frontiers | Frontiers in The Internet of Things

TYPE Review
PUBLISHED 04 December 2023
DOI 10.3389/friot.2023.1254160

OPEN ACCESS

EDITED BY
Nitin Auluck,
Indian Institute of Technology Ropar, India

REVIEWED BY
Sudeepta Mishra,
Indian Institute of Technology Ropar, India
Vidushi Agarwal,
Indian Institute of Technology Ropar, India

*CORRESPONDENCE
Raymond Chan,
Raymond.Chan@singaporetech.edu.sg

RECEIVED 06 July 2023
ACCEPTED 16 November 2023
PUBLISHED 04 December 2023

CITATION
Chan R, Yan WK, Ma JM, Loh KM, Yu T, Low MYH, Yar KP, Rehman H and Phua TC (2023), IoT devices deployment challenges and studies in building management system.
Front. Internet. Things 2:1254160.
doi: 10.3389/friot.2023.1254160

IoT devices deployment challenges and studies in building management system

Raymond Chan[1]*, Wye Kaye Yan[1], Jung Man Ma[1], Kai Mun Loh[1], Tan Yu[1], Malcolm Yoke Hean Low[1], Kar Peo Yar[1], Habib Rehman[2] and Thong Chee Phua[2]

[1]Singapore Institute of Technology, Infocomm Technology Cluster, Singapore, Singapore, [2]Firefish Communications, Singapore, Singapore

Deployment of IoT devices into an existing control system has increasingly become a new norm in recent years. Traditional approach of installing a new device into the system involves creating a separate network or infrastructure to ensure that the newly added devices do not affect the current system. However, this may not be the optimal solution for IoT devices, as they are designed to integrate and communicate with the existing systems. Therefore, it is important to understand how to properly deploy IoT devices and address the concerns of engineers. This research shares valuable experiences in deploying and integrating IoT devices into a campus Building Management System It covers considerations and requirements for the devices, as well as the deployment and integration challenges encountered during the process. These valuable experiences can serve as a useful reference for the industry when they need to install IoT devices in their infrastructure.

KEYWORDS

internet of things, building management system, MQTT, ZigBee, LoRaWAN frontiers

1 Introduction

The integration of Internet of Things (IoT) with traditional Operational Technology (OT) systems has garnered significant interest and attention in recent years. However, integrating IoT and OT systems or devices, or both, poses various challenges. These challenges encompass differences in operational methodologies between IoT and OT devices, the absence of standardized protocols, proprietary systems, isolated networks, and disparate databases.

IoT devices are designed for remote access, data processing, and data analytic, whereas OT devices are designed for real-time processing and control. This operational disparity makes it challenging to integrate and synchronize the two. Additionally, IoT and OT devices use different communication protocols, such as Hypertext Transfer Protocol (HTTP), MQ Telemetry Transport (MQTT), and ZigBee for IoT devices, while OT devices may utilize protocols like Modbus, Transmission Control Protocol/Internet Protocol (TCP/IP), and Long Range Wide Area Network (LoRaWAN). Hence, finding a common protocol that both systems or devices can use becomes imperative.

Furthermore, proprietary systems used by different vendors often run on vendor-specific hardware, software, and protocols, limiting interoperability and flexibility. While open-source solutions are frequently associated with IoT systems or devices, they often lack support and robustness. For instance, the platform on which proprietary systems run may

hinder the ability to upgrade and integrate open-source applications, rendering IoT systems or devices incompatible with existing setups. Isolated networks present another challenge, as different vendors use air-gapped networks, virtual local area networks (VLANs), and separate physical networks, restricting data sharing between systems and impeding bridging between them. Dissimilar databases used, as well as varying data storing and logging methods, pose additional challenges. IoT devices may utilize Not Only Structured Query Language (NoSQL) or Time Series Databases (TSDB), but also OT devices may use SQL Server or other databases recommended by vendors.

In light of these challenges and difficulties associated with integrating IoT and OT systems or devices, several administrative considerations must be addressed, particularly regarding the security aspect of systems from individual vendors when implementing them together. Scalability is another crucial consideration, as the proliferation of devices leads to larger volumes of data that need to be processed to derive efficient and effective insights. Therefore, the use of gateways, protocol translators, middle-ware, network monitoring and visibility tools, and a centralized management platform capable of integrating and bridging IoT and OT systems and devices, coupled with robust security policies and best practices, are necessary to ensure the integrity and security of the infrastructure. The lack of visibility in the growing number of connected devices introduces new attack vectors and security concerns, underscoring the importance of comprehensive security measures.

The objective of this research study is to understand and validate the deployment and integration challenges that IoT systems and devices have when integrating with an existing BMS infrastructure. A proof-of-concept (POC) central control system (orchestration platform) is set up as a centralized management platform for IoT and OT systems and devices in a lab. Then, with the real world knowledge and experiences gained, this will be applied on a larger scale (building and campus-wide) in the future. This research aims to address the question of how to appropriately select the connection for various types of IoT devices for BMS.

The rest of this work will be organized as follow: Section 2 discusses the related work on IoT deployments. Section 3 describes this initiative of installing IoT devices in our laboratory and campus. Section 4 introduces the deployed devices and how those devices are connected to the network. Section 5 covers the integration consideration when connecting the IoT devices to the existing control systems. Section 6 gives a conclusion of the work.

