Security-Enhanced Orchestration Platform for Building Management Systems

Raymond Chan[1(✉)], Wye Kaye Yan[1], Jung Man Ma[1], Kai Mun Loh[2], Tan Yu[1], Malcolm Low[1], Habib Rehman[3], and Thong Chee Phua[3]

[1] Singapore Institute of Technology, Singapore, Singapore
Raymond.Chan@singaporetech.edu.sg
[2] University of Glasgow, Glasgow, UK
[3] Firefense, Singapore, Singapore

Abstract. A building management system is an infrastructure asset that operates critical building components such as water supply management, electric power monitoring and heating, ventilation and air conditioning systems. Internet of Things devices are increasingly employed in building management systems for efficient operations. The Message Queuing Telemetry Transport protocol is commonly used for communications when integrating these devices. However, each device is typically isolated and has its own platform and management dashboard. The isolation and heterogeneity hinder device visibility and render it challenging to monitor and respond to abnormal conditions, including those induced by cyber attacks.

This chapter describes a security-enhanced orchestration platform for building management systems. The orchestration platform receives a variety of data from building systems and Internet of Things devices to provide situation awareness and support efficient operation. The integration of novel device auto-recovery and auto-isolation functionality in the orchestration platform enables the monitoring and mitigation of cyber attacks.

Keywords: Building Management Systems · Internet of Things Devices · Security-Enhanced Orchestration Platform

1 Introduction

A building management system incorporates several industrial control systems that manage critical electric power control, water and gas supply, elevator operation, access control and fire alarming and suppression systems. However, the various systems, which are tied to specific products and services, are often deployed separately and are isolated from each other because they are installed and managed by different providers. In fact, most providers do not recommend connecting their systems to other systems for latency and performance reasons [10].

Published by Springer Nature Switzerland AG 2024
J. Staggs and S. Shenoi (Eds.): ICCIP 2023, IFIP AICT 686, pp. 164–176, 2024.
https://doi.org/10.1007/978-3-031-49585-4_8

The use of Internet of Things (IoT) devices and sensors in building management systems has increased in recent years, making buildings smarter and more efficient [13]. However, the devices and sensors increase the cyber attack surfaces and render buildings more vulnerable to cyber attacks. An adversary who compromises a building access control system can gain entrance and steal items or destroy property without breaking physical locks. Closed-circuit television (CCTV) systems can also be compromised surreptitiously to perform malicious acts.

To address these and other security issues, orchestration platforms are required for building management systems to perform monitoring, control and threat and anomaly detection and response. An orchestration platform integrates diverse operational technology (OT) and information technology (IT) systems along with Internet of Things devices and sensors to facilitate efficient and secure building operation.

This chapter describes a security-enhanced orchestration platform for building management systems. The platform receives data from diverse building management system components and Internet of Things devices to provide situation awareness and support efficient and stable building operation. The integration of novel device auto-recovery and auto-isolation functionality enables the orchestration platform to monitor cyber attacks and mitigate their negative effects.

2 Related Work

In recent years, the building management system industry has been exploring the possibility of integrating legacy systems and devices in a single platform that collects building sensor data and efficiently controls the various building systems.

Agarwal et al. [1] have developed BuildingDepot, an extensible and distributed architecture for building data storage, access and sharing. The architecture leverages the representational state transfer application programming interface (REST API) to access sensor networks in a building. Their subsequent BuildingDepot 2.0 platform [14] provides advanced data analysis and supervisory control features. It enables reusable applications to be employed in different building environments and provides a template that describes sensors and building systems in a common language.

Alsuhli and Khattab [2] have proposed an Internet of Things architecture for building management that controls lighting and heating, ventilation and air conditioning systems. They proceeded to implement a prototype system and evaluate its accuracy and efficiency.

