LoRaWAN®

Advancements in Cyber Security and Implications for an Industrial IoT Network

aircom

YZ® SYSTEMS

THE FOUNDATION OF SECURE COMMUNICATIONS

When it comes to Industrial IoT networks, security is the bedrock—just like the foundation of a building. Without a secure base, even the most sophisticated structure is at risk of collapse. Our Aircom solution for LoRaWAN communications relies on robust security at every level to safeguard data integrity and shield critical infrastructure.

This white paper delves into the latest advancements in cyber security tailored for Industrial IoT, showing how a secure foundation enables protected data transmission.

With end-to-end encryption and a security-first architecture, Aircom employs rigorous protocols like AES-128 encryption to protect data in storage and transit. From the device level up to network servers, each communication layer is fortified, creating a "moving vault" that keeps data secure from end to end.

Our goal? To ensure Aircom provides not only precise data but also unparalleled security. Let's explore how these advancements create a resilient foundation for Industrial IoT.

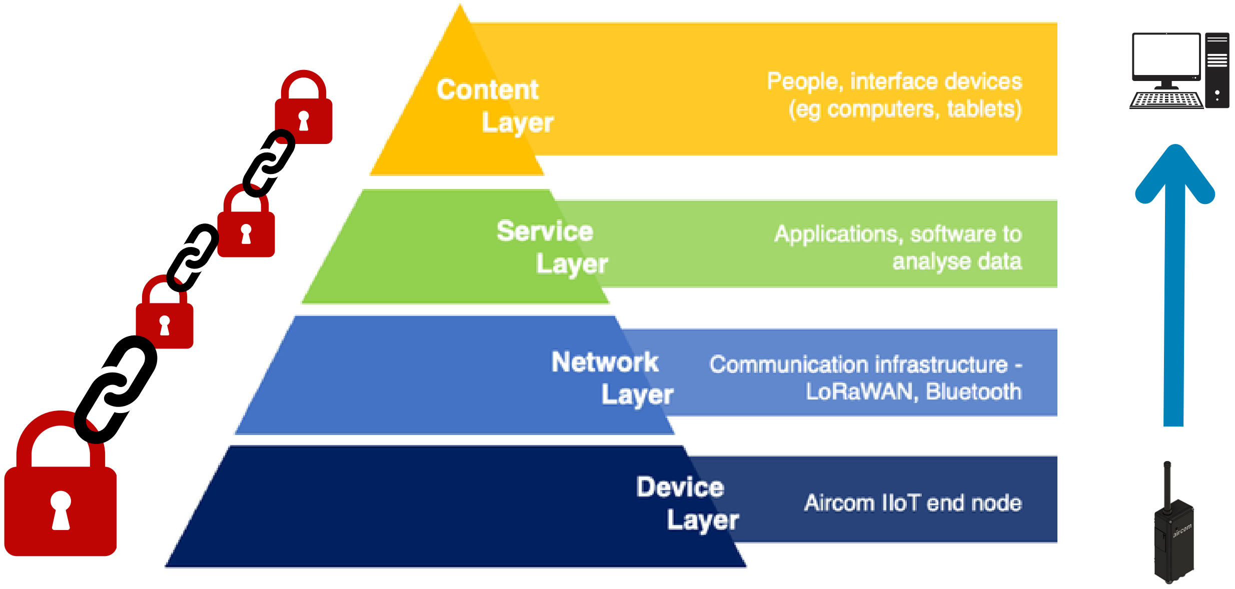
SECURING DATA THROUGHOUT ITS LIFECYCLE

A secure infrastructure addresses every stage of data’s journey, safeguarding it from the moment it leaves operational technology—such as regulators and actuators—through layers of smart devices and networks. For Aircom, this journey begins at the device level, where data security is integrated at the foundational level and extends up the entire communications stack, ensuring secure visibility on user screens.

Data security operates on two fronts:

- At Rest: When data is stored.
- In Transit: When data moves across networks.

Our strategy secures data across both states, ensuring robust, end-to-end protection.


