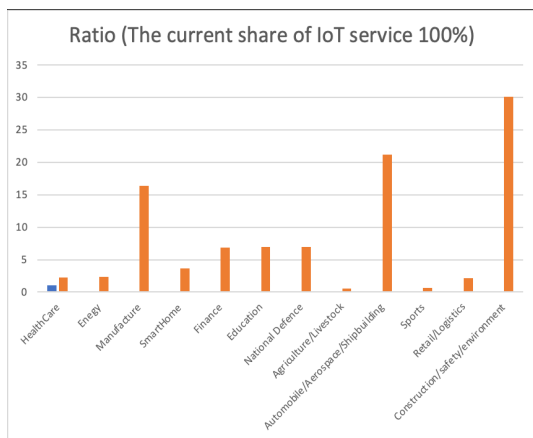
### 4.2 IoT 분류 체계 기반 점유율 분석 결과

앞서 제시한 분류 체계를 기반으로 2020년 현재 IoT 사업 분야별 매출액 기준으로 기기별 분류 및 점유율을 비교 분석하면 아래 그림과 같다. 이는 정부에서 발간한 공식 보고서 및 기타 관련 자료를 토대로 제품기기, 네트워크, 플랫폼 및 서비스의 4가지로 분류 체계를 나눌 수 있으며, 각각에 대해 통합 분석하여 IoT 전체 사업 분야별 시장 점유율을 도식화해서 표시하였다. 분석 결과를 보다 상세히 살펴보면 IoT 관련 대/중/소 분류 체계 중심으로 아래 그림과 같이 세분화 할 수 있고, 특히 IoT 제품기기 부분이 매출액 기준으로 전체의 40.9%를 차지하는 것으로 확인되었다.



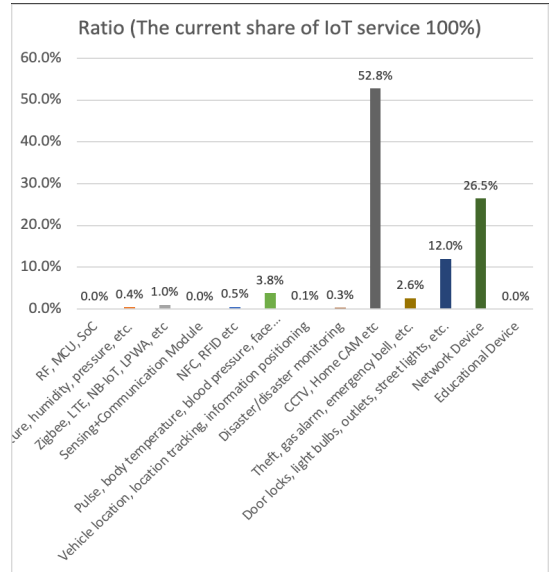
[Fig. 4] Detailed share of IoT business sector

또한 IoT 서비스 분야에 대한 현황을 파악하면 아래 그림과 같이 12개 세부 분야로 구분할 수 있으며 서비스 관련 매출액 기준으로 분석하였을 경우 자동차/교통/항공/우주/조선 분야가 21.2%를 차지하고 있으며, 건물 시설물 관리/안전/환경 분야가 30.1%로 가장 큰 비중을 차지하고 있음을 확인할 수 있었다.



[Fig. 5] Sales and Ratio Status by IoT Service Sector

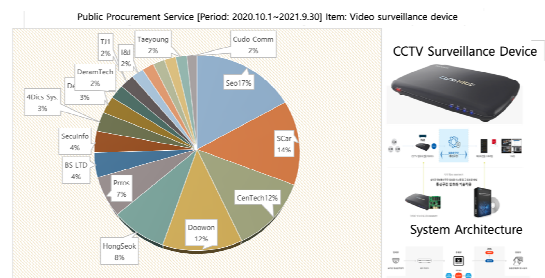
또한 아래 그림과 같이 IoT 제품기기에 대해 분야별 시장 점유율을 분석해 보았다. 특히 최근 1년간 국내에서 도입된 IoT 관련 제품기기 현황 분석 결과에 따라 아래 그림과 같이 총 6개 분야에 대한 점유율을 측정할 수 있었다.



