IoT 특론

2차시

AI첨단기술학과

이의혁

1. 사물 인터넷 개요

1-4. 사물 인터넷 관련 기술 개요

사물 인터넷 특징 및 이슈

4차 산업혁명을 견인하는 다이버전스 기술 사물 인터넷

사물 인터넷의 특징

- 기술적인 특징
  - IoT 기기들의 자원 제약성
    - 제한된 프로세서 성능
    - 제한된 메모리 용량
    - 제한된 배터리 용량
    - 제한된 네트워크 성능

  → **제한된 자원 하에서도 적용될 수 있는 경량화된 기술이 필요**

사물 인터넷의 특징

- 기술적인 특징
  - IoT 환경의 높은 이동성과 동적인 네트워크 토폴로지 (Topology)
    - 다양한 IoT 기기는 고정되어 있는 것이 아니라 이동할 수 있어 접속된 네트워크가 변경될 수 있음, 즉 네트워크의 형태가 계속해서 바뀔 수 있음
    - IoT 기기의 제한된 연산, 네트워크 성능으로 네트워크 연결이 불안정할 수 있고 이로 인해 빈번한 재연결이 수행될 수 있음

  → 사물 인터넷은 유연성과 확장성 필요

사물 인터넷의 특징

- 시장의 특징
  - 사물 인터넷은 완전히 새로운 카테고리의 상품이라기보다는 **기존 상품의 가치를 높이**는 경우가 많음
    - 냉장고 → 스마트 냉장고
    - 자동차 → 스마트 카, 커넥티드 카
  - 기존 상품의 가치를 높이는 수단은 **데이터의 생성, 전송, 분석 및 활용**
    - 기본적으로 상태 정보 단순 제공, 사용자의 원격 제어
    - 사용자의 행동, 제품 이용 행태 데이터를 수집하고 분석하여 선제적인 서비스 제공
    - 여러 다양한 IoT 제품이 서로 연계되어 서비스 제공

사물 인터넷의 특징

- 시장의 특징
  - 하드웨어, 소프트웨어, 네트워크, 보안 등 **여러 기술적 요소를 결합한 시스템 상품** (System Goods)
  - 사물 인터넷 솔루션을 제공하는 데 필요한 요소를 **제품 제조사, 통신사업자, IT기업 등 다양한 기업**이 나누어 보유
    - 필요한 모든 기술을 보유하고 있는 기업은 거의 없음
    - 기업간의 제휴 필수

사물 인터넷의 특징

- 시장의 특징
  - 플랫폼 주도권 경쟁 치열
    - 시장에 지배적인 플랫폼이 나타나면 그 이후에는 새로운 기업이 진입하기 어려워짐
    - 여러 기업들이 사물 인터넷 환경의 하드웨어, 네트워크, 소프트웨어 등 다양한 계층에서 플랫폼을 선점하여 사물 인터넷 생태계를 주도하기 위해 노력

개인용 컴퓨터 시대	윈텔(Windows + Intel)
스마트폰 시대	애플 iOS, 구글 Android
사물 인터넷 시대	??

사물 인터넷의 이슈

- 보안 및 사생활의 침해 위협
  - 제조공장, 전력망 등 사회 인프라, 자동차, 의료기기, 가전제품 등 다양한 사물이나 IoT 서비스에 대한 악의적 보안 공격
  - 개인정보 유출, 사생활 침해, 신체/생명의 위험
  - IoT 환경에서는 기존 인터넷의 보안 문제보다 훨씬 더 심각한 문제를 일으킬 수 있음
    - 사용되는 디바이스가 다양해지고 그 수가 매우 많아짐
    - 물리적으로 동작하는 다양한 액추에이터도 많아짐

사물 인터넷의 이슈

- 보안 및 사생활의 침해 위협
  - 제조공장, 전력망 등 사회 인프라, 자동차, 의료기기, 가전제품 등 다양한 사물이나 IoT 서비스에 대한 악의적 보안 공격
  - 개인정보 유출, 사생활 침해, 신체/생명의 위험
  - IoT 환경에서는 기존 인터넷의 보안 문제보다 훨씬 더 심각한 문제를 일으킬 수 있음
    - 사용되는 디바이스가 다양해지고 그 수가 매우 많아짐
    - 물리적으로 동작하는 다양한 액추에이터도 많아짐

사물 인터넷의 이슈 (보안, 사생활 침해 위협 사례)

분야	개요
사생활 침해	(CCTV) 보안카메라 업체인 트렌드넷(Trendnet)의 유아용 CCTV에서 자체 소프트웨어 결함으로 인해 인터넷 주소만 알면 누구라도 쉽게 영상과 음성을 도·감청할 수 있게 됨. 실제 인터넷상에서 약 700개의 CCTV에서 촬영 중인 실시간 영상링크가 유포되었음.
	(스마트TV) 2013년, 미국 라스베가스에서 스마트TV에 탑재된 카메라를 해킹해 사생활 영상을 유출하는 시연이 열려, 인터넷에 연결된 가전제품의 보안 취약성이 노출됨.
	(구글 안경) 세계적인 정보보안 학회인 블랙햇(Black Hat) 2014에서 한 보안전문가는 구글 안경이 시간과 장소에 구애 받지 않고 개인정보를 수집할 수 있으며, 은행계좌의 비밀번호 등 금융정보까지 훔칠 수 있다는 것을 입증함.
스마트 홈	(가전) 2014년, 미국 보안업체 프루프포인트(Proofpoint)는 스마트TV와 냉장고, 홈 네트워크 라우터를 해킹하여 '좀비 가전'을 만든 뒤 악성 이메일을 75만 건 발송한 사이버공격 사례를 공개함
	(로봇청소기) 2014년, 서울 'ISEC 2014'에서 블랙펄 시큐리티(Blackperl Security)는 로봇청소기의 앱 인증방식이나 취약점과 로봇청소기에 연결되는 접근점(Access Point)의 보안 설정상의 취약점 등을 이용한 해킹으로 로봇청소기에 탑재된 카메라로 실시간 모니터링이 가능하다는 것을 시연함.
	(온도조절기) 블랙햇 2014에서 플로리다 대학 연구진은 해커가 가정의 온도조절기를 원격으로 제어할 수 있음을 보임.
	(가전기기) 중국에서 수입된 다리미, 주전자 등 가전기기 30여 개에서 스파이 마이크로칩이 발견됨. 이들 칩은 보안설정이 되지 않은 무선네트워크에 접속해 악성코드와 스팸을 유포하고 외국에 있는 서버로 데이터 전송이 가능

사물 인터넷의 이슈 (보안, 사생활 침해 위협 사례)