Content Layer
People, interface devices (eg computers, tablets)
Service Layer
Applications, software to analyse data
Network Layer
Communication infrastructure - LoRaWAN, Bluetooth
Device Layer
Aircom IIoT end node

PROTECTING DATA IN TRANSIT: A MOVING VAULT

Securing stored data is often visualized as locking it in a secure vault—accessible only with the correct credentials. However, when data is in transit, it faces unique vulnerabilities as it moves across networks.

Much like transporting gold bars through city streets, data becomes more susceptible to attacks during its journey. To mitigate these risks, we secure in-transit data by treating it as a "moving vault," accessible only by those with the correct encryption keys.

This approach ensures that, even as data moves, it remains tightly guarded against unauthorized access.

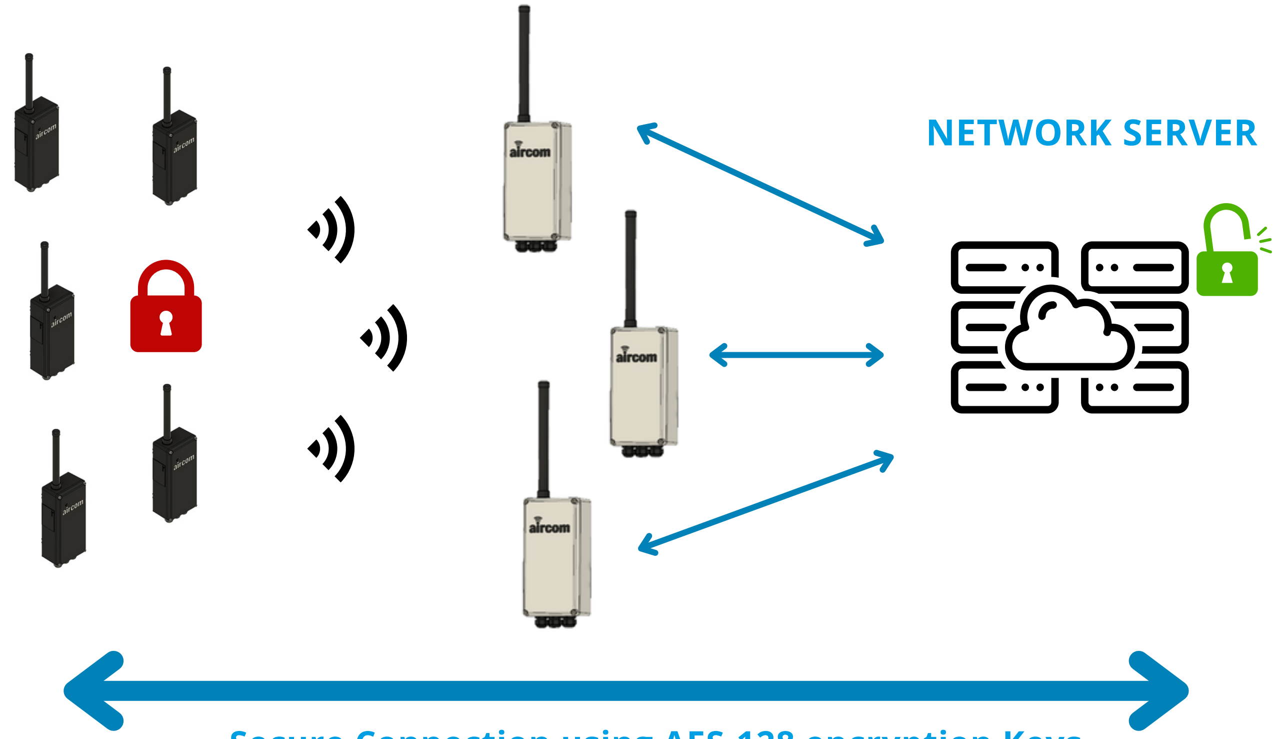
STORED (SECURED)

TRANSIT (SECURED)

LEVERAGING LORAWAN AND AES-128 ENCRYPTION FOR END-TO-END SECURITY

LoRaWAN is a powerful choice for Aircom, offering low power consumption, extensive transmission range, and highly secure communication. Using AES-128 encryption, LoRaWAN provides end-to-end security by safeguarding data from the device level to the network server, where data is decrypted.

The Advanced Encryption Standard (AES-128) is a symmetric block cipher approved by NIST and endorsed by cybersecurity bodies in both the EU and the U.S. This encryption standard, trusted by governments and industries worldwide, secures sensitive data with the same robust protocols used to protect classified information.