[Fig. 6] IoT product and device market share analysis

### 4.3 IoT 기기 공공분야 점유율 상세 분석 결과

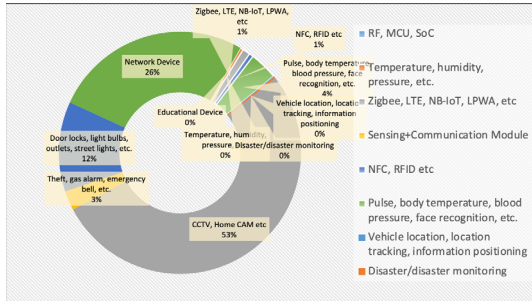
이를 구체적으로 살펴보면 다음과 같다. 2020년 10월 1일부터 2021년 9월 30일까지 1년간 조달청에서 국내에 보급/설치된 각 IoT 제품기기별 시장점유율을 조사하였다. 정부에서 제시한 제품기기 세부 분야별 해당 기기의 발주/도입 현황을 분석함으로써 실제로 국내에 설치된 IoT 기기에 대한 현황을 간접적으로 파악할 수 있었다.



[Fig. 7] IoT product device sharing rate - equipment/facility field

위 그림에서 제시된 바와 같이 ‘스마트 단말기기’ 등을 포함하여 총 6개 분야에 대한 실증 자료 및 보급 현황을 조사/분석하였고 각각에 대해 요약 정리하여 대표적인 기업체 및 제품 현황을 파악할 수 있었다. 추가로 IoT 자동원격제어 분야, 통신 모듈 분야에 대한 세부 점유율, 기업체 현황 및 각 기업체에서 보유하고 있는 제품 현황을 파악할 수 있었다. 또한 IoT 기반 생체인식, 위치추위 관련 기기에 대한 현황을 파악하였고, 경보/알람과 환경감시 분야 그리고 센서 인식, 스마트카드 및 태그 관련 분야의 제품기 현황을 파악할 수 있었다.

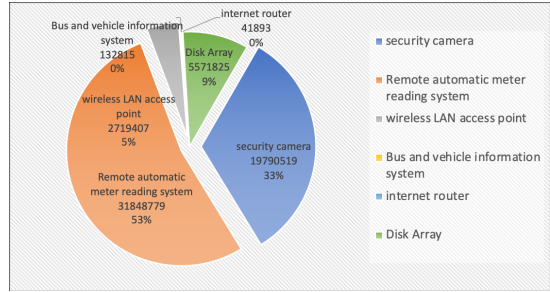
앞서 제시한 분석 결과를 토대로 IoT 제품기 내 6개 대분류 기반 13개 중분류 및 해당 제품기기에 대한 점유율 및 비중을 분석한 결과는 다음 그림과 같다. 분석 결과 최근 1년간 IoT 제품기 분야에서 CCTV, 홈캠 등과 같은 (대분류) 스마트 단말 내 (중분류) 장비/설비 부문이 53%를 차지하는 것으로 나타났다. 그리고 다음으로는 (대분류) 게이트웨이 내 (중분류) 네트워크 장비 부문이 26%를 차지하는 것으로 확인되었다.