분야	개요
네트워크	(차량 네트워크) 스페인 출신 해커 팀이 차량네트워크에 침투할 수 있는 조립 회로보드(20달러)를 공개하였음. 이를 통해 자동차업체가 컴퓨터시스템 검사를 위해 설치한 차량 내부 네트워크 (Controller Area Network, CAN)에 접근하여 브레이크 조작, 방향 설정, 경보장치 해제 등이 가능함.
	(홈 네트워크) 보안업체 카스퍼스키(Kaspersky)는 가정용 디지털 가입자 회선(Digital Subscriber Line, DSL) 라우터를 통해 홈 네트워크에 침입하여 14가지의 취약점을 찾아내는 데 20분도 걸리지 않았다고 보고함.
	(공유기) 2014년, 보안컨설팅 업체인 팀심루(Team Cymru)는 해커들이 디링크(D-Link), 텐다(Tenda), 마이크로넷(Micronet), 티피링크(TP-Link) 등이 제조한 약 30만 개의 공유기를 해킹했다고 경고함.
제어 시스템	(산업용 제어시스템) 미국 국토안보부는, 인터넷에 연결되어 있지만 방화벽, 인증접속제어 등으로 보호되지 않은 기계장비를 운용하는 산업용 제어시스템에 대한 사이버 공격을 경고함
	(냉·난방시스템 통제) KISA는 냉·난방시스템 통제에 쓰이는 셋톱 박스가 기업을 대상으로 한 디도스(DDoS) 공격에 악용된 사례가 국내에서 발견되었음을 발표함.
의료	(인슐린펌프) 2012년, 블랙햇 보안학회에서 해커가 800미터 밖에서 인슐린 펌프를 조작하여 치명적인 복용량을 주입할 수 있음을 증명함.

사물 인터넷의 이슈

- 최신 연구

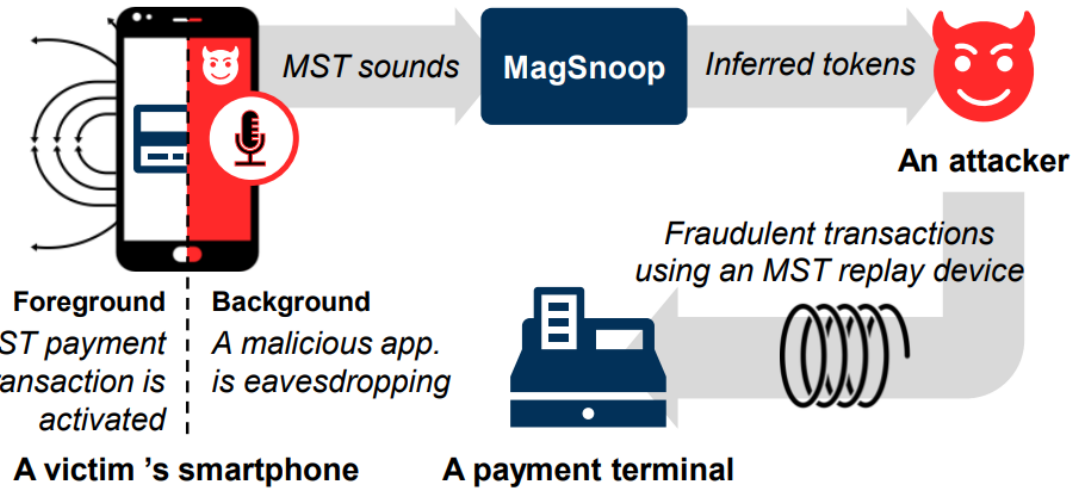


Figure 1: Attack flow for MST payment services.

MagSnoop: Listening to Sounds Induced by Magnetic Field Fluctuations to Infer Mobile Payment Tokens

Myeongwon Choi
Chung-Ang University
South Korea
auspic7@cau.ac.kr

Sangeun Oh
Ajou University
South Korea
sangeunoh@ajou.ac.kr

Insu Kim, Hyosu Kim*
Chung-Ang University
South Korea
{dlstn1121,hskimhello}@cau.ac.kr

ABSTRACT

Samsung Pay, one of the most representative mobile payment services, allows mobile users to make payment transactions almost anywhere using only their smartphone. This is thanks to MST (Magnetic Secure Transmission) that supports communication between smartphones and payment terminals for magnetic cards by transferring payment tokens via magnetic waves. Several attack methods have targeted this new technology by eavesdropping on magnetic fields to intercept the tokens, but with the use of dedicated hardware. This paper raises new security concerns for mobile payment users in a different, yet more effective way; by introducing MagSnoop, a novel framework that infers payment tokens from listening to MST sounds generated during the activation of MST payment transactions. More specifically, we first explore the principle, causing the generation of MST sounds, and the fundamental characteristics of these sounds. We then use these observations to infer payment tokens with a high degree of accuracy, robustness, applicability, and data efficiency. Our experiments with a prototype of MagSnoop demonstrate that it can support high accuracy in token inference (more than 77.8%). In addition, MagSnoop can maintain a reasonable level of accuracy regardless of the payment environments (e.g., 69.2% with a noise level of 50 dBA) and even in the real world (an inference success rate of 68.0% with 15 real-world users).

CCS CONCEPTS

• **Security and privacy** → **Mobile and wireless security**; **Side-channel analysis and countermeasures**; • **Human-centered computing** → **Smartphones**.

KEYWORDS

Mobile Security; Mobile Payment Token Inference; Acoustic Side Channel Attacks; Magnetic Secure Transmission

ACM Reference Format:
Myeongwon Choi, Sangeun Oh, and Insu Kim, Hyosu Kim. 2022. MagSnoop: Listening to Sounds Induced by Magnetic Field Fluctuations to Infer Mobile Payment Tokens. In *The 20th Annual International Conference on Mobile Systems, Applications and Services (MobiSys '22), June 25–July 1, 2022, Portland, OR, USA.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3498361.3538937

*A corresponding author

MobiSys '22, June 25–July 1, 2022, Portland, OR, USA

ACM ISBN 978-1-4503-9185-6/22/06…$15.00
https://doi.org/10.1145/3498361.3538937

1 INTRODUCTION

The widespread prevalence of smartphones has profoundly changed the commercial activities of mobile users. In particular, they tend to increasingly use mobile payment services via their smartphones instead of cash or credit cards when purchasing goods. In line with this trend, various mobile payment services, such as Samsung Pay [30], Apple Pay [4], and Google Pay [16], have been commercialized, becoming primary applications for smartphones.

These wallet-less payments are basically achieved through near-field wireless communications, including Magnetic Secure Transmission (MST) and Near-Field Communication (NFC). Particularly, MST [36] used by Samsung Pay allows a smartphone to communicate with a traditional payment terminal for magnetic cards even without any hardware or software modification[1]. To this end, MST mimics a magnetic card swipe by flowing currents through a built-in conductor coil, called an MST coil, and finally by emitting a magnetic wave around the coil. The payment terminal then processes the requested payment transaction by reading the emitted magnetic wave. Note that the magnetic wave is repeatedly generated until the completion of the payment.