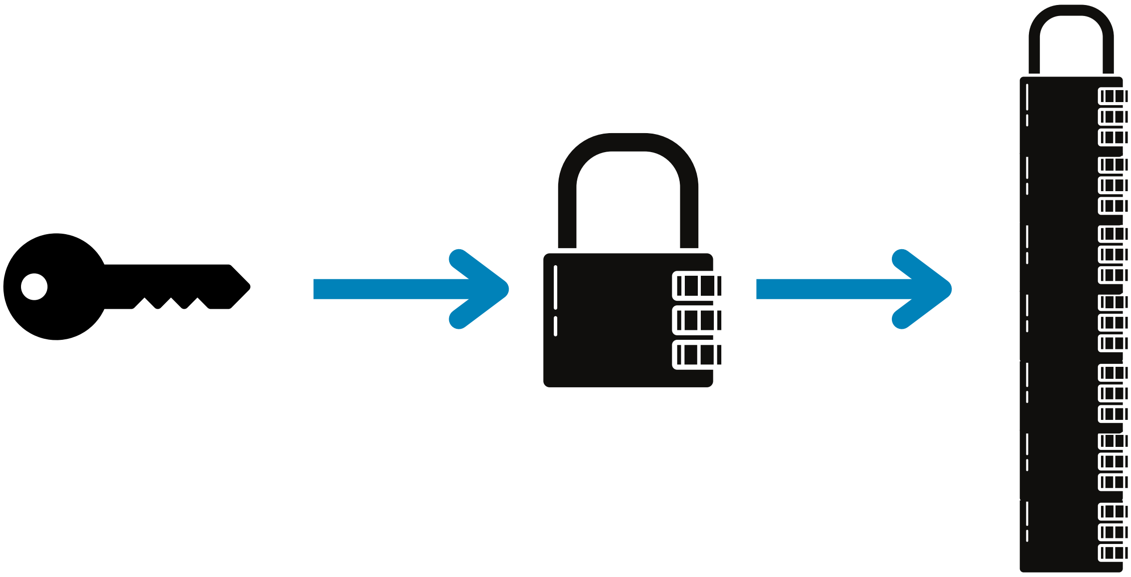


Secure Connection using AES-128 encryption Keys

WHAT IS AES-128 ENCRYPTION?

AES-128 encryption is a symmetric encryption method, meaning it uses a single key for both encrypting and decrypting data. To understand its strength, consider the key as a combination lock with a staggering 340 undecillion possible combinations (that’s 340 followed by 36 zeros).

This vast range of combinations makes AES encryption exceptionally secure, ensuring that only those with the correct key can access or decrypt the data, creating an exceptionally secure environment for sensitive information.



128bit = 340,282,366,920,938,463,463,374,607,431,768,211,455
(or 340 trillion trillion trillion) possible combinations

SECURE SECURITY: AES-128 AND UNIQUE DEVICE AUTHENTICATION

Attempting a brute-force attack on AES-128 encryption is effectively futile. Given the astronomical number of possible combinations, even the most powerful computers would require billions of years to guess the correct key. LoRaWAN further enhances this security by pairing each device with a unique 128-bit AES key (AppKey) and a globally unique identifier (64-bit DevEUI), which together authenticate the device during data transmission.

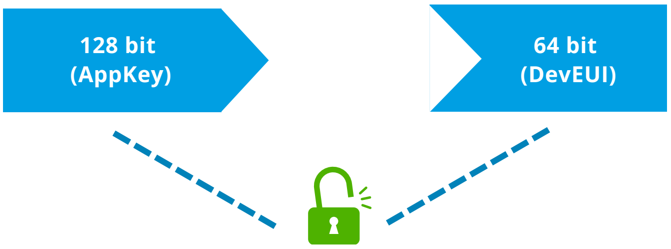
To put this in perspective, the 64-bit DevEUI provides enough unique identifiers to assign over 2 billion devices to each person on Earth, adding another layer of security. The probability of successfully matching a device's correct AES key and DevEUI combination is infinitesimal, making AES-128 not only the global standard but the ideal choice for LoRaWAN's robust, security standards.