2 Related work

There are lots of research work discuss the deployment-related issue of IoT devices. Samie et al. (2016) conducted a survey on different technologies in IoT development. Smart Building is mentioned as one of the domains which could benefit from IoT applications. A summary of the suitability of communication technologies for IoT application domains in smart buildings was presented. Pereira et al. (2020) group the IoT devices under passive, semi-passive and active. The main design challenges which could impact the deployment of IoT devices was described, focusing on power and connectivity. Zikria et al. (2019) discussed on what are the key features and characteristics of some commonly used IoT Operating Systems (OS), and the considerations users should take note of when using it. Lam and Chi (2016) discussed the identity of IoT, and what are some of the security concerns IoT devices and applications have. Yu et al. (2016) proposed a cloud-based building management system which can selects an optimum device feature subset from the computing resources and storage. Minoli et al. (2017) reviewed technical opportunities and technical challenges faced by the IoT in the smart building arena. Fraile et al. (2020) proposed a IoT-enabled school building system using LoRa-based networking. Harkare et al. (2021) implemented a IoT parking management system, which is a subset of BMS.

Although the existing works mentioned different types of IoT installation challenges and use a specific protocol for the deployment. It might be insufficient for designing a solution to address the installation challenges and the inter-connectivity between protocols. Therefore, we need to have real experiences of installing IoT devices to the BMS and verify the challenges mentioned will affect the system or not.

3 Background of Advance Cybersecurity Lab

As shown in Figure 1, deployment of IoT devices and applications have been done in a lab (Advance Cyber Security Lab, also known as ACSL) whereby, existing systems from a BMS were used. IoT devices are integrated into the setup to provide support to OT devices and systems, whereas IoT applications provide “Smart” features such as remote capabilities. A central control system is integrated into the architecture to provide a means for monitoring, controlling, and processing of data from IoT and OT devices. New security features are introduced into the system to ensure that the new vulnerabilities and risks which IoT applications bring about are minimized. Further details on the deployment and integration challenges are discussed in section 4.

As shown in Figure 2, it displays the real-time data collected from a diverse array of connected IoT sensors, OT devices and systems deployed in the Advance Cybersecurity Lab. This visual representation provides an overview of all sensor data, allowing for a comprehensive understanding of the monitored environment.

4 Deployment, integration challenges and experiences

This research describes the deployment of IoT devices in a BMS, the integration challenges and experiences garnered from the research. In this section, deployment, integration challenges and experiences for different communication protocols are discussed.

4.1 Device data refresh rate

IoT system involves a large number of connected sensors which generate a huge amount of data. These data are captured in almost real-time and arrive in intervals dependent on the devices’ capability used, and are variable in terms of structure. The volume of data

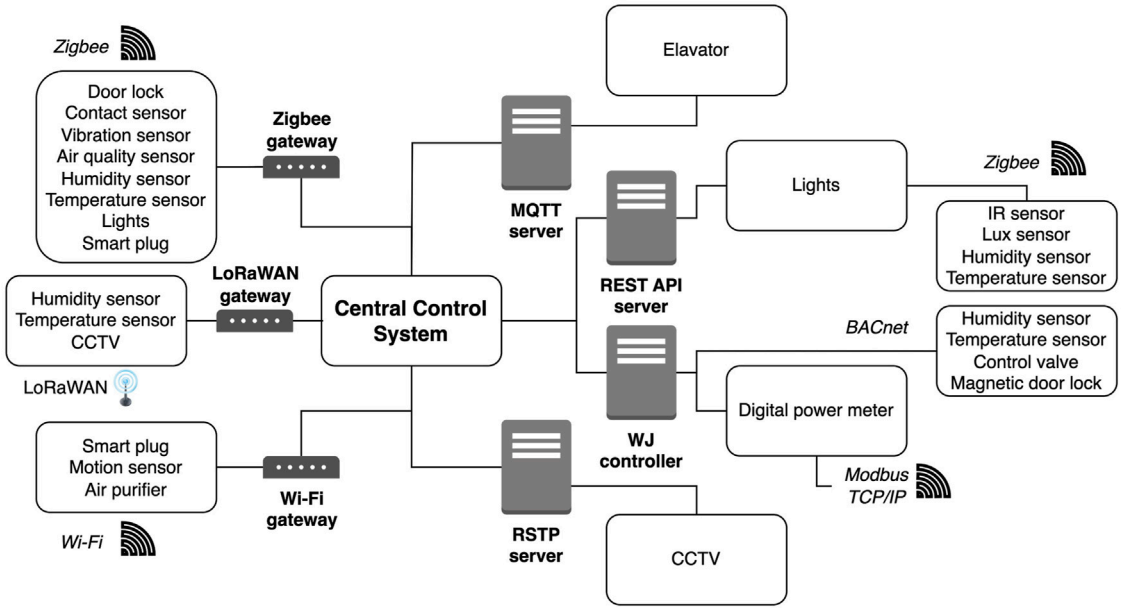

FIGURE 1
BMS with IoT devices Architecture.

generated by IoT devices can be overwhelming and it is important to have a system that can handle and process the large volume of data in real-time.

For instance, Salman et al. (2015) discusses on the different IoT protocols and standards. Zigbee devices can send data packets ranging from a few kilobits per second (Kbps) to hundreds of Kbps, allowing command and control messages, and sensor data transmission to be done every second. Whereas LoRaWAN devices have a lower data rate compared to Zigbee devices. LoRaWAN devices send data packets ranging from a few hundred bits per second (bps) to tens of Kbps. Therefore, depending on the application the LoRaWAN device is used for, the sending rates can vary vastly from anywhere between 5 s and 15 min with its data compressed. As concluded by Al-Sarawi et al. (2017), there is no perfect IoT device but only which technology is the best one for the required application. In Table 1, the data rate of different protocols used in the setup are further elaborated. It is important to note that the data rate is based on the devices and application in the setup, and may vary for other devices and applications of the same type.