Due to their vital building monitoring and control functionality, it is important to secure building management systems from cyber attacks. Fisk [6] notes that legacy systems elevate risk because they have limited computing power and many known vulnerabilities that are still unpatched. Chan et al. [4] have identified vulnerabilities in smart lighting systems and energy metering systems. The increased use of Internet of Things devices with legacy systems expands the attack surface of building management systems. Brooks [3] has investigated current and emerging security vulnerabilities in automated building systems. The results reveal that using wireless devices in open architectures with extended system communications significantly elevates the cyber risk to building management systems.

Much of the research literature has focused on capturing and sharing sensor data from diverse building systems. However, due to the increased risks posed by legacy systems and the integration of Internet of Things devices in a building management system, a security platform must be implemented to monitor real-time data and ensure system integrity. Kalaska and Czarnul [9] conducted a security evaluation of available Internet of Things platforms covering device authorization, data filtering, access control and protecting against service threats. According to the evaluation, few platforms support device authorization and limited protection is provided against network attacks, especially denial-of-service (DoS) attacks. Unfortunately, existing building management system platforms do not detect cyber attacks by analyzing the data they receive. To provide full visibility of building systems and protect them from malicious actors, it is necessary to integrate devices and systems with diverse building management system protocols in a single platform.

To address the security gap, this research has developed a proof-of-concept security-enhanced orchestration platform for building management systems. The platform supports multiple common communications protocols, including Modbus TCP [7], BACnet [5], REST API, MQTT [8], Zigbee [11], Wi-Fi and Bluetooth. Protocol traffic in the building systems and Internet of Things devices is analyzed to detect and mitigate cyber attacks.

3 Orchestration Platform

The security-enhanced orchestration platform for building management systems is designed to manage building system applications as well as security and other critical systems. The overall architecture comprises a system architecture and a security architecture. The system architecture incorporates a central control unit (orchestration platform) that integrates multiple systems in an existing building management system with Internet of Things devices to provide seamless user experience while ensuring stability and reliability. The central control unit implements a security architecture with mechanisms for monitoring and controlling access, detecting intrusions and isolating compromised systems and devices. The orchestration platform provides a robust solution for monitoring and controlling building systems while maintaining security.

3.1 System Architecture

Figure 1 shows the system architecture of the security-enhanced orchestration platform for building management systems. The system architecture comprises two components, selected systems (Systems 1 to 4) and devices in an existing

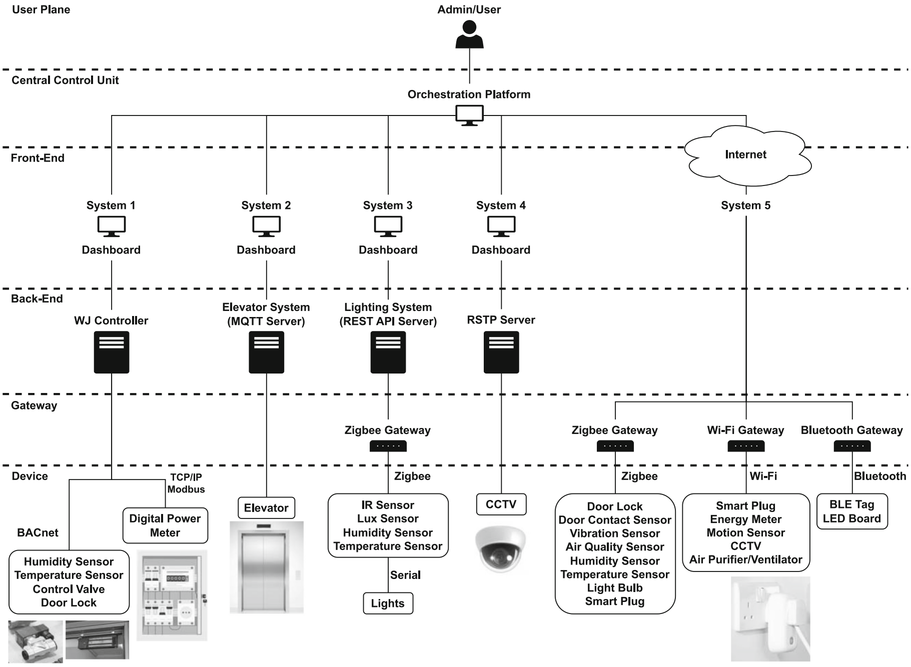

Fig. 1. System architecture.

building management system, and a central control unit with Internet of Things devices (System 5). The selected systems and devices in the building management system monitor and control various building applications. The devices are categorized as operational technology and include equipment such as lighting and elevator control systems.