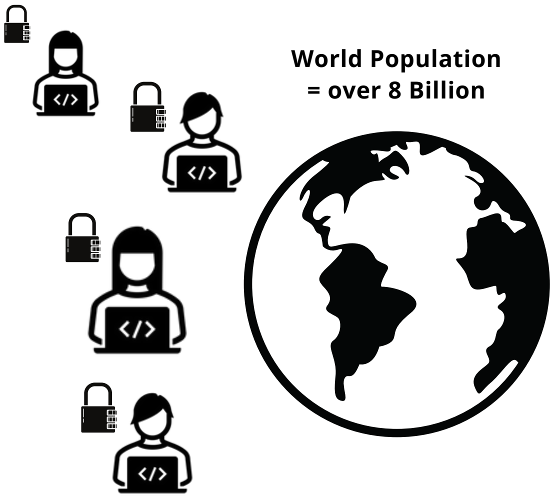
MATCHING THE KEYS

Billions of years for super computers to try all possible combinations of 1 x AES-128bit Key

64bit (DevEUI) = 18,446,744,073,709,551,615. (or 18 million trillion) possible devices

Each person can have more than 2 billion devices each with a unique AES-128bit (AppKey)





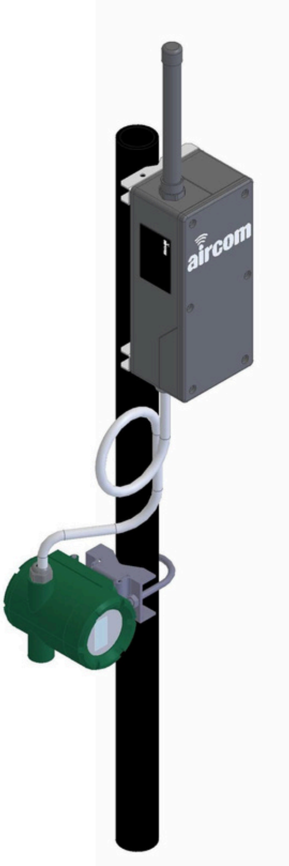
aircom

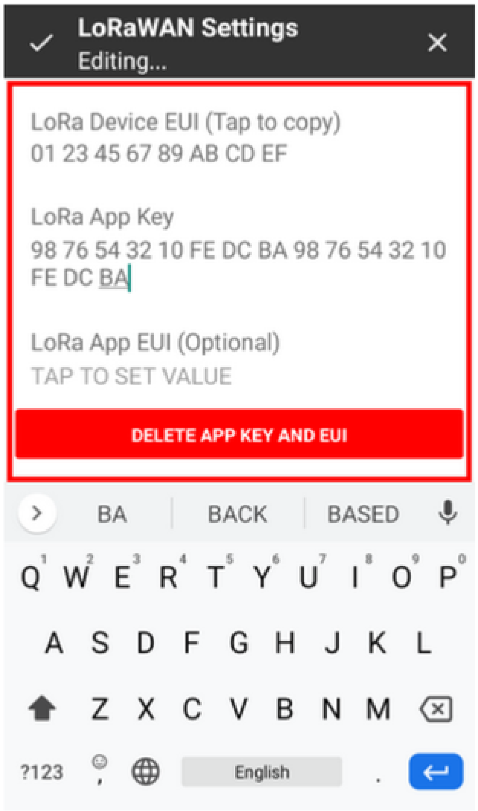
YZ SYSTEMS

KEY INTEGRITY: THE IMPORTANCE OF STRONG, UNIQUE KEY

While AES-128 encryption provides an extremely secure level of security, its effectiveness depends on the strength of the key itself. Using easily guessable keys, such as “123456” or “0000,” undermines security and is akin to leaving the front door key in the lock.

Therefore, a secure AES implementation mandates the use of a 32-character key made up of randomized, unique characters. This approach ensures that keys are unpredictable, safeguarding the encrypted data against unauthorized access and maintaining the high standards of security that AES is designed to provide.




LoRaWAN Settings
Editing...

