Est. 1841

YORK ST JOHN UNIVERSITY

IoT Security: Emerging Security Challenges for Multiprotocol IoT Gateways

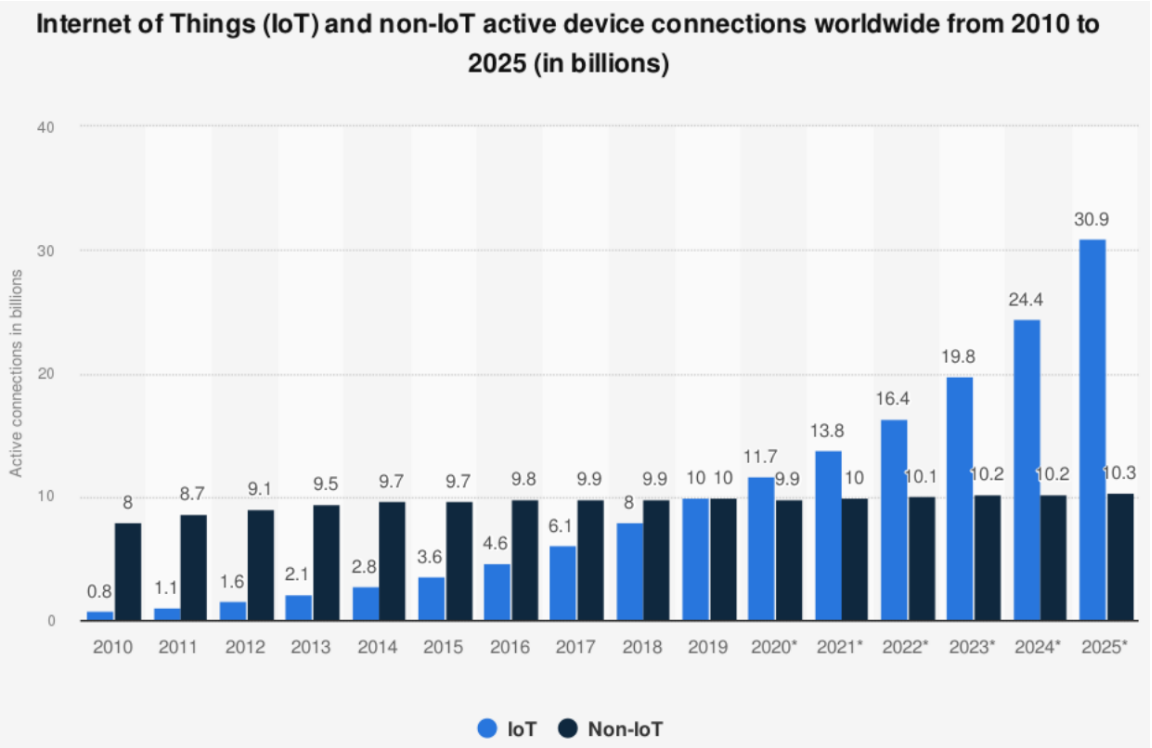
Aminu Bello Usman, PhD, SFHEA
Associate Head of Computer & Data Science

Presented at the 9th ICOWOBAS 2023 Workshop on Basic and Applied Sciences
8th May 2023

Outline

- Internet of Things (IoT) - statistics & facts
- Why IoT is Getting Popular?
- Essential Protocols for IoT
- IoT Multiprotocol Gateway
- Architecture and components of a multiprotocol IoT gateway
- Emerging Security Challenges of Multiprotocol IoT gateways

Internet of Things (IoT) - Statistics & facts



Statistica.com

- In 2023, the number of cellular IoT connections is estimated to reach 3.5 billion. (Forbes)

- **The size of the global IoT healthcare market is expected to reach $534.3 billion by 2025.** (Grand View Research)