The central control unit with Internet of Things devices is incorporated in the system architecture to integrate existing systems and devices while providing remote management capabilities. Internet of Things devices are smart systems and sensors that support and enhance building management system functionality. The devices include humidity sensors, temperature sensors, vibration sensors and air quality sensors, among others. Table 1 provides information about the devices incorporated in the system architecture.

3.2 Security Architecture

Building management system architectures typically isolate subsystems that support specific applications, often requiring different back-ends and/or front-ends for subsystem operation. However, this architecture introduces latency and performance problems when the subsystems are interconnected. The isolation significantly complicates building management governance by operators due to the reduced visibility of system state. The orchestration platform is intended to

Table 1. Device information.

System	Device	Protocol	Class
System 1 (WJ Controller)	Humidity/temperature sensors	BACnet	OT
	Control valve	BACnet	OT
	Door lock	BACnet	OT
	Digital power meter	Modbus TCP	OT
System 2 (MQTT Server)	Elevator	MQTT	OT
System 3 (REST API Server)	Infrared sensor	ZigBee	IoT
	Lux sensor	ZigBee	IoT
	Humidity/temperature sensors	ZigBee	IoT
	Light bulb	Serial	OT
System 4 (RSTP Server)	Closed-circuit TV	MQTT	OT
System 5 (IoT Devices)	Door lock	ZigBee	IoT
	Door contact sensor	ZigBee	IoT
	Vibration sensor	ZigBee	IoT
	Air quality sensor	ZigBee	IoT
	Humidity sensor	ZigBee	IoT
	Temperature sensor	ZigBee	IoT
	Light bulb	ZigBee	IoT
	Smart plug	ZigBee/Wi-Fi	IoT
	Energy meter	Wi-Fi	IoT
	Motion sensor	Wi-Fi	IoT
	Closed-circuit TV	Wi-Fi	IoT
	Air purifier	Wi-Fi	IoT

address these deficiencies by serving as the central governor of a building management system, providing key capabilities such as monitoring, control, data collection, storage and analysis, as well as physical security and cyber security.

A key advantage of the orchestration platform is its ability to overcome the limitations of traditional isolated systems. It is difficult to detect attacks and abnormalities in typical building management systems due the limited visibility they provide. However, incorporating Internet of Things devices in building management systems along with an orchestration platform with intrusion detection capabilities provides improved visibility of system performance as well as efficient governance and secure building operation.

Figure 2 shows the security-enhanced orchestration framework. It incorporates a front-end alert and notification system that displays attack alerts and abnormal reading notifications in real time. This enables building management operators to quickly identify and respond to potential security incidents. The back-end of the framework provides several key functions that ensure overall stability and security. The system health check function monitors CPU and mem-