MST with these convenient features benefits mobile payment users but also opens new opportunities for adversaries because it carries sensitive data (i.e., payment tokens). For example, some studies [6, 8, 9] showed that it is possible to intercept an MST payment token by eavesdropping on magnetic waves. The leaked token then can be used for a fraudulent transaction. However, to extract the token accurately, the proposed methods require an attacker to be located close to a victim user and use a high-performance magnetic receiver (e.g., a pizza-box-sized coil) that is too large to carry. These points make it difficult to apply the magnetic-based attack methods in the real world.

In this paper, we explore the feasibility of introducing new and more serious security threats that infer MST payment tokens by listening to sounds. A specific pattern of sounds (called MST sounds) exposing payment tokens are generated when MST payment services are running. This is because smartphones have several hardware components made of ferromagnetic materials, such as a magnetic shield used to improve wireless charging efficiency. When a magnetic wave from an MST coil is applied to such materials, they are deformed due to the movement of their magnetic domains, i.e., the magnetostriction effect. The deformation then causes the vibration of the materials and eventually produces an MST sound. Hence, once an

[1]MST support may vary by country [31]. South Korea is a major country that uses MST.

사물 인터넷의 이슈

- 보안 및 사생활의 침해 위협
  - 상호 연결되는 사물이나 기기들 간의 보안은 센서를 포함한 하드웨어, 서비스, 응용 프로그램 모든 수준에서 고려되어야 함
  - 보안을 위한 기술적 문제 해결책과 법·제도적 측면의 대비책 등 종합적인 방안 마련이 전제되어야 함

사물 인터넷의 이슈

- 상호운용성을 위한 글로벌 표준 확보
  - 사물들이 연결되어 서로 제약 없이 통신할 수 있는 표준 정립이 중요

표준 단체	개요
키비콘 (Qivicon)	2011년, 독일 통신사 도이치텔레콤(Deutsche Telekom; DT)의 주도로 설립. 엔베베(EnBW), 미에레(Miele), 삼성전자, 필립스(Phillips) 등 통신, 에너지, 가전 분야의 약 30개 기업이 가입
oneM2M	2012년, 글로벌 사물 인터넷 서비스 플랫폼 표준 개발을 위해 유럽통신표준협회 (ETSI), 미국 통신 산업 협회(TIA), 미국 통신정보표준협회(ATIS) 등 7개의 세계 주요 표준화 단체가 공동으로 oneM2M을 설립
올씬 얼라이언스 (AllSeen Alliance)	2013년, 퀄컴(Qualcomm)과 리눅스 파운데이션(Linux Foundation), 시스코, 마이크로소프트, LG전자 등이 참가하여 결성한 표준화 단체
산업 인터넷 컨소시엄(IIC)	2014년, 인텔과 시스코, AT&T, GE, IBM은 산업용 사물 인터넷에 목적을 둔 표준을 개발하기 위해 결성, 이후 마이크로소프트가 합류
IEEE P2413	2014년, IEEE는 사물 인터넷 아키텍쳐 구축을 통해 다양한 산업과 기술 영역으로 확장을 목적으로 IEEE P2413 프로젝트를 개시
쓰레드그룹 (Thread Group)	2014년, 구글(Nest Labs) 주도로 설립된 사물 인터넷 프로토콜 컨소시엄으로 삼성전자, 암(ARM), 프리스케일(Freescale), 실리콘 랩(Silicon Labs) 등이 참여
오픈 인터커넥트 컨소시엄(OIC)	2014년, 인텔, 아트멜(Atmel), 델(Dell), 삼성전자 등은 퀄컴 주도의 올씬얼라이언스에 대항하고, 사물 인터넷 기기의 연결성 확보를 목표로 설립

사물 인터넷의 이슈

- 스마트 센서 원천기술 확보
  - 스마트 센서
    - 미세 전자 기계 시스템(Micro-Electro-Mechanical Systems, MEMS), 반도체 단일 칩 시스템(System on Chip, SoC), 내장형 소프트웨어 기술의 발전으로 널리 활용
    - 데이터 처리 능력, 판단 기능, 메모리 및 통신 모듈 등을 갖추고 있어 사물 인터넷 기기의 핵심 요소
  - 국내의 경우, 센서 칩의 90% 이상을 수입해 모듈화하는 수준
- 기타 이슈
  - 배터리 수명 연장 기술이나 저전력 기술
  - 초기 구축비용이나 운영비용 최소화
  - 사물 인터넷 서비스 제공을 위한 안정적인 커버리지 확보
  - 동시 접속 기기 처리 수
    - 2025년 장거리 통신 접속 기기가 약 70억개까지 증가할 것으로 추정됨