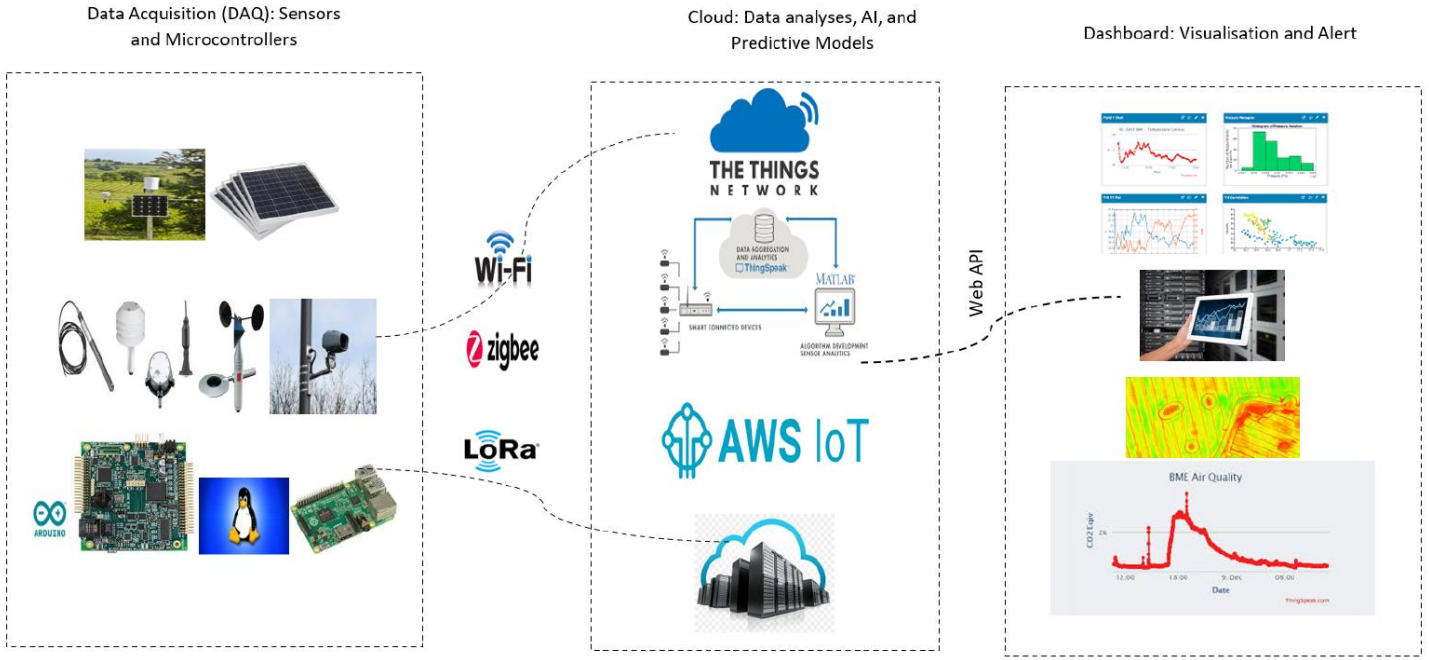
According to www.internetsociety.org,

By 2025, there could be up to 100 billion connected IoT devices with a global economic impact of more than $11 trillion.

IoT

- A network of physical objects, or "things," that are embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet.

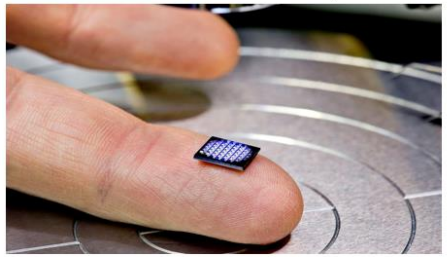
- IoT Connectivity
  - **Device to device (D2D)**
  - **Device to gateway**
  - **Gateway to data systems**
  - **Between data systems**



Ubiquitous connectivity

Cloud Computing—cloud computing has become a point with virtually unlimited processing power and storage for IoT data

Miniaturization—smaller computers and communication chips



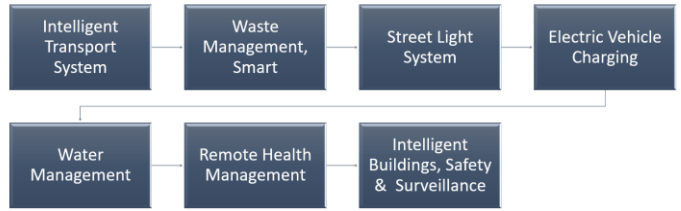
By improving operational efficiency and reducing waste

IoT technology can automate many tasks, freeing up time and resources for more valuable work

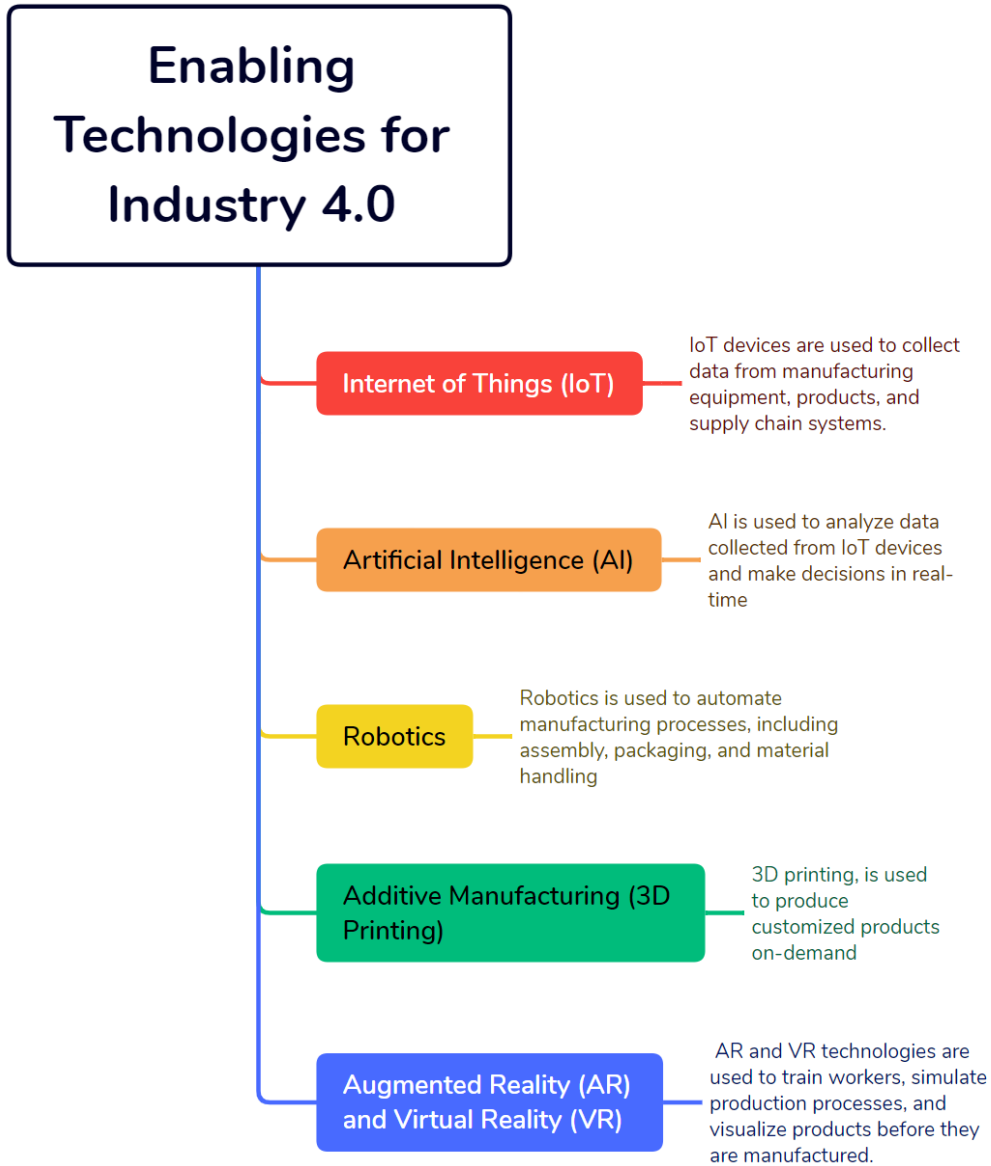
Est. 1841 | YORK ST JOHN UNIVERSITY

IoT has the potential to transform how we live and work, providing new opportunities for innovation, efficiency, and convenience.