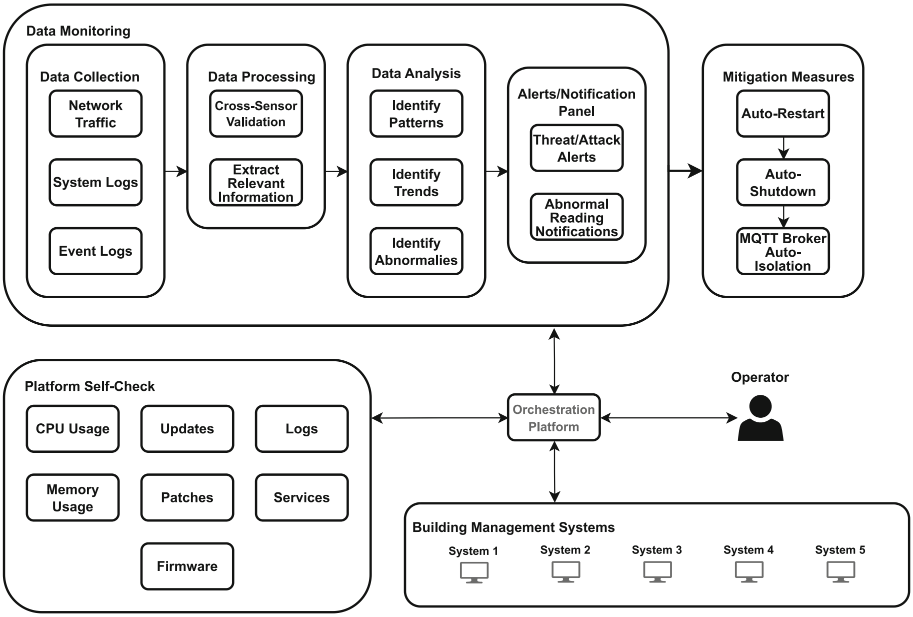

Fig. 2. Security-enhanced orchestration framework.

ory usage, updates, patches, firmware, network traffic and services to ensure that the system is operating at optimal conditions. Additionally, the framework provides monitoring and identification functionality that leverage data collection, processing and analysis to detect potential security threats and attacks.

The framework also provides response measures to mitigate the negative effects of incidents. This includes device auto-restart, device auto-shutdown and device auto-isolation. Compromised devices and networks are rapidly isolated and shut down to prevent security incidents from spreading and minimize their impacts on building management. The framework provides a comprehensive and robust solution that enables operators to rapidly identify and respond to potential security incidents and maintain overall building stability and security.

4 Device Auto-Recovery and Auto-Isolation

Incorporating Internet of Things devices in building management systems introduces new cyber security risks because it expands the attack surfaces for malicious actors. Nevertheless, the devices are vital because it is difficult to provide security services without visibility into building systems and operations. The orchestration platform provides full visibility into all aspects of the building management system, including all the connected devices.

The orchestration platform provides device auto-recovery and device auto-isolation functionality. Figure 3 shows the workflow geared for restartable and