The IoT devices utilize the industrial, scientific and medical (ISM) bandwidth for wireless communications. For example, Zigbee typically uses 2.4 GHz band. Across these channels, every Zigbee device occupies a bandwidth of up to 2 MHz while any two different channels are separated by a guard band of 5 MHz to prevent interference due to other Zigbee devices. At 2.4 GHz, the ISM bandwidth is 100 MHz. Hence, for a collision free transmission without employing any spread spectrum method, only a maximum of 14 Zigbee devices can be supported. In practice, most IoT devices will use frequency hopping spread spectrum (FHSS) technique to avoid interference from other wireless devices operating in the same frequency band. However, collision in the sub band is still unavoidable with FHSS. With channel coding, the IoT devices can tolerate some collisions among the frequency sub band. But as the number of devices increase exponentially, it will exceed the threshold and result in frequent re-transmission and lower the through put. Thus, effectively bring down the average data rate of the IoT devices and result in it failure to provide real-time data.

4.2 Connection protocols

4.2.1 Zigbee devices

Zigbee is based on IEEE 802.15.4 and is created by the Zigbee Alliance. Zigbee is a wireless standard intended for short-range integration of low-power, low-data rate devices. Samie et al. (2016) The Zigbee coverage range is usually 10–100 m which is suitable for short-range connections. This limitation makes it challenging to scale the application of Zigbee devices without adding more nodes to the Zigbee mesh network, and with nodes implemented, there may be more vulnerabilities and risk. Another challenge when deploying Zigbee devices is network coverage, especially in buildings with thick walls or interference-prone environments. Due to the nature of the 2.4 GHz frequency band used by Zigbee, which is also shared with other devices such as Wi-Fi routers and Bluetooth devices, which can cause interference and affect the signal quality and range, making it challenging to establish a robust and reliable network throughout the whole building.

In the setup deployed in ACSL, a Zigbee gateway has been integrated into the system to enable wireless communication through Zigbee. Several Zigbee devices, such as air quality sensors, light bulbs, contact sensors, door locks, and vibration sensors, have been deployed. In most cases, Zigbee devices are easy to integrate and do not require extensive configurations during deployment. Zigbee devices are generally low-power consumption devices, often operating on batteries. However, it is important to note that battery-operated Zigbee devices may not have