IoT Applications for Smart City

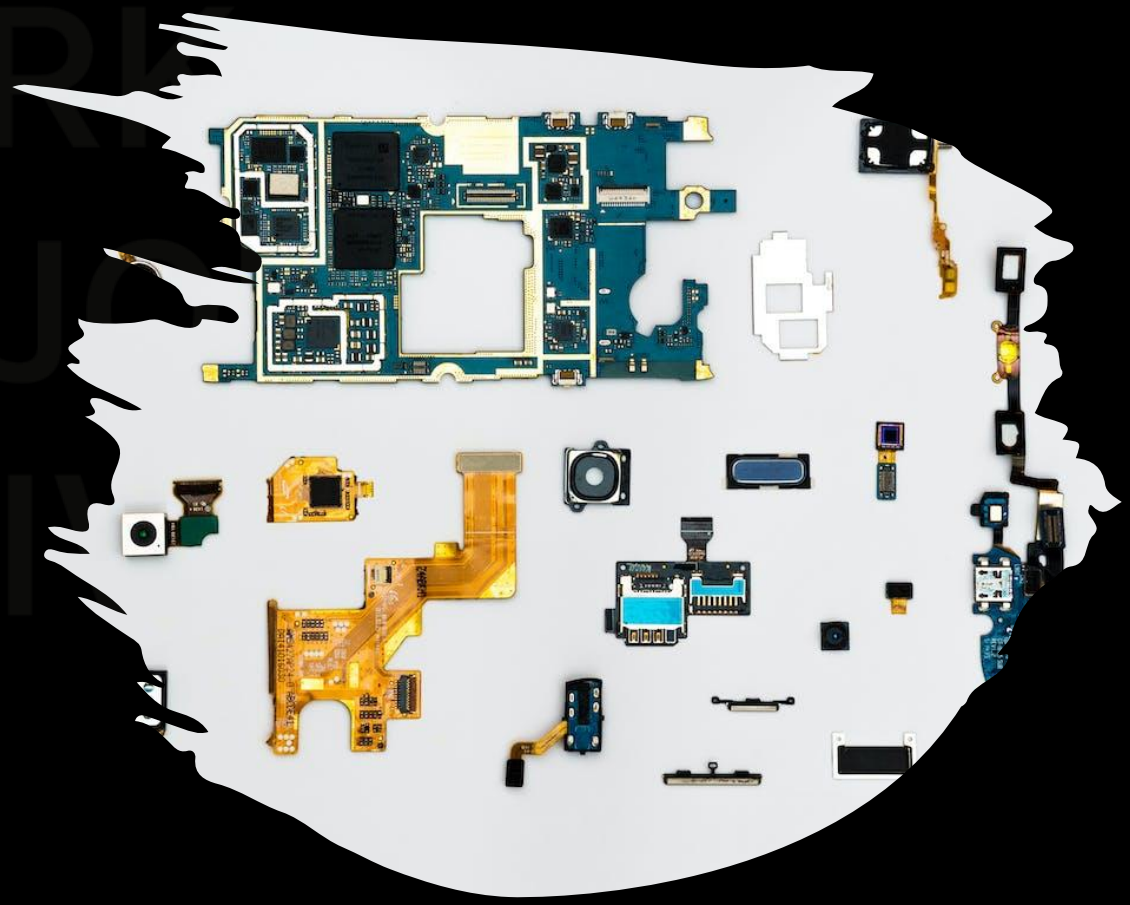


- IoT is a crucial component of Industry 4.0, enabling manufacturers to optimize production processes, reduce costs, and improve product quality



Essential Protocols for IoT

- **Communication Protocol**
  - Defines how data is communicated between the sensor nodes and the gateway and between the gateway and the cloud.
  - Wired or wireless communication
- **Data Protocol**
  - Defines how data is formatted, handled, and presented
  - MQTT (Message Queue Telemetry Transport) DDS (Data Distribution Service)
  - AMQP (Advanced Message Queuing Protocol)