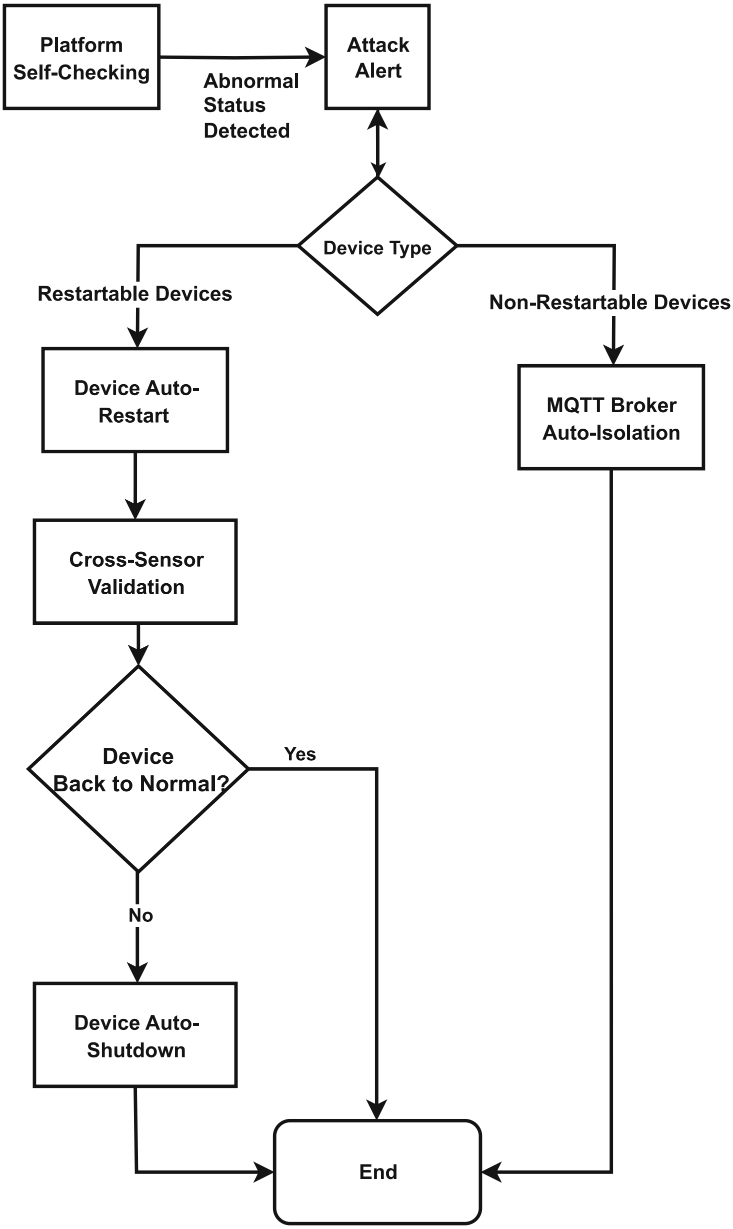

Fig. 3. Device auto-recovery and auto-isolation workflow.

non-restartable devices. Restartable devices are not critical to building management system operation and can be safely restarted by the orchestration platform after attacks or incidents. Non-restartable devices such as those installed in important elevator and door lock systems require manual intervention because auto-restarts could negatively impact building operation. The purpose of the workflow is to bring the devices and systems back to normal operation.

Self-checking and Abnormal Device Identification. The monitoring function of the orchestration platform periodically checks system parameters such as CPU and memory usage as well as network traffic. This helps track the stability and health of the orchestration platform and the connected devices.

Additionally, the orchestration platform monitors the message-sending frequencies of connected devices. Deviations from the average values are considered to be anomalous and appropriate actions are instituted to investigate and address the anomalies.

Cross-Sensor Validation. One of the key features of the orchestration platform is its ability to perform cross-sensor validation. The process is designed to ensure that the readings received from connected sensors are accurate and not compromised by a malicious actor.

The first step in cross-sensor validation is to identify the sensors that are sending abnormal readings. This is done by comparing the sensor readings against historical data. Following this, data from relevant sensors is used to validate whether or not other sensors measuring the same or similar data have similar patterns as the sensors with abnormal readings. If most of the other sensors have different readings, it is concluded that the sensors with abnormal readings have issues that are more serious than simply anomalous. In such a situation, the orchestration platform proceeds to the device auto-restart phase.

Device Auto-Restart. In many situations, restarting a device is an effective way of resolving problems and bringing the device back to the normal state. This is especially true for Internet of Things devices due to their diverse hardware, software and protocols. Unfortunately, manual device restarts can be problematic and often require time-consuming human operator intervention. The orchestration platform is specifically designed to automate device restart when abnormal status is detected.

An affected device is automatically restarted after abnormal status is detected. After the restart, the orchestration platform reconnects to the device and performs cross-sensor validation to ensure that the device is operating normally. The cross-sensor validation process compares the device readings against those of other relevant sensors to ensure that the device is functioning correctly.

By automating the device restart process, the orchestration platform can quickly resolve problems and minimize disruptions to building operation. This important feature provides operators with real-time monitoring and rapid device recovery capabilities.

Device Auto-Shutdown. In the event an Internet of Things device is unable to resume normal operation after a restart, the orchestration platform takes additional measures to maintain the overall stability and security of the building management system. Specifically, the platform disconnects and shuts down the affected device to prevent it from affecting other devices and systems. This action is taken as a precautionary measure to protect the integrity of the building management system. The orchestration platform also notifies operators that the device should be repaired or replaced.

Device Auto-Isolation. Unlike Internet of Things devices, certain building management devices and systems may be deemed critical and cannot be restarted or shut down by the orchestration platform without disrupting building operations. In such cases, the orchestration platform takes a different approach to maintain the overall stability and security of the building management system.