사물 인터넷의 주요 기술

4차 산업혁명을 견인하는 다이버전스 기술 사물 인터넷

사물 인터넷 관련 기술

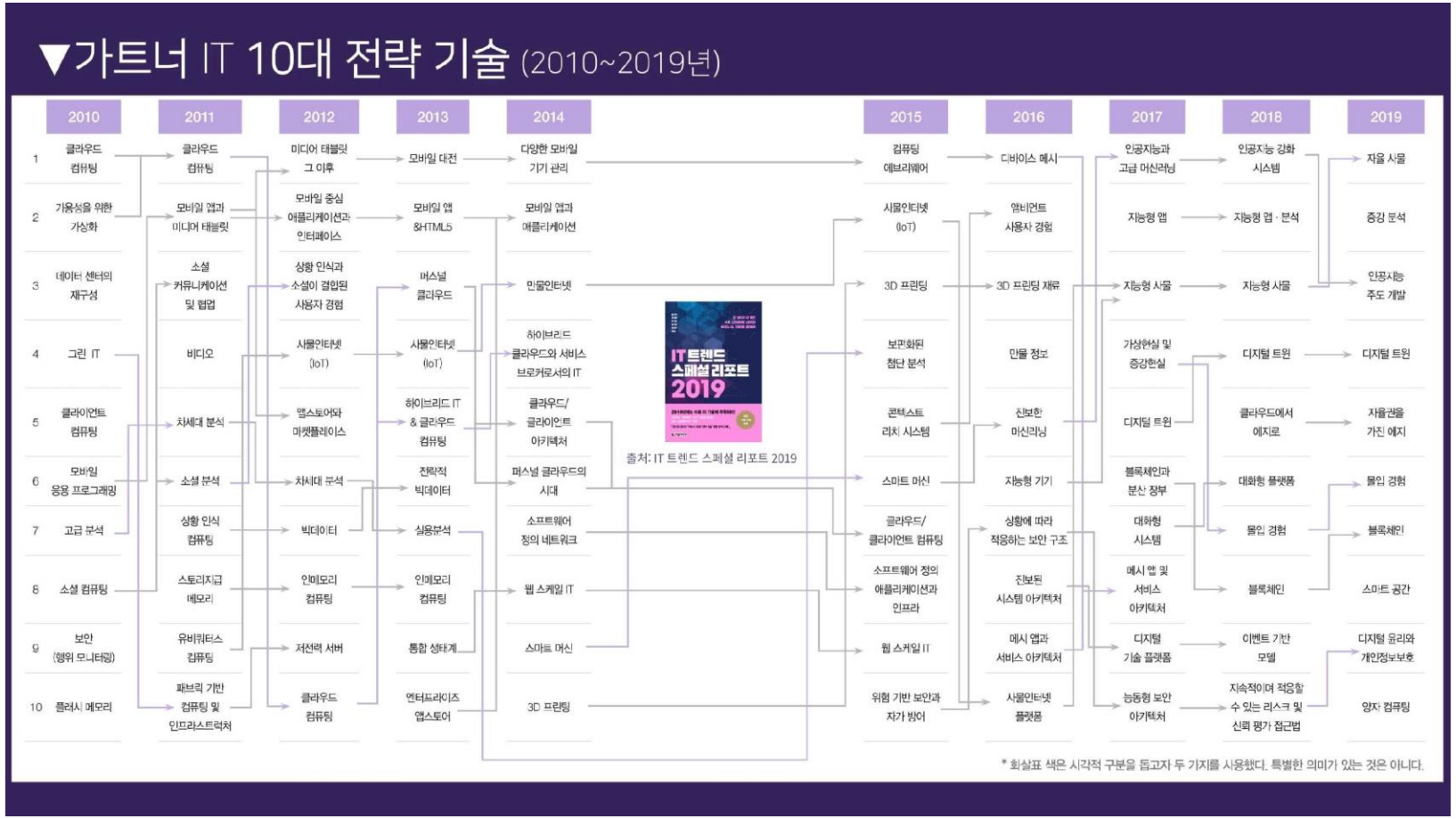
- 센싱 기술
  - 사물과 주위 환경에서 정보를 얻기 위한 기술
  - 센서
    - 대상으로부터 물리, 화학, 생물학적 요소를 측정하여 사용자나 시스템에서 사용할 수 있는 데이터를 제공
    - 온도, 습도, 열, 가스, 조도, 위치, 모션 센서 등 다양한 기능의 센서가 활용
- 유·무선 통신 및 네트워크 인프라 기술
  - 인간-사물-서비스를 연결하는 데 필요
    - 와이파이(Wireless-Fidelity, Wi-Fi), 이동통신(4G/LTE, 5G)
    - 블루투스(Bluetooth), 지그비(ZigBee), RFID (Radio Frequency IDentification), 근거리 무선 통신(Near Field Communication, NFC)
- 서비스 및 인터페이스 기술
  - 사람·사물·서비스를 통해 특정 기능을 수행하는 응용 서비스와 연동하는 역할
  - 단순한 네트워크 인터페이스 개념이라기 보다는 사물 인터넷 망을 통해 데이터 저장, 처리 및 변환, 검색 등 다양한 서비스를 제공

사물 인터넷 관련 기술

- 빅 데이터 기술
  - 수많은 센서로부터 수집된 방대한 양의 데이터에 대한 분석 및 가공의 필요성이 증가
- 클라우드 컴퓨팅(Cloud Computing) 기술
  - 방대한 센싱 데이터를 다양한 분석 방법으로 패턴, 연관관계 등을 추출함으로써 의미 있는 정보로 가공해내어 다양한 서비스에서 활용하기 위해 필요한 컴퓨팅 기술
  - 컴퓨팅 자원을 필요할 때 필요한 만큼 효율적으로 사용할 수 있도록 지원하는 기술
- 인공 지능/딥 러닝(Deep Learning) 기술
  - 수많은 데이터를 학습하고 해당 데이터가 의미하는 바를 스스로 해독하여 목적에 맞는 최적의 답안을 찾아내는 기술의 필요성 증가
  - 고객 개인의 취향과 수요(needs)를 예측하여 가장 적합한 맞춤 서비스 제공, 고객이 원하는 정보 검색, 고객 상황에 맞는 기기 제어(조명, 온도 등), 고객에게 필요한 상품 주문 등이 가능

가트너(Gartner)의 사물 인터넷 핵심 기술

- 가트너: 미국의 저명한 시장 조사 기관으로 매년 주목해야할 10대 전략에 대해 발표하고 있음

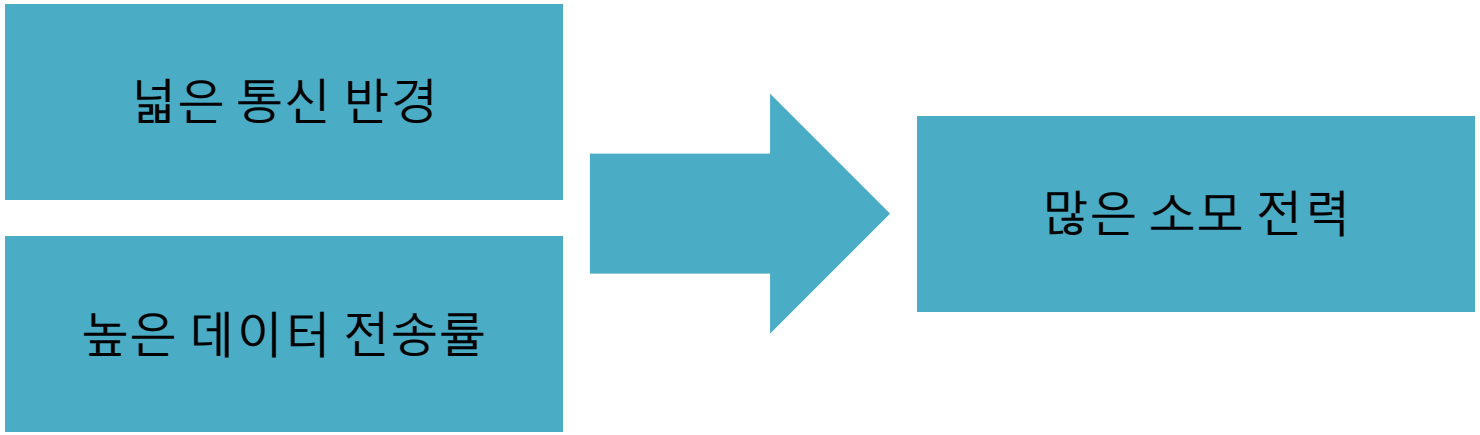


가트너(Gartner)의 사물 인터넷 핵심 기술

- 저전력 네트워킹 기술
- 센싱 데이터 경로 최적화 및 관리 기술
- 저전력 내장형 운영체제 기술
- 새로운 전력 공급 및 저장 기술
- 저가격, 저전력 프로세서 기술

가트너(Gartner)의 사물 인터넷 핵심 기술

- 저전력 네트워킹 기술
  - 사물의 통신 방식에 따라 단말에서 지원되는 통신 반경, 데이터 전송률, 단말 가격, 소모 전력이 많이 달라짐
  - 데이터 전송률은 낮지만 저전력 특성의 지그비, 블루투스 LE, 지-웨이브(Z-Wave) 등의 통신 방식 사용 가능