LoRa Device EUI (Tap to copy)
01 23 45 67 89 AB CD EF

LoRa App Key
98 76 54 32 10 FE DC BA 98 76 54 32 10 FE DC BA

LoRa App EUI (Optional)
TAP TO SET VALUE

LoRaWAN® SECURITY

In our implementation, authentication and encryption are mandatory from the moment data is generated by the end device. Aircom devices can be configured to initiate communication only when required, unlike always-on devices that are continuously vulnerable.

This event-driven communication minimizes the device's exposure to potential attacks by only transmitting data briefly—within milliseconds—and remaining dormant otherwise. Configurable transmission intervals enable flexible scheduling, reducing the device's attack surface.

The LoRaWAN network architecture includes:

- End Devices: Aircom devices that encrypt and transmit data packets via short RF signals.

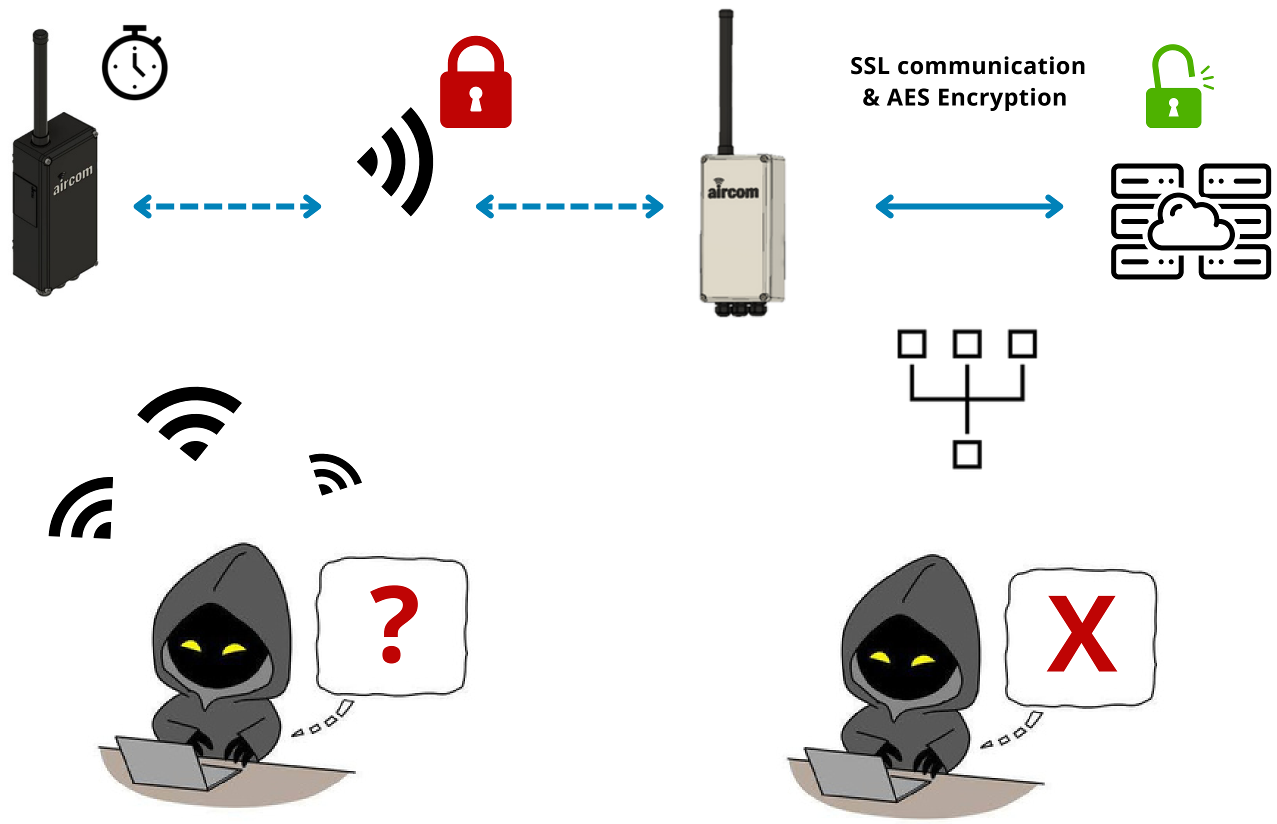
- Gateways: These receive the RF signals and forward them as network packets over SSL-encrypted tunnels, enhancing the AES encryption layer.

- Network Server: The server recognizes the device and decrypts the data.