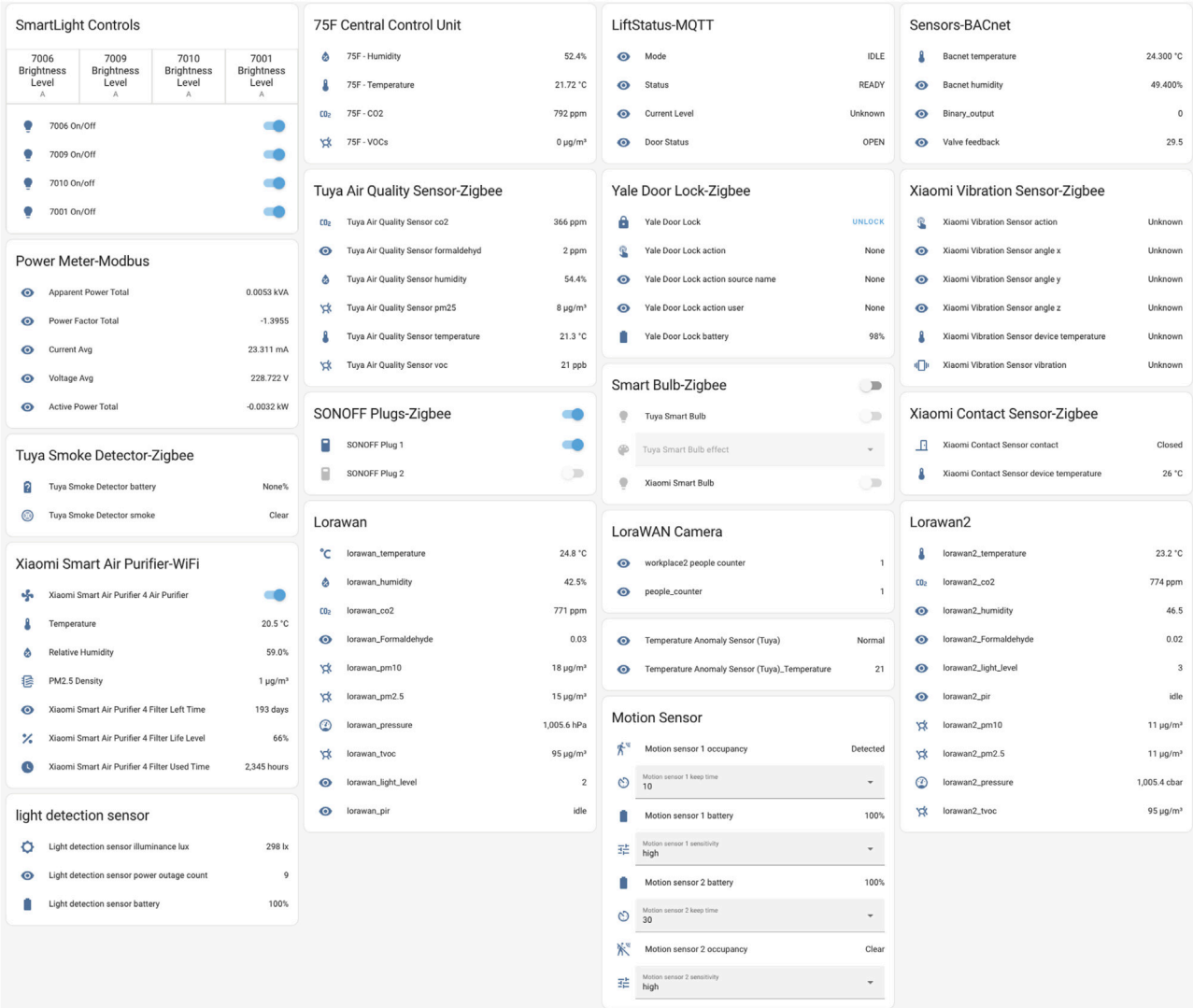

FIGURE 2
Real-time IoT sensor readings.

TABLE 1 IoT devices data refresh rate.

Application	Protocol	Communication type	Message format	Bandwidth usage	Sending rate
IoT (Door lock, Contact sensor, Vibration sensor, Air quality sensor, Humidity sensor, Temperature sensor, IR sensor, Lux sensor, Lights, Smart plug)	Zigbee	Wireless	Custom	Low	Every second
General purpose (Air purifier, Motion sensor, Smart plug)	Wi-Fi	Wireless	IP based	High	Every second
IoT (Humidity sensor, Temperature sensor, CCTV)	LoRaWAN	Wireless	Binary	Low	Every 5 to 300 s
Web API (Lights)	RESTful	HTTP	JSON, XML	High	Every 1 to 30 s
IoT, M2M (Elevator, Brigded Zigbee devices)	MQTT	Publish-Subscribe	Binary	Low	Every second
Industrial (Digital power meter)	Modbus	TCP/IP	Binary	Medium	Every second
Building Automation (Humidity sensor, Temperature sensor, Control valve, Magnetic door lock)	BACnet	Ethernet/RS-485	Binary	Medium	Every second

a function to monitor the lifespan of the battery. Therefore, manual intervention is required to keep track of the device's battery lifespan. This becomes a challenge when multiple Zigbee devices are battery-operated, as the devices may consume power at different rates, affecting the reliability of the system.

4.2.2 Wi-Fi devices

Wi-Fi is another commonly used wireless communication protocol for IoT and industrial applications. Similar to the Zigbee communication protocol, Oughton et al. (2021), it operates in the 2.4 GHz frequency band. Unlike Zigbee, the coverage range of Wi-Fi is dependent on access points or routers. Therefore, there are various ways to extend the coverage area, such as implementing Wi-Fi extenders into the network. However, although Wi-Fi is capable of covering a wide area, due to the architecture of most systems, networks and systems are often isolated from each other. Thus, it may be challenging to integrate Wi-Fi devices into multiple systems.

Wi-Fi devices, such as air purifiers and smart plugs, have been deployed in the setup at ACSL. Apart from the challenge of isolated networks, the connectivity of Wi-Fi devices is also a challenge. In most cases, Wi-Fi devices communicate with the cloud, which means that control and access may be limited as these cloud services are often managed by third-party providers. Consequently, ensuring these devices' security, support, and maintenance becomes challenging. Based on experience, this becomes an issue as the downtime of a particular device may affect the system and limit the functionality of the central control system.

4.2.3 LoRaWAN devices

Deploying IoT devices in remote or inaccessible locations can pose a significant challenge during IoT deployment. For example, it is common for power meters and switch rooms to not have access to Ethernet which can make it difficult to deploy IoT devices for remote monitoring. To address this issue, LoRaWAN is often used for remote monitoring of such scenarios. As discussed in Loukil et al. (2022), the choice of frequency for LoRaWAN deployments can vary depending on the country or region. European operates in the 863–870 MHz (MHz) frequency band, while US operates in the 902–928 MHz frequency band, and Asia operates in the 920–923 MHz frequency band, South Korea operates in the 920–923 MHz frequency band, and India operates between 865 and 867 MHz. In the setup deployed in ACSL, a 923 MHz LoRaWAN gateway has been integrated into the system to enable wireless communication through LoRaWAN. In some cases, LoRaWAN gateways are required to communicate with the cloud before transmitting the data to a platform or application. This adds an additional communication layer to the LoRaWAN setup, and another network reliability concern for operators. Therefore, in this setup, a LoRaWAN gateway which is able to process data locally without having to relay to a cloud is used, and is the recommended way.

Another challenge is LoRaWAN signal strength and reliability, Adelantado et al. (2017). An air quality sensor and smart closed-circuit television (CCTV) are deployed and tested in remote areas without wired and wireless communications. In theory, LoRaWAN devices can communicate up to 7 km. However, in actuality, this is a challenge as the range will depend on both the device and gateway. Both the device and gateway must have a strong and reliable signal to achieve longer distances, and environmental factors may affect the signal strength as well. Therefore, it is important to note that when deploying LoRaWAN devices, signal quality must be tested.