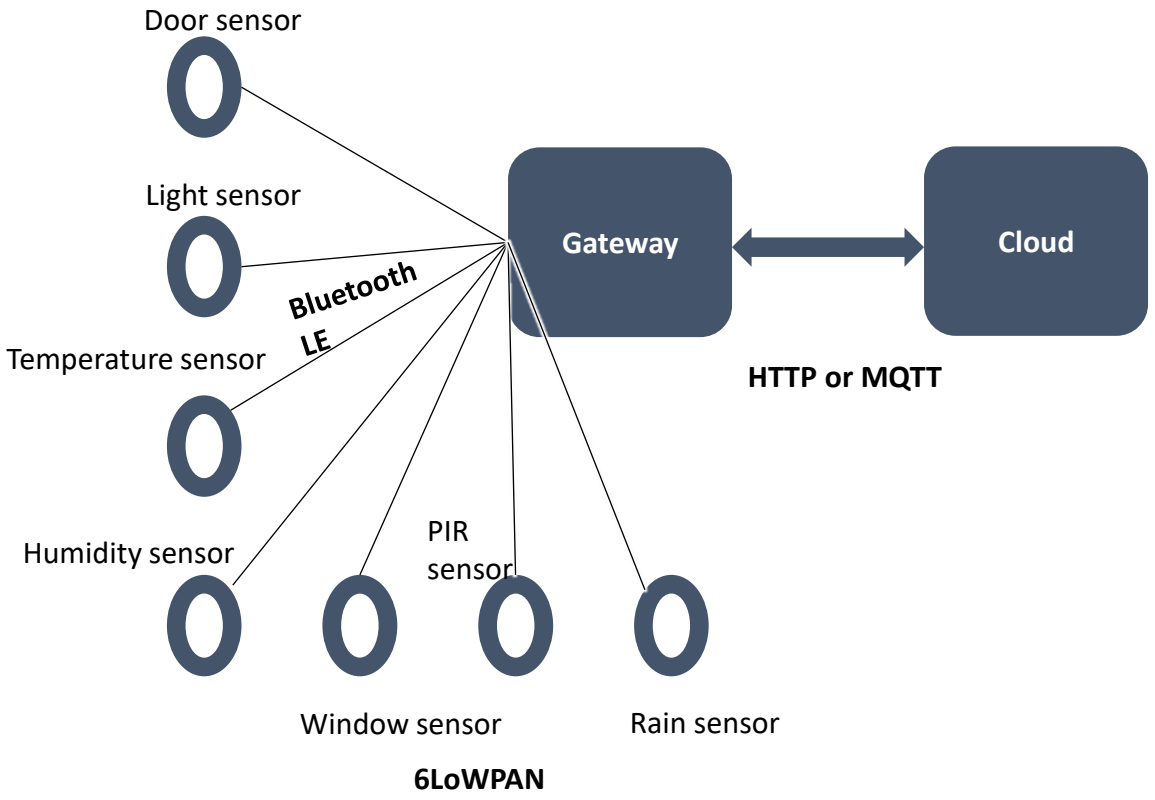
IoT Communication Protocol

- Two main categories of IoT Communication Protocols
- 2.4GHz IoT protocols.
  - **Wi-Fi**
  - **Bluetooth Low Energy (BLE)**
  - **Zigbee**
  - **Thread is a newer 2.4GHz IoT protocol**
- Sub-GHz IoT protocols
  - offers long-range, low-power connectivity and are suitable for a wide range of IoT applications, especially those that require coverage over large areas.- LPWAN
  - **LoRaWAN**
  - **Sigfox**
  - **NB-IoT**
  - **Weightless**

Protocol	Range	Data Rate	Multimedia Support
WiFi	30-100 meters	11 Mbps - 10 Gbps	Yes
Zigbee	10-100 meters	20-250 kbps	No
Bluetooth	10 meters	1-3 Mbps	Yes
LoraWAN	Up to 10 km	0.3-50 kbps	No
NB-IoT	Up to 10 km	50-250 kbps	No
Sigfox	Up to 40 km	100 bps - 1 kbps	No
Z-Wave	Up to 100 meters	9.6-100 kbps	No
Thread	Up to 700 meters	250 kbps	Yes
6LoWPAN	Up to 100 meters	250 kbps	Yes
MQTT-SN	Up to several kilometers	10-250 kbps	No
CoAP	Up to several kilometers	10-250 kbps	Yes
LoRa	Up to 10 km	0.3-50 kbps	No
NB-Fi	Up to 5 km	100-250 kbps	No

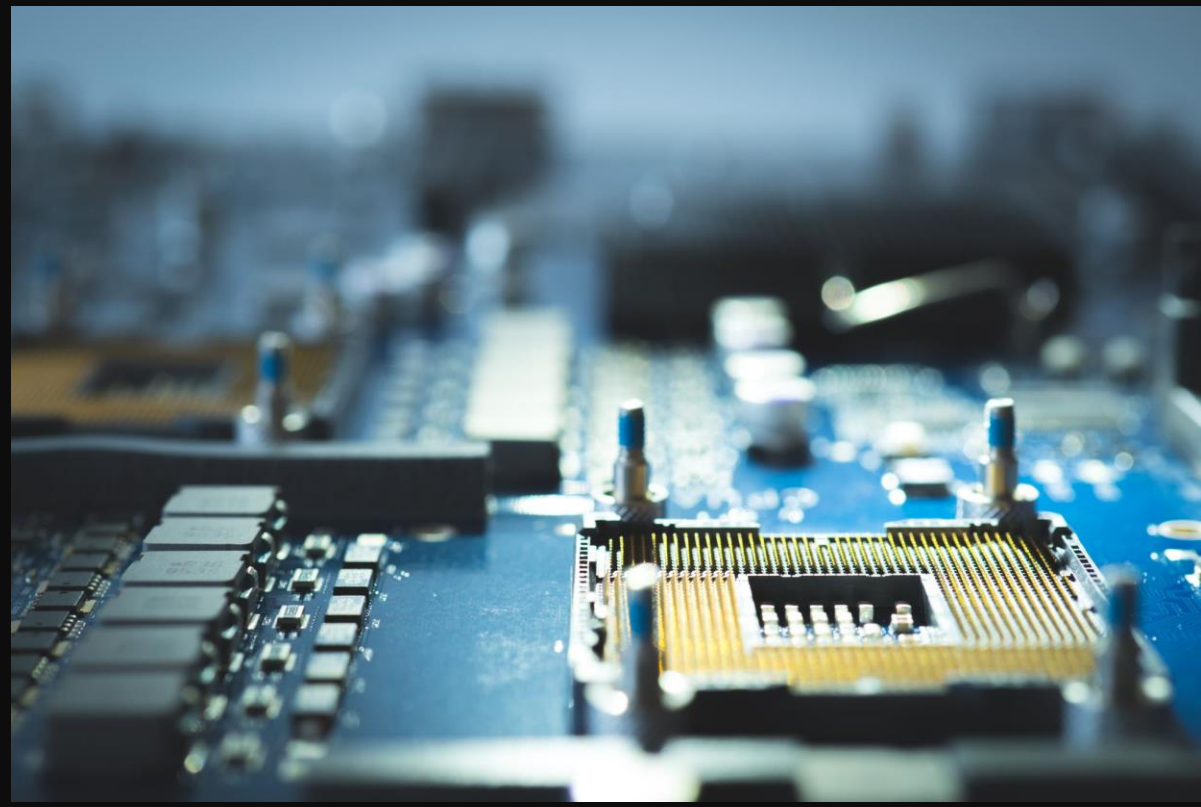
IoT Gateway

The gateway is responsible for collecting data from various devices, aggregating it, and transmitting it to the cloud or enterprise network for processing and analysis.