가트너(Gartner)의 사물 인터넷 핵심 기술

- 센싱 데이터 경로 최적화 및 관리 기술
  - 사물 인터넷 서비스는 수많은 단말로 구성되고, 단말 간 데이터 전송이 빈번하게 발생할 수 있어 단말의 전력 소모가 많아지게 됨
  - 이러한 환경에서 저전력 네트워킹 수행을 위해 데이터의 경로 설정 및 흐름 제어 등의 데이터 전송 효율화 기술이 중요
    - 중복된 데이터, 불필요한 데이터 전송 방지
    - 특정 단말로 데이터 전송 및 중계 집중 방지

가트너(Gartner)의 사물 인터넷 핵심 기술

- 저전력 내장형 운영체제 기술
  - 사물 단말에 사용되는 저가격·저전력 하드웨어 모듈은 제한적 메모리와 컴퓨팅 파워만 제공
  - 데이터 수집 및 데이터 전송을 효율적으로 관리해 주는 경량 운영체제 필요
  - TinyOS, Contiki, NanoQplus 등

가트너(Gartner)의 사물 인터넷 핵심 기술

- 새로운 전력 공급 및 저장 기술
  - 다양한 형태의 사물 인터넷 단말, 웨어러블 기기 등을 지원하기 위한 플렉서블 (flexible) 전력 공급 장치 기술
  - 작은 사이즈로도 장기간 사용할 수 있는 고밀도 배터리 기술
  - 반영구적인 사용을 위해 전력을 자가 생산하거나 무선 충전하는 기술

Flexible battery example

가트너(Gartner)의 사물 인터넷 핵심 기술

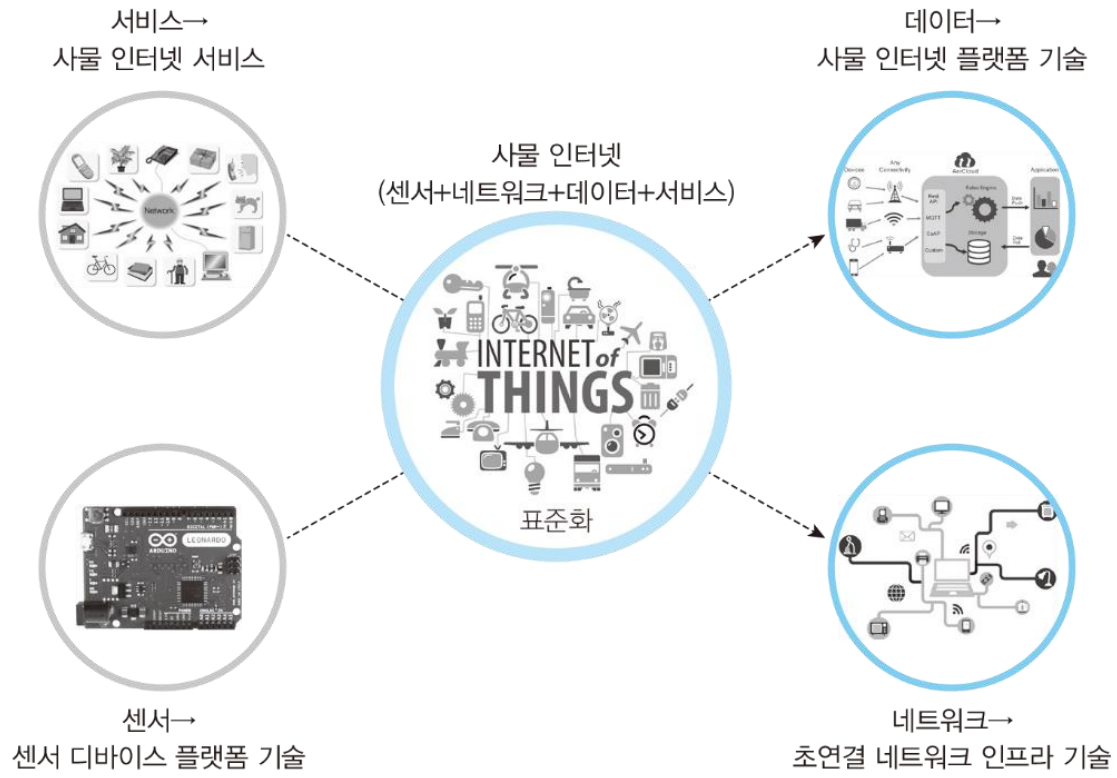
- 저가격, 저전력 프로세서 기술
  - IoT 제품의 가격이 낮아야 소비자의 구매 의향을 높일 수 있고 이를 통해 IoT 디바이스 및 서비스가 확산될 수 있음
  - IoT 디바이스가 많이 보급되어야 그만큼 이를 활용하는 애플리케이션이 활발히 개발될 수 있고 이를 통해 사용자들이 효용성을 느낄 수 있어 IoT 디바이스 보급에 선순환 구조가 만들어짐

닉 웨인라이트(Nick Wainwright)의 사물 인터넷 핵심 기술

- HP 연구소의 닉 웨인라이트는 사물 인터넷을 센서, 네트워크, 데이터, 서비스의 융합으로 정의
  - 센서를 통해 사물이나 주변 환경의 데이터를 수집하고,
  - 네트워크를 통해 이 데이터를 다른 사물이나 사람에게 전송하며,
  - 전송된 데이터를 이용하여 서비스가 가능해지는 것

닉 웨인라이트(Nick Wainwright)의 사물 인터넷 핵심 기술

- 사물 인터넷을 센서, 네트워크, 데이터, 서비스의 융합으로 정의
  - 센서 디바이스 플랫폼, 네트워크 인프라, 사물 인터넷 통합 플랫폼, 사물 인터넷 서비스 기술



사물 인터넷 기반 기술 도메인

- 디바이스
  - 센서
  - 디바이스 플랫폼
- 네트워크
- 서비스 플랫폼
- 애플리케이션/서비스
- 보안 및 프라이버시 보호

사물 인터넷 기반 기술 도메인

- IoT 디바이스
  - 센서를 통해 주변 환경과 사물의 상태를 감지
  - 사물들과 서로 통신하고 상호 연동을 하며 필요한 액션을 수행
  - 여러 애플리케이션 도메인과 관련하여 각종 사물, 환경, 개체들의 데이터 생성
- 액세스/코어 네트워크
  - 생성된 데이터들이 게이트웨이를 통해서 액세스 및 코어 네트워크로 전송
  - 백엔드 서비스 플랫폼으로 전달
- 서비스 플랫폼
  - 네트워크를 통해 흘러 들어온 데이터를 각 애플리케이션 도메인에 맞게 가공하고 필요한 지능형 서비스를 제공할 수 있도록 지원
  - 서비스 운영을 위해 필요한, 과금이나 네트워크 관리, 서비스 품질 관리 등의 시스템 요소들이 플랫폼 단에 포함