4.3 Communication protocols

4.3.1 RESTful devices

Representational state transfer or RESTful protocol is a commonly used IoT communication protocol due to the simplicity, scalability and familiarity of HTTP. As reviewed by Maurya et al. (2021). RESTful systems use a client-server model, data from devices and systems are identified by a unique Uniform Resource Locator (URL). Device capabilities are a challenge of RESTful devices. The limited memory and processing power of IoT devices may constrain the resources of the devices by constructing and parsing HTTP requests and responses. This led to the other challenge of RESTful devices, latency and reliability. As resources are limited, certain HTTP requests and responses require more memory and processing capabilities therefore, latency may incur, thus, affecting the operational functionality of the system.

In the setup deployed in ACSL, because of these challenges, the reliability of the data from RESTful devices is affected due to the latency. However, not all HTTP requests and responses have the same latency issues. Therefore, it is important to validate the HTTP request and responses. Another challenge faced when using RESTful devices is with regard to the connectivity of the RESTful server. In the setup, the RESTful Application Programming Interface (API) server is deployed in a separate server from the central control system. This makes it challenging when determining the uplink of the RESTful API server with the central control system. Thus, security features that monitor the status of RESTful devices and systems must be implemented.

4.3.2 MQTT devices

MQTT is a lightweight data streaming standard often used in IoT applications. It is based on publish-subscribe networks that transport messages from devices to an MQTT broker (server), Al Enany et al. (2021). In the setup deployed in ACSL, an elevator system has been made "smart" by integrating it with an MQTT broker. For MQTT, one of the security concerns of the MQTT broker, whether there are any protection to prevent cyber attack. Therefore, it is imperative to have security features that monitor for possible attacks, and vulnerabilities of MQTT. A compromised MQTT broker could allow malicious actors to control the smart elevator system, which could lead to serious safety and security risks.

Another challenge is with regard to interoperability between the client and the broker of MQTT as discussed by Spohn (2022). The MQTT broker for the elevator system is deployed on a separate server from the central control system. Therefore, in the event that the broker for the elevator system is under attack from malicious actors or has vulnerabilities, the central control system may not be notified of such events. Thus, security features such as device inactivity monitoring, and up-link monitoring, amongst others on the client side must be implemented as well.

4.3.3 Modbus devices

In the setup deployed in ACSL, data from a power meter is retrieved using the Modbus protocol. The Modbus communication protocol is a traditional and widely used protocol in industrial applications, providing master/slave communications across buses and networks. Fovino et al. (2009) Specifically, Modbus TCP/IP is used in this setup. By leveraging Modbus TCP/IP, a seamless connection is established, and remote capabilities are provided to the power meter for retrieval of sensor data such as voltage, current, active power, apparent power, and power factor. This data provides valuable insights into the power consumption and performance of the monitored system.

A challenge of Modbus devices is deciding on which communication protocol to use, Modbus TCP/IP or Serial Modbus. Based on the experiences from the setup, although Modbus TCP/IP provides remote capabilities, there is a limit to how many master/slave connections that can be established. Therefore, the more complex (too many master devices) the system is, Modbus TCP/IP may not be the favorable communication protocol to use. However, Serial Modbus may not be the solution as well as it can be challenging to bridge it to a common communication protocol such as MQTT in the system. Therefore, if there are multiple devices using Modbus as its communication protocol, a possible solution would be to use another device to support the intended application. For instance, a LoRaWAN power meter can be used to monitor the energy consumption of the Modbus device.

4.3.4 BACnet devices

Building Automation and Control Networks, also known as BACnet is a widely used industrial protocol in building automation systems. It is designed to facilitate the exchange of data between building devices and systems. Some commonly used devices and systems such as heating, ventilation, and air conditioning (HVAC), lighting, access controls, and more are often connected to a BACnet server. Although BACnet provides interoperability between devices and systems, based on the experiences from the setup in the ACSL, compatibility with modern IoT devices is a challenge as most of the devices and systems integrated into the BACnet server are legacy systems. Therefore, it is a challenge to scale older systems whilst integrating new devices.

Another challenge of using BACnet devices is with regard to the upkeep of it. Like the research conducted by Clauß et al. (2023), building devices and systems evolve over time, and managing and maintaining those devices and applications can be difficult. Especially in this case whereby, the BACnet devices which are connected to the BACnet server are operating on a separate server. For instance, a server for lighting, and another for access controls. It becomes even more challenging when the control and management of devices and systems are on another server such as the central control system.

5 Platform integration consideration

With the successful deployment and integration of IoT devices in the ACSL, this section discusses the considerations that building operators, managers, and third-party providers, amongst others, should take into account before deploying or integrating IoT devices into their systems. In this section, various considerations can be applied at the different stages of deployment: pre, post, and during deployment. Each of these insights has been garnered from the experiences gained in the different stages of deployment throughout the research, also included are other studies with relation to the insights that may be considered when deploying and integration IoT devices and systems.

5.1 Vendor diversity

Traditionally, BMS consist of multiple systems supplied by different vendors, creating a major challenge. In some cases, vendors may be unwilling to integrate their systems with others due to competition or potential conflicts. To overcome this challenge, it is crucial to identify potential conflicts between systems and understand their complexities. Each system must be thoroughly understood, including communication protocols, data formats, and operational requirements. Working closely with vendors and gaining a deep understanding of their systems is essential to ensure the smooth and optimal performance of the BMS. Successful integration can improve building management efficiency and lead to long-term operational cost reduction.