When abnormal status is detected in a critical device or system, the orchestration platform automatically disconnects and isolates the component from the network infrastructure. This prevents the abnormality from affecting other normal devices and systems and the cyber attack from propagating. Additionally, the orchestration platform also automatically blacklists the IP address of the device or system to block further communications with the building management system and prevent malicious traffic from entering.

The orchestration platform notifies operators that the abnormality should be investigated. Steps are then taken to repair or replace the device or system and return it to normal operation.

Disconnecting, isolating and blacklisting IP addresses also apply to devices that cannot be restarted or shut down. This ensures that the building management system is always operating at optimal conditions and protects against cyber attacks.

5 Experiments

Experiments were conducted to demonstrate the security features of the orchestration platform for building management. Figure 4 shows the experimental setup. A Mosquitto MQTT broker [8] was deployed on the orchestration platform and connected to several devices and systems. Many devices using the MQTT communications protocol do not provide adequate security measures and often rely on insecure default configurations [12]. Therefore, a username-password authentication mechanism was employed to set up the MQTT broker configuration in the experiments. As seen in the figure, the MQTT broker was connected to multiple Internet of Things devices and a Raspberry Pi computer that served as the malicious attack device. A smart plug connected to the Raspberry Pi was employed to shut down and restart the device during the experiments.

Three experimental scenarios were investigated. The first scenario focused on the device auto-restart security feature. The second scenario focused on the

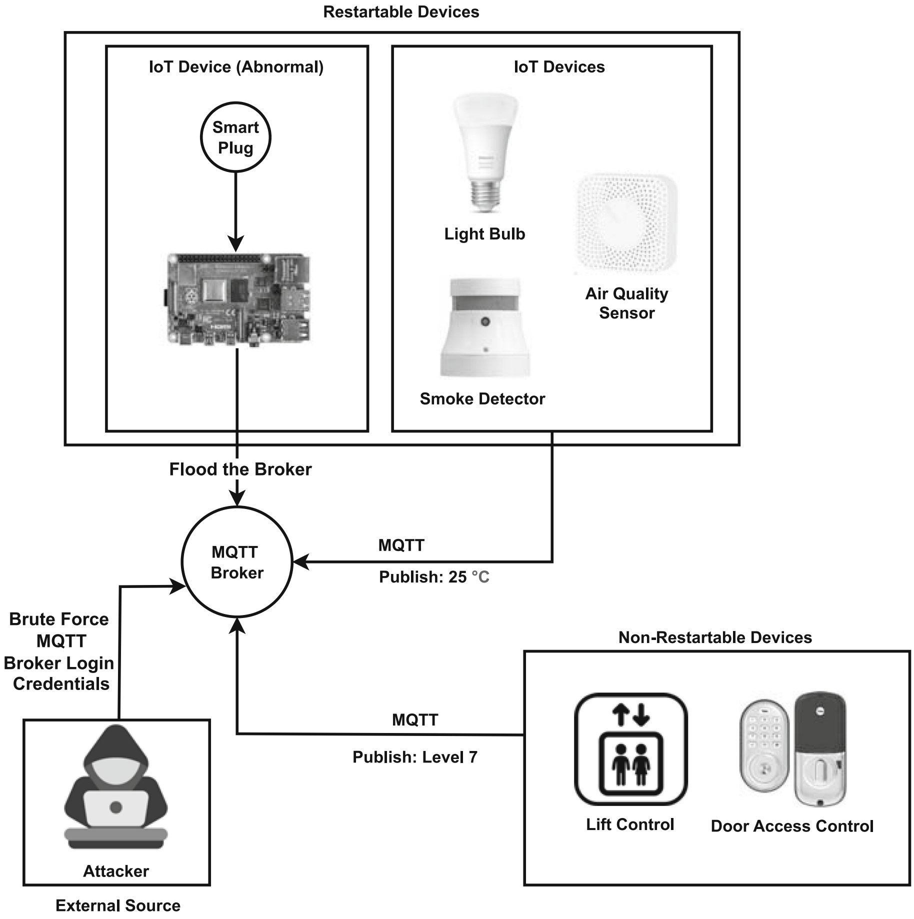

Fig. 4. Experimental setup.

device auto-restart and device auto-shutdown security features. The third scenario focused on the device auto-isolation security feature when a device cannot be restarted or shut down due to its criticality when the building management system is under attack.