사물 인터넷 기반 기술 도메인

- 애플리케이션/서비스
  - 스마트 홈, 스마트 헬스 케어, 스마트 팩토리 등 각 서비스 도메인에 따라 최적화된 서비스를 제공
  - 빅 데이터 분석을 통한 맞춤형 정보 제공, 지능형 의사 결정, 최적화된 사물/환경 제어 등이 이루어짐
- 보안 및 프라이버시 보호
  - IoT 디바이스에서 애플리케이션까지 전체 도메인에 걸쳐서 보안 및 프라이버시 보호 기술이 결합되어 신뢰성 있고 안전하게 서비스가 제공되고 이용될 수 있도록 지원되어야 함

사물 인터넷 요소 기술 (예)

- IoT 디바이스
  - 스마트 센서 기술
  - 초소형/저전력/고성능 센싱 기술
  - IoT 디바이스 하드웨어 플랫폼(초소형/저전력 하드웨어 칩셋 기술, 저전력 통신 기술 등)
  - IoT 디바이스 운영체제 및 미들웨어(디바이스 자원 관리 기술, 개발 지원 도구, 데이터 처리 기술, 상황 인지 기술 등)
- IoT 네트워크
  - 네트워크 게이트웨이 기술 (데이터 수집 및 처리, 디바이스 관리 등)
  - (근거리/원거리) 저전력 무선 통신 기술
  - 액세스/코어 네트워크 기술

사물 인터넷 요소 기술 (예)

- IoT 서비스 플랫폼
  - 지능형 데이터 분석 및 가시화(기계 학습, 데이터 마이닝 기술 등)
  - 디바이스 관리/클라우드 자원 관리 기술
  - 애플리케이션 개발 지원 도구(API, SDK)
  - 서비스 운영 및 관리(과금, Service Level Agreement, 고가용성/고신뢰성 서비스 기술 등)
- IoT 애플리케이션/서비스
  - 지능형 서비스
  - 사용자 친화적 인터페이스(멀티 모달 인터페이스, 감성 인터페이스 기술 등)

IoT 디바이스 – 센서 기술

센서 기술

- 센서(Sensor)
  - 이미지, 동작, 소리, 빛, 열, 가스, 온도, 습도 등 주변의 물리·화학·생물학적 정보를 감지하여 전기적 신호로 변환하는 장치
  - 데이터를 수집하고 이를 처리하여 전달하는 기능을 수행
  - 예)
    - 자동차를 타고 가다가 앞차가 급정거를 하는 경우, 충돌 방지 레이더나 충돌 방지 센서, 카메라 등이 이를 감지

센서 기술

- 사물 인터넷 서비스 부문별 센서 응용 예

분야	응용 예	구체적 응용	활용 센서
스마트시티	**구조적 건전성** **스마트조명**	-빌딩, 다리 등 구조물 상태 모니터링 -날씨 적응형 가로등 조명	균열 검출, 균열 전파, 가속도계, 선형변위 센서 광 센서(LDR), 구동기 릴레이
스마트환경	**산불 조사** **공기 오염**	-연소가스 및 화재예방 조건 모니터링 -공장 CO_2 배출, 차량 오염가스 배출 등 제어	CO, CO_2, 온도, 습도 센서 NO_2, SH_2, CO, CO_2, 탄화수소, 메탄 검출 센서
스마트계측	**스마트그리드** **저장 탱크 관리**	-에너지 소비 모니터링 및 관리 -저장탱크에서의 물, 오일, 가스 감시	전류 및 전압 센서 레벨 센서(수위검지기), 초음파 센서(용량 측정)
안전·긴급	**주변 접근 제어** **폭발·유해가스**	-제한구역 내 침입자 감시 및 접근 제어 -산업 환경에서 가스 레벨 및 누출 감시	적외선(Pyroelectric Infrared Ray, PIR), 홀효과(창문 등), RFID·NFC 태그 O_2, H_2, CH_2, 이소부탄, 에탄올 검출 센서
소매	**공급망 제어** **제품 관리**	-저장 제품 상태 모니터링 및 제품 이력 추적 -선반, 창고에서의 제품 회전 제어	RFID·NFC 태그 하중 센서(로드 셀), RFID·NFC 태그
물류	**선적물 품질감시** **근접 저장 회피**	-진동, 컨테이너 개방, 저온유통 등 모니터링 -인화성 제품을 보관한 컨테이너의 경고 발령	빛, 온도, 습도, 충격, 진동 가속도계 센서 O_2, H_2, CH_4, 이소부탄, 에탄올, RFID·NFC 태그

센서 기술

- 사물 인터넷 서비스 부문별 센서 응용 예

분야	응용 예	구체적 응용	활용 센서
산업 제어	**사물 통신 응용** **실내 공기 품질**	-기계 자가 진단 및 자산 통제 -화학공장 내부 독가스 및 산소 수준 감시	전압, 진동, 가속도계, 전류 센서 CO, CO_2, NH_3, NO_2, SH_2, O_3 검출 센서
스마트 농업	**그린하우스** **와인 품질 제고**	-과일 생산 및 품질 제고를 위한 농작물 생육환경 제어 -포도 당도 제어를 위한 토양 수분 모니터링	토양 온도, 습도, 잎 습기, 기압, 일사량 센서
스마트 동물 농장	**새끼 돌봄** **동물 추적**	-생존 및 건강을 위한 새끼 성장 환경 제어 -개방 목장에서 동물 위치 파악 및 식별	CH_4, SH_2, NH_3, 온도, 습도 센서 수동태그(RFID, NFC), 능동태그(Zigbee, WiFi 등)
스마트홈	**에너지·물 사용** **원격 제어 가전**	-에너지·물 공급과 소비 모니터링 -원격으로 가전제품 제어	전류 및 전압 센서, 액체유동 센서 구동기 릴레이
헬스케어	**의료용 냉장고** **환자 모니터링**	-백신, 의약품 저장 냉장고의 상태 제어 -병원 및 환자 자택에서 환자 상태 모니터링	빛, 온도, 습도, 임팩트, 진동, 가속도계 센서 ECG(심전도), 펄스, 가속도계, 호흡 센서

출처: Libelium(2014) 요약 발췌, 재정리

IoT 디바이스 – 디바이스 플랫폼 기술

디바이스 플랫폼 기술

- 플랫폼 (Platform)
  - 다양한 제품이나 서비스를 제공하고 소비하기 위해 사용하는 토대
  - 컴퓨터 분야로 확대해보면, 하나의 운영체제 또는 컴퓨터 아키텍처
  - 다양한 소프트웨어를 실행할 수 있는 기반
  - 예)
    - 개인용 컴퓨터의 운영체제(MS Window, Linux, Mac OS X)
    - 스마트폰의 운영체제 (iOS, 안드로이드)