With this multi-layered approach, LoRaWAN securely transports data from the device to the network server. The next layer of security addresses protecting data once it reaches the IT infrastructure, ensuring comprehensive protection throughout its lifecycle.

LoRaWAN® SECURITY

With this multi-layered approach, LoRaWAN securely transports data from the device to the network server. The next layer of security addresses protecting data once it reaches the IT infrastructure, ensuring comprehensive protection throughout its lifecycle.



━━━ IP Connection

- - - - LoRaWAN Connection

AES Encryption

SSL communication & AES Encryption

Bad Actor (RF wireless)

Bad Actor (wired network)

SECURE DATA VIEWING AND ANALYSIS THROUGH APPLICATION SERVERS

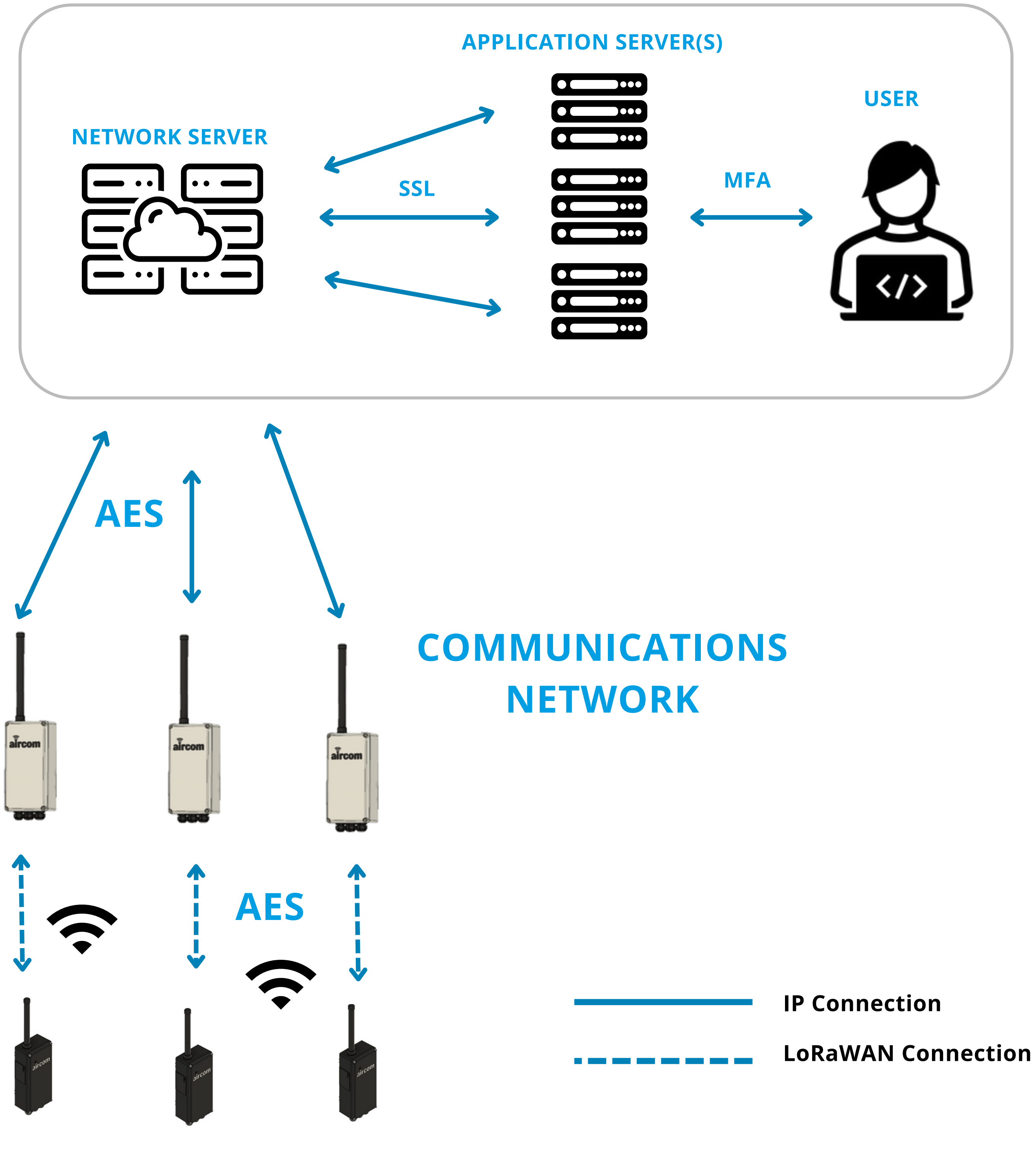
Once data reaches the IT infrastructure, maintaining a high level of security is essential as more services—such as web browsers, databases, and end users—access and interact with it.