5.1 Scenario 1

Scenario 1 involved a situation where a legitimate device connected to the MQTT broker malfunctions or where an attacker gains control of a legitimate device and floods the MQTT broker with messages. Upon receiving an alert, the orchestration platform is designed to engage its device auto-restart security feature. After restarting the device, the orchestration platform performs cross-sensor validation to ensure that the device is functioning normally and does not continue to flood the broker.

The Raspberry Pi was set up as the abnormal device connected to the MQTT broker. A Python script on the Raspberry Pi established a connection with the

MQTT broker and flooded it with 10,000 messages per second for 15 min. Attack alerts were triggered and the orchestration platform leveraged the smart plug to restart the connected Raspberry Pi. After restarting the Raspberry Pi, the orchestration platform performed cross-sensor validation to ensure that the device was working normally. The security feature successfully prevented the abnormal device from flooding the MQTT broker and overloading the server CPU.

5.2 Scenario 2

Scenario 2 involved a situation where a device upon restarting continues to flood the MQTT broker with messages. The orchestration platform is designed to detect and mitigate the attack by automatically shutting down the device after cross-sensor validation.

The Raspberry Pi was set up to run the Python script that simulated an abnormal device flooding the MQTT broker with messages after it was auto-restarted. The orchestration platform detected the flooding attack by monitoring the MQTT broker and identified the device based on the attack alert. After the Raspberry Pi was restarted, cross-sensor validation was performed, but the device was found to be abnormal and was, therefore, shut down. This scenario demonstrates the effectiveness of the orchestration platform at mitigating message flooding attacks and ensuring the stability of the MQTT broker.

5.3 Scenario 3

Scenario 3 was designed to evaluate the effectiveness of the MQTT broker auto-isolation security feature. A brute force attack was launched to gain unauthorized access to the MQTT broker by repeatedly trying different login credentials in a short time frame. Specifically, ten connection attempts were made in 20 s from an external source.

Upon receiving the attack alert, the MQTT broker auto-isolation feature captured the username and removed it from the broker's access control list, effectively isolating the attack by preventing a connection to the MQTT broker. The security feature ensures that, even if access is gained to the MQTT broker via a brute force attack, the compromised username and password cannot be used to connect to the MQTT broker or access any MQTT topics.

It should be noted that the device auto-restart and auto-shutdown security features do not apply to critical building devices and systems such as the lift control and door control systems. Instead, the MQTT broker auto-isolation security feature is leveraged to protect these critical systems from external attacks.

5.4 Results and Limitations

Table 2 shows the average recovery times for the security features triggered during the three scenarios. The recovery times were measured by determining the time elapsed from when an attack alert was received to when the device was returned to its normal state or when isolation was successfully activated by removing the username from the MQTT broker access control list. The average

Table 2. Experimental results.

Scenarios	Average Recovery Time	Triggered Security Feature
1	15.26 s	Device auto-restart
2	55.57 s	Device auto-restart and shutdown
3	24.10 s	MQTT broker auto-isolation

recovery times were computed as the averages over ten executions in each of the three scenarios.

The experimental results involving the MQTT broker demonstrate the effectiveness of the security features implemented in the orchestration platform.

In Scenario 1, the device auto-restart feature successfully mitigated an MQTT message flooding attack by restarting the abnormal device and performing cross-sensor validation to ensure normal operation.

The results in Scenario 2 further show the importance of the device auto-shutdown security feature in preventing repeated MQTT message flooding. The orchestration platform successfully detected the attack, restarted the abnormal device and subsequently shut it down when it determined that the device was not functioning properly.

The results in Scenario 3 involving a brute force (credential stealing) attack demonstrate the effectiveness of the MQTT broker auto-isolation feature in preventing unauthorized broker access and minimizing potential damage.

However, it is important to consider the potential negative side effects of the auto-restart and auto-shutdown features. If triggered too frequently, the two features could disrupt normal device operation, causing user inconvenience and frustration.

