Department of Electronic and Telecommunication Engineering

University of Moratuwa

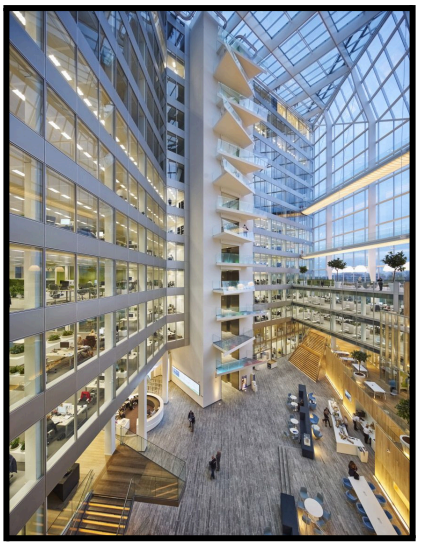
- 200123H DHANOMIKA A.P.N.
- 200134R DISSANAYAKA R.M.R.H.
- 200310E KODITHUWAKKU K.A.W.T.
- 200702H WEERASINGHE P.D.G.U.M.B.

Team CyberSphere

EN4720: Security in Cyber-Physical Systems

Course Project

A detailed description of the smart building system



The Edge, located in Amsterdam, is widely recognized as one of the world's most intelligent and sustainable office buildings. Its smart building system integrates various advanced technologies to optimize energy efficiency, comfort, and security. Here's a detailed overview of its key components:

1. IoT-Enabled Lighting

The Edge utilizes a sophisticated lighting system powered by nearly 30,000 IoT sensors. These sensors monitor occupancy and natural light levels to adjust artificial lighting accordingly, ensuring optimal illumination while minimizing energy consumption.

2. HVAC Systems

The building's Heating, Ventilation, and Air Conditioning (HVAC) systems are integrated with IoT sensors that continuously collect data on temperature, humidity, and occupancy. This real-time information allows the system to adjust heating and cooling dynamically, maintaining a comfortable environment and enhancing energy efficiency.

3. Security Cameras

While specific details about the security camera system at The Edge are not publicly disclosed, it is common for smart buildings of this caliber to incorporate advanced surveillance technologies. These systems typically include high-definition cameras with capabilities such as facial recognition and motion detection, integrated into the building's central management system to enhance security measures.

4. Access Control Mechanisms

Access to The Edge is managed through a combination of technologies designed to ensure security and convenience:

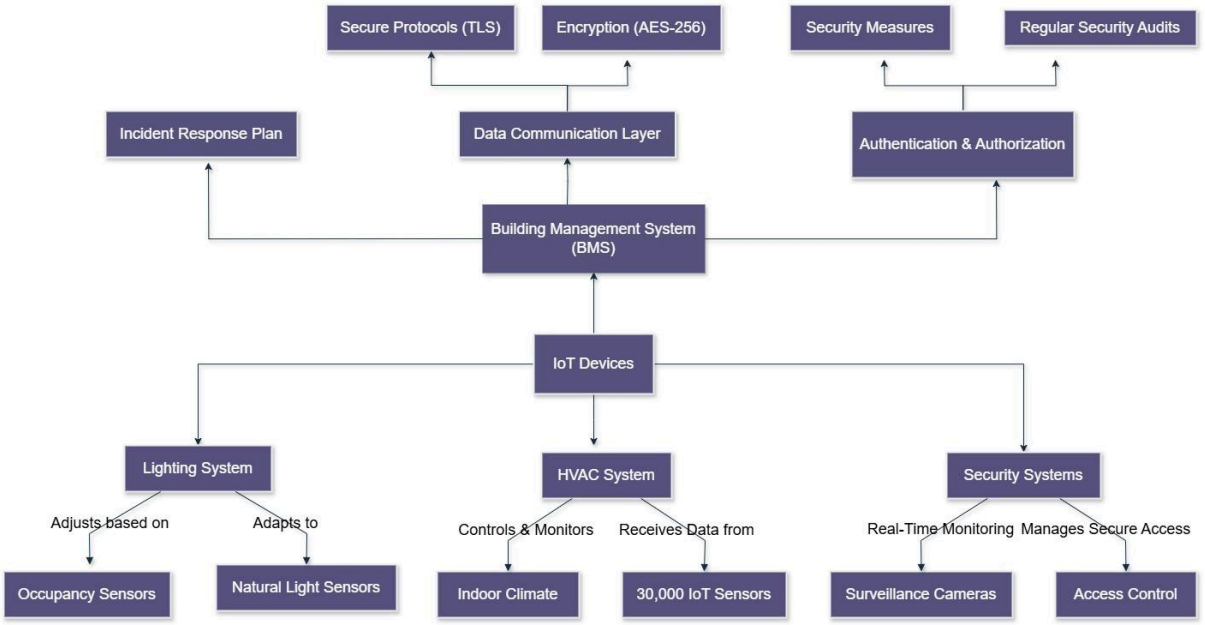
- **Smartphone Integration**: Employees use a dedicated smartphone app to access various building services, including room bookings and personalized settings.