디바이스 플랫폼 기술

- 센서 디바이스(Sensor Device)
  - 칩셋과 모듈을 이용하여 통신이 가능하고, 주변상황을 인지하는 센서가 포함되며, 간단한 데이터 처리를 수행하는 경량 소프트웨어가 포함된 형태
  - 프로세서, 통신 모듈, 센서 모듈, 구동기 모듈, 개방형 응용 프로그래밍 인터페이스(Open Application Programming Interface, Open API) 소프트웨어로 구성

- 개방형 센서 디바이스 플랫폼
  - 센서 디바이스의 기능을 쉽게 이용하고 센서 내부 모듈에 대한 접근 및 제어를 효율적으로 제공할 수 있는 개방형 응용 프로그래밍 인터페이스 소프트웨어를 오픈 소스 기반으로 제공 / 하드웨어 플랫폼도 오픈 소스 형태로 개방되어 있음
  - 서비스 개발자들은 개방형 응용 프로그래밍 인터페이스를 이용하여 자신이 원하는 서비스들을 손쉽게 개발

디바이스 플랫폼 기술

- 개방형 센서 디바이스 플랫폼 사례

센서 디바이스 플랫폼		주요특징
아두이노 (Arduino)		- ATMega 계열 저전력 프로세서 이용 - 아두이노 통합 개발 환경 제공, C/C++ 언어 기반 개발(넓은 사용자) - 윈도, 리눅스, 맥 OS X의 크로스 플랫폼 지원 - http://www.arduino.cc
라즈베리 파이 (Rasberry Pi)		- Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit SoC @ 1.4GHz (Pi 3 B+) - 리눅스 운영체제 플랫폼 중심, 파이썬(Python) 언어 기반 개발 -http://www.raspberrypi.org
비글보드 (Beagle Board)		- ARM Cortex-A8 시리즈 프로세서 이용 - 이클립스 같은 기존의 통합 개발 환경 이용 - 리눅스, 안드로이드 운영체제(Ardroid OS) 플랫폼 - http://beagleboard.org/

네트워크 인프라 기술

네트워크 인프라 기술

- 사물 인터넷의 네트워크 인프라
  - 기존의 유·무선 통신기술과 근거리 무선통신 기술을 융합
    - 부호 분할 다중 접속(Code Division Multiple Access, CDMA), 광대역 부호 분할 다중 접속(Wideband Code Division Multiple Access, WCDMA), 와이파이, LTE 등 무선 통신기술
    - 지그비, 블루투스, NFC 등의 저전력·저비용 근거리 무선통신 기술
  - 저비용·저전력이 가능하고, 폭넓은 통신 커버리지, 서비스 품질(Quality Of Service, QoS)이 보장되어야 함

  - 국내는 이동통신사들이 중심이 되어 사물 인터넷 네트워크 인프라 구축을 주도
    - SKT : 다양한 표준화 기구에 참여하여 LTE 망의 사물 인터넷 인프라 이용 방법을 모색
    - KT : 노키아와 함께 LTE-M(Machine) 기술에 대한 표준화를 추진
    - LG U+ : 스마트홈 시장과 관련하여 지-웨이브 규격을 활용

네트워크 인프라 기술

네트워크 방식	주요 특징
지그비 (Zigbee)	- IEEE 802.15.4 PHY 표준, 그물형 망(Mesh Network) 구성 가능 - 초소형, 저비용, 저전력의 무선 센서 네트워크 구축 가능 - 868mhz(20kbps), 915MHz(40kbps), 2.4GHz(205kbps) / 통신거리 10~100m
블루투스 (Bluetooth)	- 초소형, 저비용, 저전력(Bluetooth Low Energy), 방사형 망(Star Network) - 블루투스를 채택한 다양한 제품들 존재(마우스, 키보드, 이어폰, 스피커) - 통신거리 수~100m
지-웨이브 (Z-wave)	- 스마트 홈 서비스를 위해 개발된 표준(유럽 중심의 지-웨이브 연합), 그물형 망 - 저비용, 저전력의 무선 센서 네트워크 구축 가능 - 869MHz(9.6kbps), 908MHz(40kbps) / 통신거리 30m
와이파이 (WiFi)	- IEEE 802.11 표준, 방사형/그물형 망 - 무선 인터넷을 가능하게 해주는 Access Point (AP) 근처에서만 이용 가능 - 고속 무선 네트워크 구축 가능, 지그비, 블루투스에 비해 고전력 소모 - 통신거리 100m

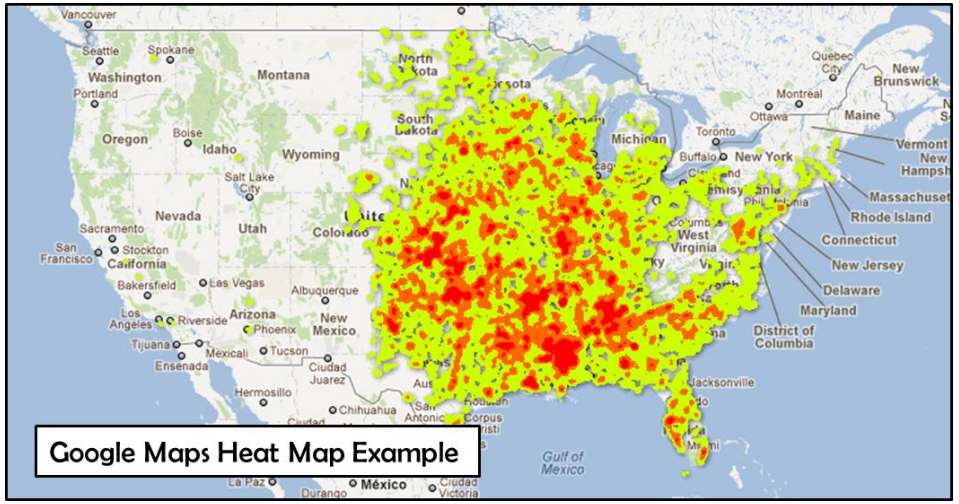
서비스 플랫폼 기술

서비스 플랫폼 기술

- 이기종 센서 디바이스 연결 및 제어
  - 센서 디바이스 플랫폼, 네트워크 인프라 기술, 통신 프로토콜 등이 필요
  - 통신 프로토콜은 MQTT(Message Queuing Telemetry Transport), CoAP(Constrained Application Protocol), HTTP 등 이용
    - TCP/IP(Transmission Control Protocol/Internet Protocol) 기반
- 사물 정보 수집 및 저장
  - 대용량이면서 다양한 형식의 센서 데이터를 효율적으로 수집, 저장
  - 실시간 데이터는 메인 메모리 기반 데이터 저장 관리
  - 배치 처리용 데이터는 데이터베이스 기반 데이터 저장 관리
  - 대규모 데이터는 클라우드 인프라 기반의 분산 빅 데이터 저장 관리