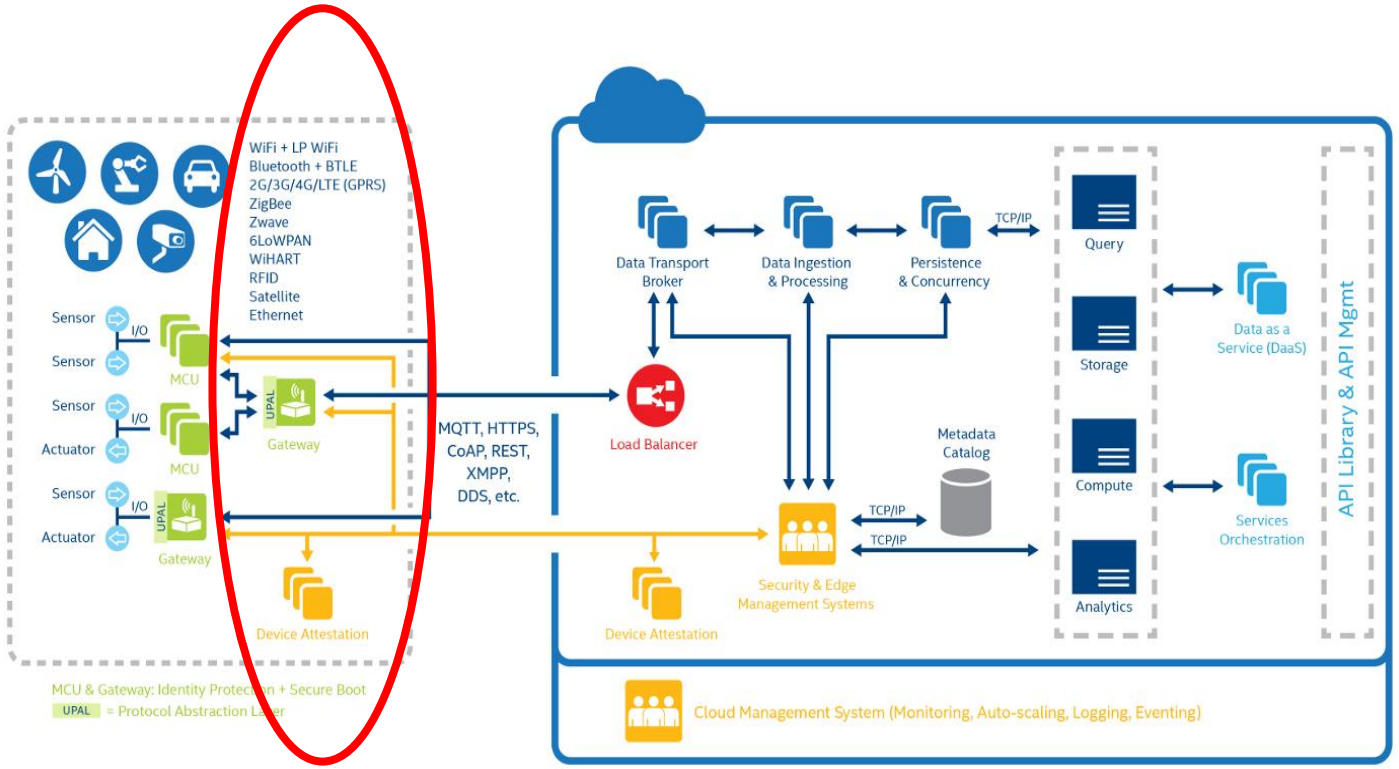


Why IoT Multiprotocol Gateway

- Interoperability
- Cost savings
- Scalability
- Flexibility
- Security



IoT Multiprotocol Gateway



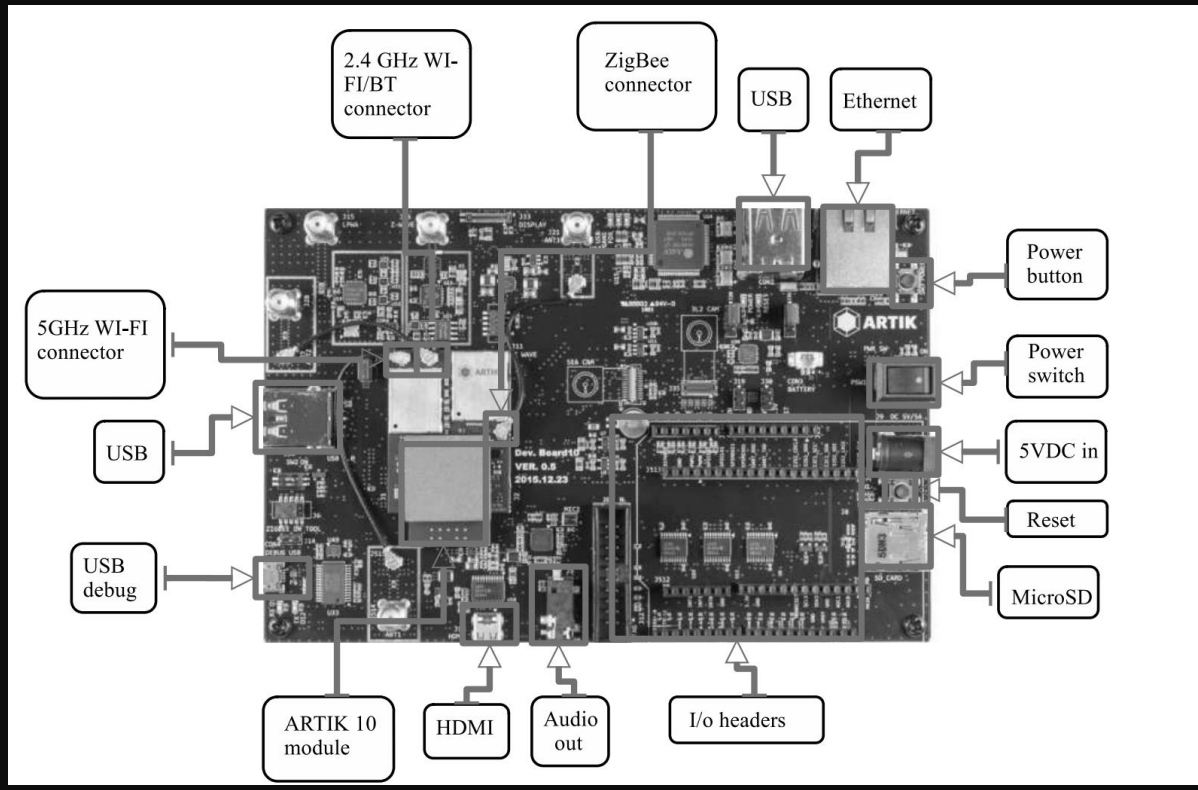
Intel® IoT Gateway

- Intel® IoT Gateway Technology supports Wi-Fi, Bluetooth, ZigBee, and Ethernet
- LoRa Gateway supports Wi-Fi, Ethernet, and Bluetooth
- Cisco IR809 Industrial Integrated Services Router supports 4G/LTE, Wi-Fi, and Ethernet