[Fig. 8] Analysis result of public sector IoT device share

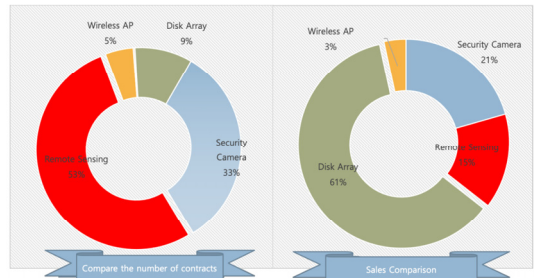
하지만 위와 같이 조달청에서 발주된 내용만으로 실제 공공분야에서 사용되고 있는 IoT 기기에 대한 실제 적용/설치 현황이라 단정하기에는 무리가 있는 것이 사실이다. 특정 기간 내를 대상으로 분석한 결과이므로 실제 공공분야에 배포/설치된 장치에 대한 점유율과 실제 현황이라 판단하기에는 이르다. 따라서 본 연구에서는 위 분석 내용을 토대로 공공분야에 많이 사용되는 IoT 기기인 무선 AP, 인터넷 공유기, 버스/차량정보 안내장치, 디스크 어레이 및 보안용 카메라, 원격자동검침 시스템 등에 대한 상대적인 비중을 비교 분석해 보았으며, 도출된 결과물과 수치 데이터를 토대로 상기에 계산한 수치 데이터에 대한 보정 작업을 수행하여 현실세계에 적용된 IoT 장비에 대한 점유율 계산의 정확도 및 타당성을 높이고

자 했다.



[Fig. 9] Market share analysis of major IoT devices in public sector

제품기별 시장점유율이 높은 중분류(보안용 카메라 및 AP 공유기)를 대상으로 세부 제품별 상세 분석 결과를 상호 비교 분석하였다. 앞서 제시한 바와 같이 IoT 제품기 내 점유율이 높은 항목 중에서 세부 내용을 분석하였으며, 이를 계약 건수와 매출액 별로 상호 비교 분석한 결과는 다음 그림과 같다. 결국 계약 건수와 매출액 간에는 정량적 수치 데이터 상에 차이가 있을 수밖에 없으므로 앞서 제시한 점유율 결과 값에 대한 보정 과정을 수행할 필요가 있다는 것을 확인 할 수 있었다.

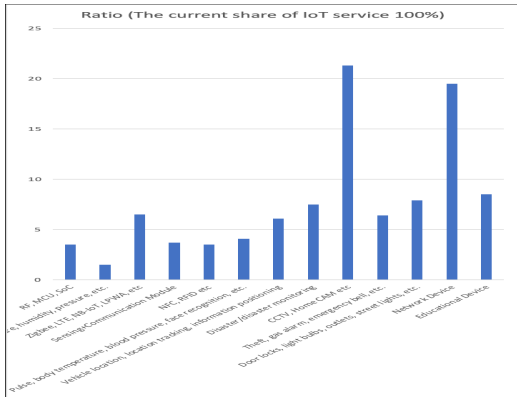


[Fig. 10] Detailed status of each IoT product device - Comparison of 4 specific detailed items

#### 4.4 IoT 기기 공공분야 점유율 보정 결과

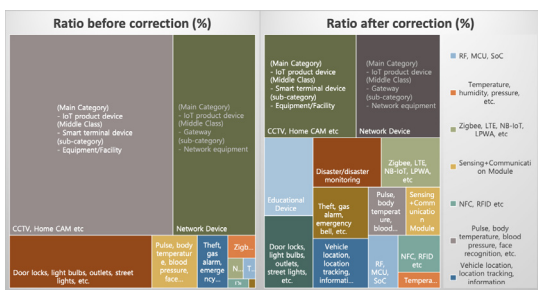
이에 아래 그림과 같이 제품기 내 시장 점유율 부분을 IoT 서비스 분야 매출액 및 비율과 연계하여 최종적인 형태의 IoT 제품기 시장 점유율을 도출하는 방법을 사용하였다. 각각의 제품기는 적용 가능한 서비스 분야가 있으므로, 각각에 대한 연계를 통해 최종적으로 제품기내에 대한 시장 점유율을 도출하는 방법을 적용하였다. 결과적으로 실측 데이터에 대한 보정 작업을 통해 보다 정확한 시장 점유율을 산출 정보를 도출할 수 있었

며 보정 후 분석 데이터에 대한 검증 결과 신뢰성을 더욱 향상시킬 수 있었다. 이에 본 연구에서는 실증 데이터를 토대로 IoT 제품기기에 대한 시장 점유율을 세부 품목별로 보정하였으며 최종적으로 도출된 결과는 아래 그림과 같다.