서비스 플랫폼 기술

- 사물 정보 검색·분석·시각화
  - 사물들로부터 수집되거나 축적된 데이터를 분석하여 지능형 서비스를 제공하기 위해 활용
  - 실시간 분석, 배치 분석, 축적된 데이터 규모에 따라 빅 데이터 분석 제공
  - 사물 인터넷 서비스에 따라 필터링, 통계, 데이터 마이닝 등의 다양한 분석 기법들 제공



1950~2010까지 토네이도 이동을 추적한 히트맵

출처: http://www.cartographicperspectives.org/index.php/journal/article/view/cp72-peterson-et-al/479

서비스 플랫폼 기술

- 사물 정보의 개방형 웹 서비스
  - 서비스의 개발을 효율적으로 지원하기 위해 자신이 보유한 기능/데이터를 개방형 응용 프로그래밍 인터페이스(Open API)를 통해 외부에 제공
  - 대규모 사물들과 대용량 데이터를 처리할 수 있는 개방형 사물 인터넷 플랫폼 기반으로 사물 인터넷 시장이 지속적으로 확산 가능

서비스 플랫폼 기술 - 사물 인터넷 아키텍처

- 사물 인터넷 모델의 변화
  - 체계적인 사물 인터넷 아키텍처가 구성되면, 효율적인 사물 인터넷 서비스 제공이 가능
  - 다양하고 방대한 양의 정보가 수집과 SW의 규모가 커지면서 필요한 아키텍처가 다양해지고 있음
  - 정보를 한 곳으로 모았다 제공하는 중앙 집중식 클라우드 형태와 분산 클라우드 형태가 연구되고 있음

출처: “분산형 데이터베이스 기반 비중앙식 IoT 플랫폼을 이용한 스마트 홈 서비스”

서비스 플랫폼 기술 - 사물 인터넷 아키텍처

출처: Intel

사물 인터넷 아키텍처 구성도의 예

서비스 플랫폼 기술 - 사물 인터넷 아키텍처

- 사물 인터넷 아키텍처의 특징
  - 이러한 특징을 고려하여 소프트웨어를 설계하도록 안내

구분	내용
확대성(Expansion)	다량의 디바이스 지원
자율성(Autonomy)	사람의 제어가 거의 불필요
탄력성(Resiliency)	장애를 극복하고 기능을 지속적으로 수행
내구성(Durability)	장시간 사용에도 견딜 수 있는 성능
접속성(Connectivity)	사물 간 (M2M) 또는 사람과 사물 간의 원활한 통신

인텔에서 제시하는 사물 인터넷 아키텍처의 특징

서비스 플랫폼 기술 - 사물 인터넷 아키텍처

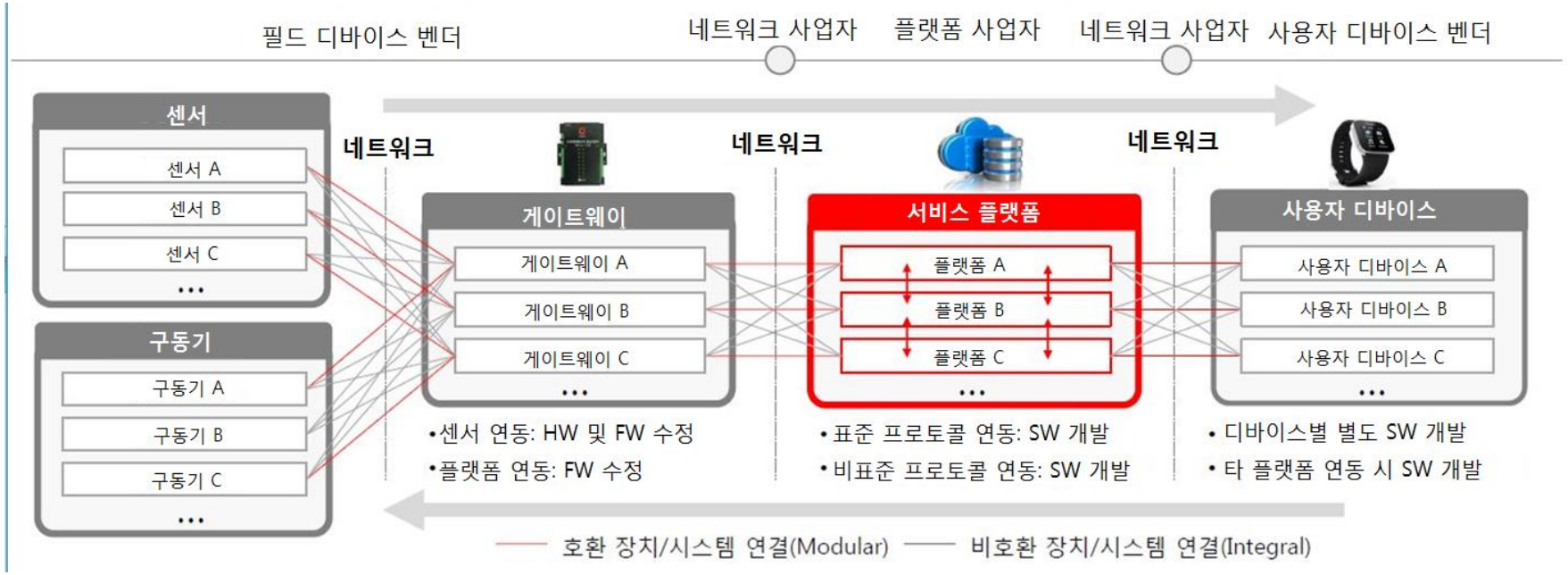
- 사물 인터넷 아키텍처의 기본 구성
  - 사물 인터넷으로 연결된 디바이스는 게이트웨이를 거쳐 시스템으로 연결
  - 무선 네트워크 노드에서 수집된 정보가 게이트웨이에서 걸러져서 빅 데이터로 저장되고 필요한 서비스에 제공

출처: www.seminartoday.net

- WPAN(Wireless Personal Area Network): 단거리 무선망

서비스 플랫폼 기술 - 사물 인터넷 아키텍처

- 사물 인터넷 서비스 아키텍처
  - 센서를 통해 수집된 데이터가 게이트웨이를 거쳐 서비스 플랫폼에 전달
  - 서비스 플랫폼은 앞 단의 사물 인터넷 구성요소를 연결하는 역할과 데이터 기반 서비스를 제공하는 역할을 수행



출처: KT - IoT 서비스 플랫폼 아키텍처 분석

마무리

2차시 정리

- 사물 인터넷 특징 및 이슈

- 사물 인터넷의 주요 기술
  - IoT 디바이스 – 센서
  - IoT 디바이스 – 하드웨어 플랫폼
  - IoT 네트워크
  - IoT 서비스 플랫폼

3차시 소개

- IoT 디바이스
  - 센서 및 액추에이터
  - 하드웨어 플랫폼