- The Things Gateway supports Wi-Fi, Bluetooth, and LoRa
- Advantech WISE-710 supports Wi-Fi, Bluetooth, ZigBee, and LoRa.

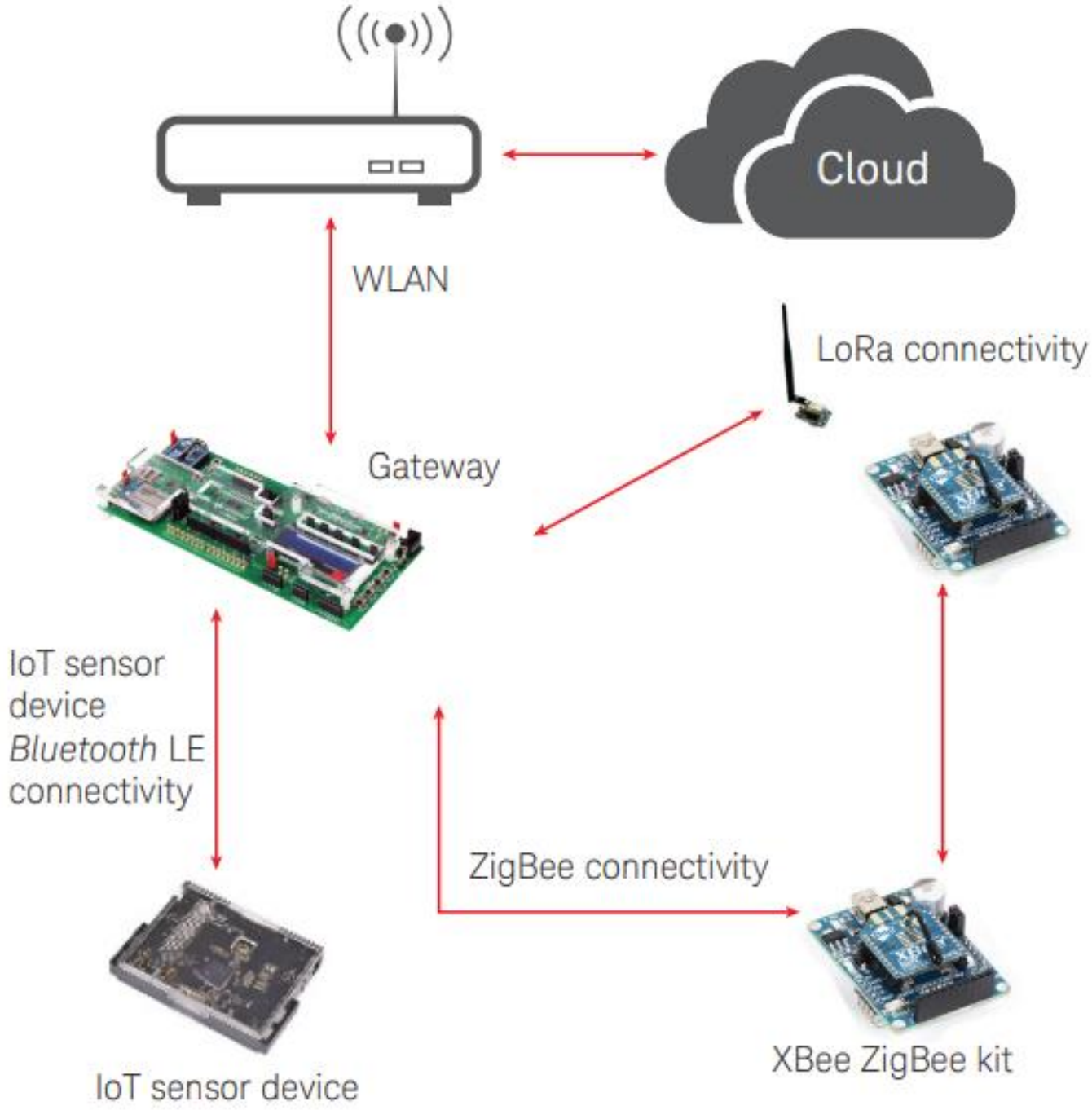
The Artik 1020 board - Internet of Things (IoT) platform

- The Artik 1020 board is an Internet of Things (IoT) platform developed by Samsung that supports multiprotocol, including Wi-Fi, Bluetooth Low Energy, ZigBee, and Thread