[Fig. 11] IoT product device market share correction result (1)

보정 후 공공분야 IoT 기기 점유율 정보를 히스토그램 형태로 제시하면 아래 그림과 같이 CCTV, 홈캠 등과 같은 (대분류) 스마트 단말 내 (중분류) 장비/설비 부문이 21.3%를 차지하는 것으로 나타났고 다음으로는 (대분류) 게이트웨이 내 (중분류) 네트워크 장비 부문이 19.5%를 차지하는 것으로 나타났다.



[Fig. 12] IoT product device market share correction result (2)

보정 과정 수행 결과에 대한 타당성을 검증해 보았다. 정부 및 연구소에서 제공하는 공공데이터 정보 및 컴퓨터/주변기기 관련 유사 분야에서의 제품기기에 대한 일반적인 시장 점유율 정보를 확인해 보니, 위와 같은 보정 과정을 통해 최종적으로 제시된 정보가 현실적으로 타당한 결과치라는 것을 확인할 수 있었으며, 보정 결과를 토

대로 IoT 제품기기에별 주요 업체 및 세부 기기 현황을 대/중/소 분류 체계에 따라 최종적으로 정리 및 구분할 수 있었다.

#### 4.5 기존 연구와의 비교 분석 및 평가

본 연구에서 제시한 IoT 기기 분류 체계는 기존 연구와 차별성을 제공한다. 우선 기존 연구와 달리 본 연구에서 제시한 분류 체계는 정부 및 연구기관에서 제시하고 있는 연간 IoT 산업 실태조사 정보를 토대로 체계적이고 지속적으로 활용 가능한 형태이다. 산업계 또는 학계에서 제시한 IoT 기기 분류 체계와 연계가 가능하며 현실 세계에도 적용 가능하다.

최근 IoT 기기에 대한 사용 및 활용도가 급격히 증가하고 있다. 따라서 앞으로 다양한 형태의 IoT 기기를 대상으로 한 대단위 DoS 공격 또는 이와 유사한 악성코드 감염을 통한 악의적인 침해사고/공격 등이 발생하였을 경우[10-14] 이를 사전에 능동적으로 대응하기 위한 기술개발[15-17]이 필요한데, 이 과정에서 연구개발 분석 대상이 되는 IoT 장비 등을 선정하는 과정에서 본 연구에서 제시한 실제 점유율 정보를 활용할 수 있을 것으로 기대된다. 예를 들어 분석 대상이 되는 특정 분류 체계에 속한 IoT 기기로부터 수집된 대단위 침해사고 흔적 데이터를 분석[10-12]하거나 IoT Botnet 공격에 능동적으로 대응할 수 있는 기술을 개발하는 과정[15,17]에서 IoT 기기 선정 시 우선순위를 부여할 수 있는 학술적 근거를 제공할 것으로 예상되며, 이를 통해서 향후 IoT 기기에 대한 보안성 강화 및 침해사고 대응을 위한 연구개발 과정에서 매우 유용하게 사용될 수 있을 것으로 기대된다.

### 5. 결론

본 논문에서는 최근 4차 산업혁명의 핵심 기술 분야에 해당하는 사물인터넷 기술과 관련하여 기존의 분류 체계의 한계점과 문제점에 대해 분석하였고, 현실 세계와의 괴리 등을 최소화 하기 위한 방법을 제시하였다. 구체적으로 기존에 정부와 산업계에서 급변하는 사물인터넷 환경 변화를 감안하지 못하고 있는 문제점을 해결하기 위해 실용적인 측면에서의 IoT 기기 분류 체계를 재정립하고, IoT 기기를 대상으로 다양한 연구 개발 과정 등을 수행하는 과정에서 공공기관 등을 중심으로 실제로 설치/운영되고 있는 IoT 기기에 대한 점유율을 분석하였으며

이를 각각 대/중/소 분류 체계로 구분하여 제시하였다. 또한 상세 분석 결과의 정확도를 향상시키기 위해서 유사 IoT 기기 품목 데이터에 대한 상호 비교 분석을 통해 점유율 데이터에 대한 보정 과정을 수행하였다. 도출된 분석 결과는 앞으로 IoT 기기에 대한 악성코드 공격 대응, 침해사고 분석 및 보안 취약성 강화 등 정보보호 기술 고도화를 위한 연구 분석용 IoT 기기를 선정하는 과정에서 효율적으로 활용 될 수 있을 것으로 기대된다.