- **License Plate Recognition**: The parking garage employs license plate recognition technology to grant seamless access to registered vehicles, streamlining the entry process.

5. Building Management System (BMS)

At the core of The Edge's operations is an advanced Building Management System that integrates data from various sensors and devices. This centralized platform enables real-time monitoring and control of lighting, HVAC, and other critical systems, facilitating proactive maintenance and efficient energy management.

By harmoniously integrating these technologies, The Edge exemplifies the potential of smart building systems to create sustainable, efficient, and comfortable environments for occupants.



Identified Vulnerabilities and Mitigation Strategies

Despite its advanced features, The Edge may still be susceptible to certain vulnerabilities:

a. Cryptographic Implementation Vulnerabilities

- **Insecure Encryption**: If data transmitted between IoT devices and the BMS is not adequately encrypted, it could be intercepted and exploited.
    - *Mitigation*: Implement robust encryption protocols, such as AES-256, for all data transmissions. Regularly update encryption methods to address emerging threats.
- **Weak Key Management**: Poor handling of cryptographic keys can lead to unauthorized access to sensitive information.
    - *Mitigation*: Utilize secure key management practices, including hardware security modules (HSMs), and enforce strict access controls to key storage locations.

b. Authentication and Authorization Design Vulnerabilities

- **Weak Password Policies**: Allowing simple or default passwords increases the risk of unauthorized access.
    - *Mitigation*: Enforce strong password policies requiring complex combinations of characters, regular password changes, and disallowing default credentials.
- **Improper Access Control Configurations**: Inadequate segregation of user privileges can lead to unauthorized access to critical systems.
    - *Mitigation*: Implement role-based access control (RBAC) to ensure users have the minimum necessary permissions for their roles. Regularly audit access controls to verify appropriate configurations.

c. Unpatched Systems

- **Outdated Firmware and Software**: Unpatched devices may have known vulnerabilities that attackers can exploit.
    - *Mitigation*: Establish a routine update schedule to ensure all devices run the latest firmware and software versions. Monitor vendor announcements for critical security patches.

d. Insecure Communication Protocols

- **Unencrypted Data Transmission**: Transmitting data without encryption can lead to interception and tampering.
    - *Mitigation*: Ensure all communication between devices and systems is encrypted using secure protocols like TLS.

Recommendations for Best Practices

Enhancing the security of a smart building system involves implementing a multi-layered approach that addresses both cyber and physical threats. The following best practices are recommended:

1. Implement Network Segmentation

Isolate building management systems from other networks to limit unauthorized access. This approach ensures that even if one system is compromised, the threat does not spread across the entire network.

2. Enforce Strong Authentication Mechanisms

Utilize robust authentication protocols, such as multi-factor authentication (MFA), to verify user identities before granting access to critical systems. This reduces the risk of unauthorized access due to compromised credentials.

3. Regularly Update and Patch Systems

Keep all software and firmware up to date to address known vulnerabilities. Establish a routine patch management process to ensure timely updates.

4. Secure Physical Access

Restrict physical access to critical infrastructure components, such as server rooms and network devices, to prevent tampering or unauthorized modifications.

5. Conduct Continuous Monitoring and Incident Response

Implement real-time monitoring of network traffic and system activities to detect anomalies. Develop and regularly update incident response plans to address potential security breaches effectively.

6. Educate and Train Staff

Provide regular cybersecurity training to all personnel to ensure they can recognize and respond to potential threats, such as phishing attempts. citeturn0search6

7. Utilize End-to-End Encryption

Protect data integrity and confidentiality by implementing end-to-end encryption for data transmitted across networks.

8. Develop a Comprehensive Risk Management Strategy

Assess potential risks and implement a layered security approach to deter, detect, delay, defend, and deny threats.

By adopting these best practices, smart building systems can significantly enhance their security posture, ensuring the safety and integrity of both digital and physical assets.

Mapping Vulnerabilities to CVEs

CVE ID	Brief Description	Breach of Security Goal	Known Real-Life Case
CVE-2021-31621	Weak encryption methods used in IoT lighting systems could allow attackers to intercept and manipulate commands.	Confidentiality, Integrity	Smart Light Vulnerability Exploit
CVE-2020-29583	Poor authentication implementation in access control systems allows unauthorized access via brute force attacks.	Confidentiality, Availability	Access Control Hack in Smart Buildings
CVE-2019-17101	Insufficient validation of software updates in HVAC systems could let attackers inject malicious firmware.	Integrity, Availability	HVAC System Attack
CVE-2021-22779	IoT sensor networks with default credentials make it easy for attackers to gain unauthorized access to data	Confidentiality	IoT Default Credential Risks
CVE-2018-5390	Network DoS attack vulnerability in smart building systems could lead to performance degradation.	Availability	IoT-Based DoS Attacks