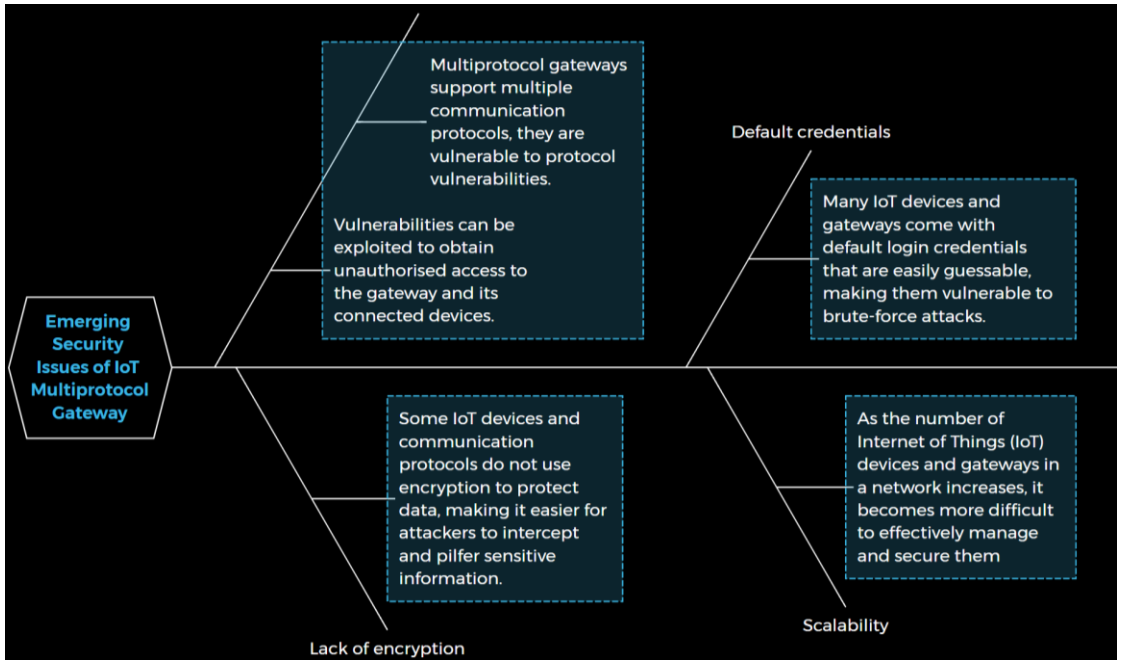
- The board features 1GB of LPDDR3 RAM, 4GB of eMMC flash storage, and Wi-Fi and Bluetooth connectivity. In addition, it includes a range of sensors and interfaces, including GPIO, SPI, I2C, UART, and USB.