## ACKNOWLEDGMENTS

이 논문은 한신대학교 교내 일반연구비의 지원으로 수행된 연구임

## REFERENCES

- [1] S.N.Swamy and S.R.Kota, "An Empirical Study on System Level Aspects of Internet of Things (IoT)," IEEE Access, Vol.8, pp.188082-188134, 2020.
- [2] E. Kim, K. Kim, C. Leem, C. Lee, "A Study on Development and Application of Taxonomy of Internet of Things Service," The Journal of Society for e-Business Studies, Vol.20, No.2, May 2015, pp.107-123.
- [3] Alfonso, V., Eric, G., Sree, C., and Jouni, F., Market Trends: TSPs Must Invest in the Rapidly Evolving IoT Ecosystems Now, Gartner, 2013.
- [4] Ministry of Science and ICT, NIPA, 2020 IoT Industry Survey, 2020.
- [5] NIPA, GIP Global ICT Portal, Global IoT(Internet of Things) Market, 2020
- [6] Ministry of the Interior and Safety, NIPA, Government guidelines for IoT adoption, 2019.
- [7] Gartner, Internet of Things: Unlocking True Digital Business Potential, <https://www.gartner.com/en/information-technology/insights/internet-of-things>
- [8] IDC, Worldwide Internet of Things Forecast, 2020-2024. <https://www.idc.com/getdoc.jsp?containerId=US45861420>
- [9] IDC, IDC: Global IoT Market Report, 2021. <https://medium.com/tech-in-china/idc-global-iot-market-report-5cb5be303e51>
- [10] H.Lee, "Intrusion Artifact Acquisition Method based on IoT Botnet Malware," Journal of The Korea Internet of Things Society, Vol.7, No.3, pp.1-8, 2021.

- [11] S.Ramesh and M.Govindarasu, "An Efficient Framework for Privacy-Preserving Computations on Encrypted IoT Data," in IEEE Internet of Things Journal, Vol.7, No.9, pp.8700-8708, 2020.
- [12] H.Seo, J.K.Park, "The prevent method of data loss due to differences in bit rate between heterogeneous IoT devices," Journal of the Korea Institute of Information and Communication Engineering, Vol.23, No.7, pp.829~836, 2019.
- [13] Maria Stoyanova, Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, Vol.22, No.2, pp.1191-1221, SECOND QUARTER 2020.
- [14] Ibrar Yaqoob, Ibrahim Abaker Targio Hashem, Arif Ahmed, S. M. Ahsan Kazmia, Choong Seon Hong, "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges," Future Generation Computer Systems · September 2018.
- [15] M. Wazzan, D. Algazzawi, O. Bamasaq, A. Albeshri, L. Cheng, "Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future Research," Applied Science Vol.11, 5713, 2021.
- [16] A. Alenezi, H. Atlam, R. Alsagri, M. Allassafi, and G. Wills, "IoT Forensics: A State-of-the-Art Review, Challenges and Future Directions," Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS 2019), pages 106-115.
- [17] Weam Saadi Hamza, Hassan Muayad Ibrahim, Methaq Abdullah Shyaa, Jane J. Stephan, "IoT Botnet Detection: Challenges and Issues," Test Engineering & Management, Vol.83, pp.15092-15097, 2020.

이 형 우(Hyung-Woo Lee)

[중심회원]



- 1994년 2월 : 고려대학교 컴퓨터학과 (학사)
- 1996년 2월 : 고려대학교 컴퓨터학과 (석사)
- 1999년 2월 : 고려대학교 컴퓨터학과 (박사)
- 1999년 3월 ~ 2003년 2월 : 백석대학교 정보통신학부 교수
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터공학부 교수

<관심분야>

사물인터넷, 정보보호, 모바일 보안 및 디지털 포렌식