To enable secure data visualization and analysis, we deploy application servers. These servers decode and present data for viewing, graphing, and analysis.

Application servers may operate on the same server as the network server or be distributed across multiple servers. This flexibility allows us to scale resources as needed and perform maintenance without disrupting business continuity.

By isolating data analysis functions, we enhance both security and operational resilience, ensuring data remains protected while accessible for critical insights.

SECURE DATA VIEWING AND ANALYSIS THROUGH APPLICATION SERVERS



COMMUNICATIONS NETWORK

▬	IP Connection
‐ ‐ ‐	LoRaWAN Connection

aircom

YZ® SYSTEMS

PRACTICAL SECURITY ARCHITECTURE:
Virtual Private Cloud and Defense in Depth

Our cybersecurity architecture, developed in collaboration with an Industrial Information Cyber Security and Operational Technology specialist, follows best practices for risk management, compliance, and secure server-side implementation.

At the core of our offering is a **Virtual Private Cloud (VPC)**, an isolated, secure network where data is stored, viewed, and managed. Firewalls segregate the VPC from external networks, allowing only specified, authenticated connections in or out. Data transmitted between internal application servers, external network servers, and backup storage is protected by **SSL encryption**, securing sensitive transactions throughout the network.

Hosting Options: Cloud or On-Premises Deployment

YZ Systems offers a **complete hosted cloud solution**, providing managed services within our secure VPC architecture. This approach centralizes security and management within our infrastructure, ensuring clients benefit from our automated safeguards, 24/7 monitoring, and a streamlined environment.

For clients who prefer direct control over their infrastructure, we also provide an **on-premises solution**. This deployment mirrors the cloud service architecture, allowing clients to tailor the setup to their specific security and operational needs. The on-premises option ensures the same level of robust protection and control, adapted to fit within the client's unique environment.

PRACTICAL SECURITY ARCHITECTURE:
Virtual Private Cloud and Defense in Depth

Defense in Depth Strategy

Our approach utilizes a **Defense in Depth** strategy, layering multiple security measures:

- **Backend Access**: Restricted to technical and development staff for core service administration.
- **Frontend Access:** Controlled through a secure web portal for user data visualization.

Defense in Depth integrates **Multi-Factor Authentication (MFA),** VPNs, and firewalls to ensure only authenticated access, thereby reducing vulnerabilities.

Human Element and Continuous Monitoring

To further enhance cybersecurity, we conduct **risk assessments** and deploy automated safeguards to mitigate human error. Vulnerability management software, provided by our parent company Ingersoll Rand, continuously scans systems to identify and address potential risks. Additionally, our **Managed Detection and Response (MDR) service** delivers 24/7 security monitoring, detection, and rapid response capabilities.

This architecture, whether deployed in the cloud or on-premises, offers adaptable, resilient security that meets both high compliance standards and the unique needs of each client.

STRENGTHENING OUR CYBERSECURITY MEASURES

We’re excited to announce our partnership with the National Cyber Security Centre (NCSC), ensuring our solutions undergo rigorous PEN testing and compliance checks. From mandatory AES-encrypted LoRaWAN design and secure, segregated networks to SSL-encrypted communications, we’re committed to advancing cybersecurity at every level.

Working alongside approved bodies, Aircom and LoRaWAN represent a significant step forward in protecting critical infrastructure and providing a robust, secure environment.

IR Ingersoll Rand®

National Cyber Security Centre

VIBERT
Security Advisory

NIST
National Institute of Standards and Technology

aircom

YZ® SYSTEMS

To find out more about the Aircom end-to-end products,

Visit our ebsite
www.yzsystems.com/aircom

aircom

YZ®
SYSTEMS