5.2 Reliability

The reliability of IoT devices is crucial when deploying or integrating them with existing and new systems. As these devices have a direct impact on the daily operations of end-users, it is important to consider the following considerations before deploying or integrating in actual operational settings.

5.2.1 Interoperability

As mentioned in the section with regards to vendor diversity, IoT devices and systems are often from different vendors and may have different communication protocols, making the interoperability of these devices and systems challenging for building operators. Furthermore, IoT devices and systems may use different data formats, which makes it difficult to consolidate data, share data and access the functionality of IoT applications. Interoperability is critical for the success of IoT applications. Overcoming these challenges will lead to enhanced system performance, flexibility, scalability, and the effectiveness of building management will be greatly improved.

5.2.2 Security

IoT devices are vulnerable to security threats such as hacking, which can be exploited to attack other devices, networks, and systems, resulting in system malfunction or failure in some cases. The more IoT devices are integrated, the more new vulnerabilities and risks will be introduced into the systems. Therefore, security is a critical aspect of implementing an integrated platform, and security measures must be in place to ensure the reliability of the system, as multiple IoT devices and systems are involved. By enhancing the security features in the overall architecture of the BMS, data breaches, financial losses, and physical harm, among others may be prevented.

Studies conducted by Koivu et al. (2016) and Minoli et al. (2017) discuss some security considerations under specific conditions with relation to IoT devices and systems. Building operators, managers, and third-party providers, amongst others, may take note of this consideration when integrating and deploying IoT devices and systems to further enhance the security aspect of the overall architecture.

5.2.3 Connectivity

Buildings are usually built upwards or across a large plot of land. Therefore, network wiring is a challenge when integrating with BMS. In many cases, the multiple BMSs are located in different parts of a building, and connecting them can be difficult. IoT and OT devices may differ in connectivity technologies and require a reliable network connection to communicate with other devices or systems, and with the cloud for some devices. Network connectivity issues can cause system downtime, affecting end users. Therefore, a stable network connection is essential to ensure reliable communication between devices and systems.

In the setup, due to the variety of devices and applications used, there are multiple connection and communication protocols to account for to establish a reliable network infrastructure. This may be increasingly challenging as well as some devices and applications from different vendors may operate different from those that the general public can use. To further understand the connectivity techniques of IoT, a study by Ahmad et al. (2019) reviews of different IoT connectivity technologies and how to select the right one for different applications.

5.2.4 Power consumption

Many IoT devices are battery-operated, giving them the flexibility to be deployed in more constrained locations. However, the reliability of the device may affect daily operation due to the limited battery life. In some cases, IoT devices are non-battery operated, and can be connected to an external power source. This is also a challenge as most IoT devices are often designed to be low-power consumption devices. Therefore, when deployed side by side with OT devices and systems, the power source may not be compatible. Minoli et al. (2017), optimizing power consumption is critical to prolonging the device lifespan (up-time) and reducing maintenance costs, and ensuring that the IoT device is operationally reliable.

5.2.5 Environmental factors

The built of IoT devices are generally not as sturdy as OT devices. Therefore, environmental factors of the location the devices are deployed in will affect the reliability of the device. Harsh conditions such as temperature and humidity in switch rooms, and server rooms may affect how IoT devices operate. Vibration and shock in a generator room may reduce the performance, and lifespan of the IoT device exponentially. Selecting the right device for specific environmental conditions is crucial for deployment, particularly those used in harsh or remote environments.

5.3 Scalability

The Scalability of IoT devices and applications can be factored into several considerations. It is important to take note of these considerations as they may impact the system when existing and new devices and systems for buildings evolve over time.

5.3.1 Device management

In most cases, IoT devices are used to support existing OT devices and systems to enhance the overall functionality of the intended application. However, as the number of IoT devices deployed increases, managing and monitoring the increased number of devices can become a challenge, and has a direct effect on how configurations and firmware updates are managed, device and system health is monitored, security and access control rights are given, and life cycle management of devices.

5.3.2 Data processing and storage

As more devices are deployed and integrated, the volume of data generated also increases. Scalability becomes a challenge when systems cannot keep up with the volume of data. Overcoming this challenge helps make sense of the vast amount of raw data, including sensor readings, logs, and events. This enables real-time processing and analysis for IoT applications to execute immediate actions or timely decision-making decisions.

5.3.3 Network capacity

IoT devices rely on wireless networks to communicate with other devices, systems, and the cloud. The network capacity must be able to handle the increased traffic with the increased number of devices deployed. As there are multiple communication protocols used, existing or new bandwidth constraints may affect the integration of IoT devices. Thus, the protocol efficiency of IoT applications such as Wi-Fi, Bluetooth, and Cellular, among others may be affected. Ensuring that the network infrastructure is designed to handle large volumes of data is essential to prevent potential bottlenecks and latency issues.

5.4 Administrative considerations

There are many administrative considerations to take into account. Whether the deployment, and integration of IoT devices and applications are for testing or operational usage, different considerations must be taken. This section discusses some of the administrative considerations garnered from the experiences gained from the setup.

5.4.1 Governance and stakeholder

Deployment of IoT applications often involves multiple stakeholders. Externally, they may include technology providers, manufacturers, network providers, data storage providers, amongst others. Similarly, internally there may be technology operators, network operators, data owners, and regulatory bodies. Oftentimes, multiple vendors are involved in different components of the project. Coordinating and managing multiple stakeholders is essential to achieving the desired outcomes for pre-deployment, post-deployment, and during the deployment of IoT applications. By establishing clear communication channels, and collaborative frameworks between stakeholders, it ensures that regulatory compliance is met, and security concerns are aligned with the business model across multiple parties.