6 Conclusions

Increasing numbers of Internet of Things devices are being deployed in infrastructure assets such as buildings. However, it is challenging for building management operators to monitor these heterogeneous devices and troubleshoot them when they malfunction or are targeted by cyber attacks.

The security-enhanced orchestration platform described in this chapter is designed for building management systems that incorporate operational technology and diverse Internet of Things devices. The orchestration platform receives a variety of data from building management components and Internet of Things devices to provide situation awareness and support efficient and stable operation. The integration of novel device auto-recovery and auto-isolation functionality in the orchestration platform enables the monitoring and mitigation of abnormal conditions, including those initiated by cyber attacks.

Future research will attempt to apply machine learning techniques to enhance the detection of abnormal Internet of Things device operations. Additionally, it will augment the orchestration platform to monitor and manage additional building components such as gas and water supply systems.

References

1. Agarwal, Y., Gupta, R., Komaki, D., Weng, T.: BuildingDepot: an extensible and distributed architecture for building data storage, access and sharing. In: Proceedings of the Fourth ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings, pp. 64–71 (2012)
2. Alsuhli, G., Khattab, A.: A fog-based IoT platform for smart buildings. In: Proceedings of the International Conference on Innovative Trends in Computer Engineering, pp. 174–179 (2019)
3. Brooks, D.: Intelligent buildings: an investigation into current and emerging security vulnerabilities in automated building systems using an applied defeat methodology. In: Proceedings of the Fourth Australian Security and Intelligence Conference, pp. 16–26 (2011)
4. Chan, R., Tan, F., Teo, U., Kow, B.: Vulnerability assessments of building management systems. In: ICCIP 2020. IAICT, vol. 596, pp. 209–220. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-62840-6_10
5. Fernbach, A., Granzer, W., Kastner, W.: Interoperability at the management level of building automation systems: a case study for BACnet and OPC UA. In: Proceedings of the International Conference on Emerging Technologies and Factory Automation (2011)
6. Fisk, D.: Cyber security, building automation and the intelligent building. Intell. Buildings Inter. **4**(3), 169–181 (2012)
7. Fovino, I.N., Carcano, A., Masera, M., Trombetta, A.: Design and implementation of a secure modbus protocol. In: Palmer, C., Shenoi, S. (eds.) ICCIP 2009. IAICT, vol. 311, pp. 83–96. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04798-5_6
8. Hillar, G.: MQTT Essentials - A Lightweight IoT Protocol. Packet Publishing, Birmingham, United Kingdom (2017)
9. Kalaska, R., Czarnul, P.: Some security features of selected IoT platforms. TASK Q. **24**(1), 29–61 (2020)
10. Makonin, S.: App programming and its use in smart buildings. In: Pacheco-Torgal, F., Rasmussen, E., Granqvist, C., Ivanov, V., Kaklauskas, A., Makonin, S. (eds.) Start-Up Creation: The Smart Eco-Efficient Built Environment, Woodhead Publishing, Sawston, United Kingdom, pp. 451–463 (2016)
11. Muthu Ramya, C., Shanmugaraj, M., Prabakaran, R.: Study on ZigBee technology. In: Proceedings of the Third International Conference on Electronics Computer Technology, pp. 297–301 (2011)
12. Palmieri, A., Prem, P., Ranise, S., Morelli, U., Ahmad, T.: MQTTSA: a tool for automatically assisting the secure deployments of MQTT brokers. In: Proceedings of the IEEE World Congress on Services, pp. 47–53 (2019)
13. Rathore, M., Ahmad, A., Paul, A., Rho, S.: Urban planning and building smart cities based on the Internet of Things using big data analytics. Comput. Netw. **101**, 63–80 (2016)
14. Weng, T., Nwokafor, A., Agarwal, Y.: BuildingDepot 2.0: an integrated management system for building analysis and control. In: Proceedings of the Fifth ACM Workshop on Embedded Systems for Energy-Efficient Buildings (2013)