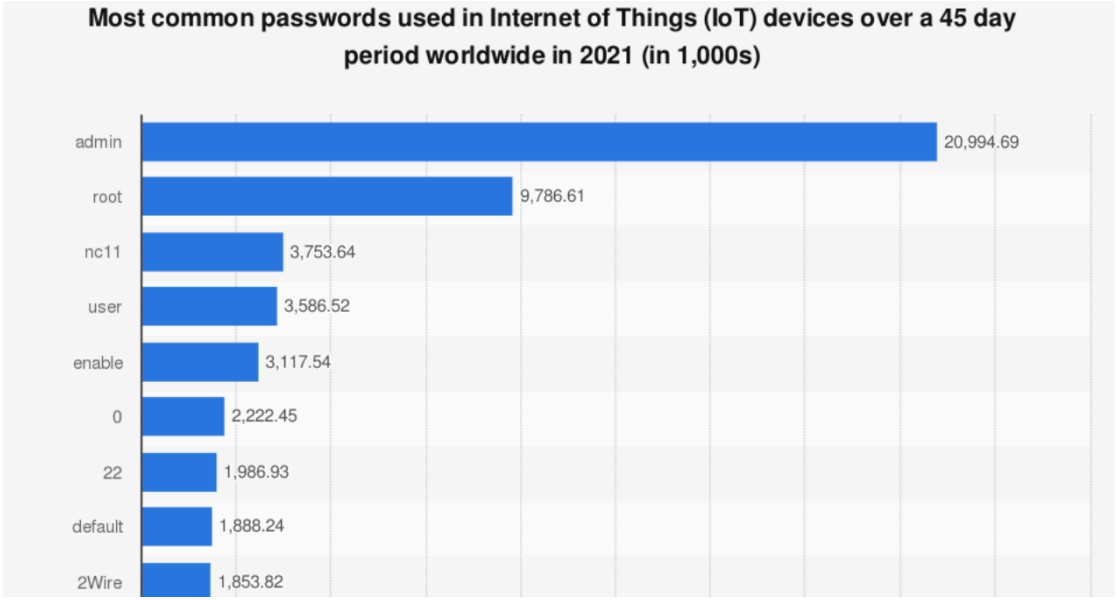


Components of a Multiprotocol IoT Gateway



Keysight Tech. U3800A IoT Development Kit

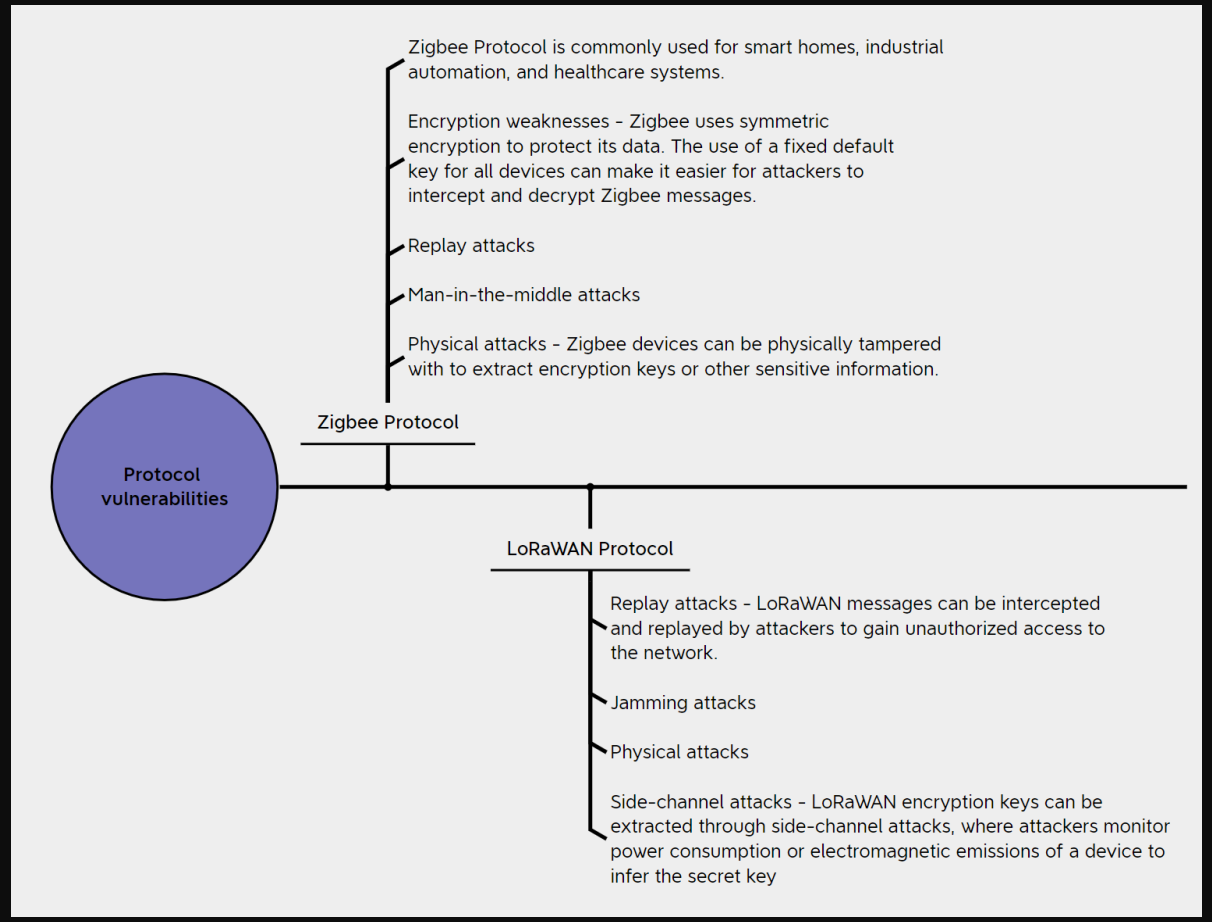




Statistica.com

Protocol Vulnerabilities

- Each communication protocol supported by the gateway may have its own security vulnerabilities.
  - For example, ZigBee and LoRaWAN protocols has known vulnerabilities
    - Zigbee and LoRa uses a simple security mechanism that relies on a shared secret key for encryption and authentication.
    - Zigbee and LoRa does not use a secure timestamp or nonce mechanism, which can make it easier for attackers to replay network traffic.



Pivot Attack on IoT Multiprotocol Gateway

- The attacker can exploit a vulnerability in the gateway to gain access and then uses that access to move laterally through the network and compromise other devices.
    - Once the attacker have access to the gateway, they can use it to pivot to other devices on the network, such as smart locks, cameras, or sensors.
    - Prevention
        - Regular vulnerability assessments and patch management, network segmentation, access controls, and encryption.
        - Network monitoring - monitor the network for unusual activity and respond quickly to any detected attacks
        - keep IoT devices up-to-date with the latest security patches and firmware updates to prevent known vulnerabilities from being exploited.

A Signal Jamming on IoT Multiprotocol Gateway

- The IoT devices may become disconnected from the gateway causing them to malfunction or become unresponsive.
  - this could lead to service disruptions, data loss
  - or even physical harm if the devices are part of a critical infrastructure or medical system
- To prevent signal jamming attacks, it's essential to secure the wireless communication channels used by IoT devices.
  - monitor the network for suspicious activity and respond quickly to any detected attacks.
  - using frequency-hopping techniques to avoid interference from jamming signals

AI-Based attacks on an IoT Multiprotocol Gateway

- Deep learning-based attack
  - AI algorithm is used to analyse the behaviour of the IoT devices connected to the gateway for attacks.
- AI-powered malware
  - AI is being used to generate malware that can adapt to changes in network traffic, evade detection by gateway security mechanism
- Botnets
  - AI can be used to create more sophisticated botnets that can evade detection and launch more effective attacks.

- Prevention
  - Regular security audits and vulnerability assessments
  - Implement strong security measures such as network segmentation, access controls, and encryption
  - Using AI-based security solutions that are capable of detecting and responding to AI-based attacks

Case studies on successful implementation of Security Measures for Multiprotocol IoT Gateways

Intel® IoT Gateway Technology supports Wi-Fi, Bluetooth, ZigBee, and Ethernet

LoRa Gateway supports Wi-Fi, Ethernet, and Bluetooth

Cisco IR809 Industrial Integrated Services Router supports 4G/LTE, Wi-Fi, and Ethernet

The Things Gateway supports Wi-Fi, Bluetooth, and LoRa

Advantech WISE-710 supports Wi-Fi, Bluetooth, ZigBee, and LoRa.

Bosch, a global provider of technology and services - The solution included strong authentication mechanisms, encryption, access control, and intrusion detection and prevention systems.

Protocols
SIM card socket x 1, 3G/4G LTE mini PCIe connector, NB-IoT connector

Schneider Electric - The solution included strong authentication mechanisms, encryption, access control, and intrusion detection and prevention systems. The gateway was also deployed in a segmented network to limit the impact of security incidents.

NXP Semiconductors - The gateway was also designed with a secure boot mechanism to ensure the integrity of the firmware.

Conclusion

- Several companies offer successful implementations of security measures for multiprotocol IoT gateways.

We are interested in understanding

How can blockchain technology be used to enhance the security and integrity of IoT data transmitted through an IoT multi-protocol gateway?

What are the ethical and legal implications of using an IoT multi-protocol gateway, particularly with respect to data privacy and security?

What are the most effective methods for implementing secure over-the-air firmware updates to IoT devices through an IoT multi-protocol gateway?

Thank you for listening

Questions?

Est. 1841 | YORK ST JOHN UNIVERSITY

www.yorksj.ac.uk

References

- Castellanos, W., Macias, J., Pinilla, H. and Alvarado, J.D., 2021. Internet of things: a multiprotocol gateway as solution of the interoperability problem. *arXiv preprint arXiv:2108.00098*.

- Derhamy, H., Eliasson, J. and Delsing, J., 2017. IoT interoperability—on-demand and low latency transparent multiprotocol translator. *IEEE Internet of Things Journal*, *4*(5), pp.1754-1763.

- MODE, T., MODE, S. and MODE, S., 2016. Keysight Technologies.