5.4.2 Compliance

The integration and deployment of devices are subjected to various regulations and standards, depending on both industry and geographical locations. Some common regulations to adhere to are: Data Privacy, Industry Specific, and Wireless Spectrum, amongst others. Data Privacy regulations concern the collection, processing, and storage of personal data and data generated by devices. Industry Specific regulations may differ as the target audience can be different. For instance, healthcare and manufacturing industries will have different operational needs, therefore, different industry-specific regulations to adhere to. IoT applications often rely on wireless communication protocols such as Wi-Fi, cellular, and other Wide Area Networks (WANs) therefore, wireless spectrum regulations must comply to geographical locations.

5.4.3 Ownership and privacy

As the use of these devices involves collecting and processing data from sensors, devices, and end-user interactions, data ownership, and data governance policies are imperative in addressing privacy concerns for users. IoT applications often involve sharing of data with third-party services such as cloud providers or integrating with other systems locally which may be from different vendors. Therefore, it is best practice to evaluate the data before sharing it with other parties. Personal Data Protection Act (PDPA) or Personal Identifiable Information (PII) is also a common concern of users. Anonymization of the data by employing techniques such as data masking, encryption, or tokenization amongst others may prevent specific details of an individual from being revealed. By having a clear policy for ownership and privacy, organizations can build trust with users, and maintain compliance.

5.4.4 Support and maintenance

IoT deployment requires continuous support and maintenance to ensure the reliability, and efficiency of daily operations. The visibility of devices and systems is crucial in ensuring that the deployed devices and systems are in operational condition. Therefore, measures to monitor the health, connectivity, and lifespan status such as battery status, amongst others must be implemented. Firmware updates and patch management is another consideration operators must have. System administrators must log all best working versions of devices and systems, and take responsibility for ensuring that the devices and systems are functioning as intended. In some cases, a third-party provider is involved in the deployment. Therefore, clear directives for support and maintenance must be drawn up to ensure that the third-party providers adhere to the operational needs.

6 Discussion

The experiment was conducted in a controlled environment to evaluate the integration and deployment of IoT devices, applications, and protocols with existing OT devices and systems of a BMS. Typically, it involves integrating, configuring, and testing IoT devices, applications, and protocols into the existing BMS infrastructure. The duration of the experiment vary significantly depending on the connection, and communication protocols. IoT devices, and applications are integrated, configured, and tested in batches, grouped by the connection or communication protocol used. The duration for each batch may vary from a few weeks to several months, depending on factors such as the number of devices, devices from different manufacturers, interoperability, and complexity of applications for specific use cases involved with the underlining connection or communication protocol.

Throughout the experiment, several challenges and issues were encountered. For example, compatibility issues between new and existing devices, problems with network connectivity, data management, and security vulnerabilities were identified. Certain Zigbee devices connected directly to the central control system or bridged to MQTT communication protocol had security vulnerabilities, which is related to the lack of periodic communication using the Keep Alive feature. To address these vulnerabilities, a POC monitoring system was implemented in the central control system. The docker container-based monitoring system was designed to detect common vulnerabilities such as brute force attacks, denial of service, and flooding. Additionally, a custom feature was integrated into the monitoring system to detect device inactivity and alert operators when a device remained inactive for an extended period outside its normal operational patterns.

To avoid using devices that may not suit the operational needs of the setup, and security vulnerabilities that may come with the integration of new devices, it is crucial to integrate and test the devices, and applications before deploying for operational usage. This will minimized issues that may arise in the future. It gives operators a better understanding of the devices, and protocols used for creating a more efficient infrastructure.

7 Conclusion and future work

In conclusion, this manuscript discusses various factors to consider when deploying IoT devices. It draws insights from real-world experiences and the challenges encountered during such deployments. After thoroughly evaluating and validating these challenges, it is essential to take into account the factors discussed in this manuscript before planning any IoT deployment.

The discussion includes different wireless communication protocols for IoT. It is acknowledged that there is not a single protocol that can meet all requirements simultaneously, like short-range and long-range communication abilities, transfer speed, lightweight messaging, and low latency.

Hence, having a good understanding of the pros and cons of different IoT protocols is crucial. This understanding helps combine their strengths to optimize IoT deployment. It is also important to know why you're deploying an IoT device and integrating it into an existing system. For instance, deploying IoT devices in buildings requires careful thought and understanding of the characteristics and capabilities of each IoT communication protocol. By using the right protocols and devices, building owners and operators can create a strong and efficient IoT network tailored to their system's needs.

The rapid growth of the smart home and building sector has led to many competing standards and protocols, causing challenges.

The diversity of IoT communication protocols has made it hard to seamlessly integrate and make different devices work together. Matter aims to solve these problems by creating a new smart home standard. This standard seeks to bring unified control, enhance security, and establish more reliable connections for smart homes.

In future work, our focus will be on studying the Matter protocol and how it fits into building environments. We'll evaluate how well Matter performs, how it handles data transmission, and what potential security risks it might introduce. This evaluation will be conducted as we move from lab setups to larger, campus-wide IoT integrated systems.

Author contributions

RC: Writing–original draft, Writing–review and editing. WY: Writing–original draft, Writing–review and editing. JM: Writing–original draft, Writing–review and editing. KL: Writing–original draft. TY: Writing–original draft. MYHL: Writing–review and editing. KY: Writing–review and editing. HR: Writing–review and editing. TP: Writing–review and editing.

Funding

The authors declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

The author (MYHL) declared that they were an editorial board member of Frontiers at the time of submission. This had no impact on the peer review process and the final decision.

Publisher's note

References

Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melia-Segui, J., and Watteyne, T. (2017). Understanding the limits of lorawan. *IEEE Commun. Mag.* 55, 34–40. doi:10.1109/mcom.2017.1600613

Ahmad, M., Ishtiaq, A., Habib, M. A., and Ahmed, S. H. (2019). A review of internet of things (iot) connectivity techniques. *Recent trends Adv. Wirel. IoT-enabled Netw.*, 25–36. doi:10.1007/978-3-319-99966-1_3

Al Enany, M. O., Harb, H. M., and Attiya, G. (2021). "A comparative analysis of mqtt and iot application protocols," in 2021 International Conference on Electronic Engineering (ICEEM) (IEEE), USA, 3-4 July 2021 (IEEE).

Al-Sarawi, S., Anbar, M., Alieyan, K., and Alzubaidi, M. (2017).Internet of things (iot) communication protocols, *2017 8th Int. Conf. Inf. Technol. (ICIT)*. China, IEEE, 685–690. doi:10.1109/ICITECH.2017.8079928

Clauß, J., Caetano, L., Skeie, K. S., and Svinndal, Å. B. (2023). "Practical challenges towards data-driven applications in buildings: lessons-learned from two real-life case studies," in 2023 8th International Conference on Smart and Sustainable Technologies, China, 20-23 June 2023 (SpliTech IEEE).

Fovino, I. N., Carcano, A., Masera, M., and Trombetta, A. (2009). "Design and implementation of a secure modbus protocol," in Critical Infrastructure Protection III: Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, New Hampshire, USA, March 23-25, 2009 (Springer), 83–96.

Fraile, L. P., Tsampas, S., Mylonas, G., and Amaxilatis, D. (2020). A comparative study of lora and ieee 802.15. 4-based iot deployments inside school buildings. *IEEE Access* 8, 160957–160981. doi:10.1109/access.2020.3020685

Harkare, A., Potdar, V., Mishra, A., Kekre, A., and Harkare, H. (2021). "Methodology for implementation of building management system using iot," in *Evolutionary computing and mobile sustainable networks: proceedings of ICECMSN 2020* (China: Springer), 939–948.

Koivu, A., Koivunen, L., Hosseinzadeh, S., Laurén, S., Hyrynsalmi, S., Rauti, S., et al. (2016). Software security considerations for iot. In IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart 22-25 Aug. 2022, USA, Data (SmartData) (IEEE, 392.

Lam, K.-Y., and Chi, C.-H. (2016).Identity in the internet-of-things (iot): new challenges and opportunities, Information and Communications Security: 18th International Conference, ICICS 2016, Singapore, Singapore, November 29–December 2, 2016, Germany, 18. Springer, 18–26.

Loukil, S., Fourati, L. C., Nayyar, A., and Chee, K.-W.-A. (2022). Analysis of lorawan 1.0 and 1.1 protocols security mechanisms. *Sensors* 22, 3717. doi:10.3390/s22103717

Maurya, R., Nambiar, K. A., Babbe, P., Kalokhe, J. P., Ingle, Y., and Shaikh, N. (2021). Application of restful apis in iot: a review. *Int. J. Res. Appl. Sci. Eng. Technol.* 9, 145–151. doi:10.22214/ijraset.2021.33013

Minoli, D., Sohraby, K., and Occhiogrosso, B. (2017). Iot considerations, requirements, and architectures for smart buildings—energy optimization and next-generation building management systems. *IEEE Internet Things J.* 4, 269–283. doi:10.1109/jiot.2017.2647881

Oughton, E. J., Lehr, W., Katsaros, K., Selinis, I., Bubley, D., and Kusuma, J. (2021). Revisiting wireless internet connectivity: 5g vs wi-fi 6. *Telecommun. Policy* 45, 102127. doi:10.1016/j.telpol.2021.102127

Pereira, F., Correia, R., Pinho, P., Lopes, S. I., and Carvalho, N. B. (2020). Challenges in resource-constrained iot devices: energy and communication as critical success factors for future iot deployment. *Sensors* 20, 6420. doi:10.3390/s20226420

Salman, T. (2015). *Internet of things protocols and standards*.

Samie, F., Bauer, L., and Henkel, J. (2016). "Iot technologies for embedded computing: a survey," in *Proceedings of the eleventh IEEE/ACM/IFIP international conference on hardware/software codesign and system synthesis* (USA: IEEE), 1–10.

Spohn, M. A. (2022). On mqtt scalability in the internet of things: issues, solutions, and future directions. *J. Electron. Electr. Eng.*, 4. doi:10.37256/jeee.1120221687

Yu, J., Kim, M., Bang, H.-C., Bae, S.-H., and Kim, S.-J. (2016). Iot as a applications: cloud-based building management systems for the internet of things. *Multimedia Tools Appl.* 75, 14583–14596. doi:10.1007/s11042-015-2785-0

Zikria, Y. B., Kim, S. W., Hahm, O., Afzal, M. K., and Aalsalem, M. Y. (2019). Internet of things (iot) operating systems management: opportunities, challenges, and solution. *Sensors* 19, 1793. doi:10.3390/s19081793