Analecta Technica Szegedinensia
Vol. 19, No. 1 ISSN 2064-7964 2025

SECURING IOT-BASED HEATING CONTROL SYSTEMS IN CRITICAL INFRASTRUCTURE: CHALLENGES AND SOLUTIONS

[1]Boldizsár Bednárik, [2]László Gogolák

[1]Doctoral School on Safety and Security Sciences, Óbuda University, 1034 Budapest, Hungar,
[2]Department of Mechatronics and Automation, Faculty of Engineering, University of Szeged, 6720 Szeged, Hungary

e-mail: bednarik.boldizsar@uni-obuda.hu

Received: 13th February	*Accepted: 20th March*

ABSTRACT

The integration of smart technology into heating systems has led to increased efficiency and remote management capabilities. However, these advancements also introduce security vulnerabilities, especially in critical infrastructure. This paper explores the development of an IoT-based heating control system utilizing MQTT, ESP8266 microcontrollers, and Node-RED for centralized management. The study examines system design, identifies potential security threats, and proposes strategies to mitigate risks. Additionally, real-world case studies illustrate how cybersecurity weaknesses have impacted similar IoT applications in critical infrastructure, reinforcing the importance of implementing robust security measures.

Keywords: IoT, Critical Infrastructure, Cyber Security, MQTT, ESP8266

1. INTRODUCTION

The ability to manage heating systems remotely through IoT technology [1] has significantly improved energy efficiency and operational convenience in critical infrastructure sectors, such as power plants, hospitals, and government facilities. However, this convenience comes with risks, as connected systems are often the target of cyberattacks [2]. This paper discusses the construction of a secure IoT-based heating control system, addressing threats such as unauthorized system access, data breaches, and communication reliability, which are especially critical in infrastructure essential for public safety and national security.

Attackers gaining access to heating control systems in critical infrastructure can manipulate temperatures, disrupt energy distribution, and cause severe damage. For instance, a compromised hospital heating system could endanger patients, while an attack on an industrial facility could lead to financial losses and safety hazards. This paper provides insights into designing a secure system that can withstand cyber threats, articularly in environments where security is paramount.

2. MATERIALS AND METHODS

The IoT-based heating control system integrates both hardware and software components to enable efficient and secure operation. The hardware setup consists of ESP8266 microcontrollers, which facilitate wireless communication between the temperature sensor module and the heating control module. These microcontrollers interact with the DHT22 temperature sensor, which provides precise real-time temperature readings. The system also includes a relay module that controls the heating system by switching it on or off based on MQTT messages received from the server. The backbone of the system's operation is a Linux server, responsible for running the Mosquitto MQTT broker and Node-RED, which together handle data processing and command execution.

DOI: https://doi.org/10.14232/analecta.2025.1.38-44

On the software side, the MQTT protocol ensures smooth communication between IoT devices and the central server. Node-RED, a visual programming tool, is utilized for managing data flow and automating system responses, enhancing the system's efficiency. To maintain security, Transprdware and software components enable efficient and secure operation. The hardware setup consists of ESP8266 microcontrollers, which facilitate wireless communication between the temperature sensor module and the heating control module. These microcontrollers interact with the DHT22 temperature sensor, which provides precise real-time temperature readings. The system also includes a relay module that controls the heating system by switching it on or off based on MQTT messages received from the server. The backbone of the system's operation is a Linux server, responsible for running the Mosquitto MQTT broker and Node-RED, which together handle data processing and command execution.ort Layer Security (TLS) encrypts MQTT messages, preventing unauthorized data interception. Additionally, firewall and intrusion detection systems are implemented to monitor and filter malicious network traffic, safeguarding the system from potential cyber threats.

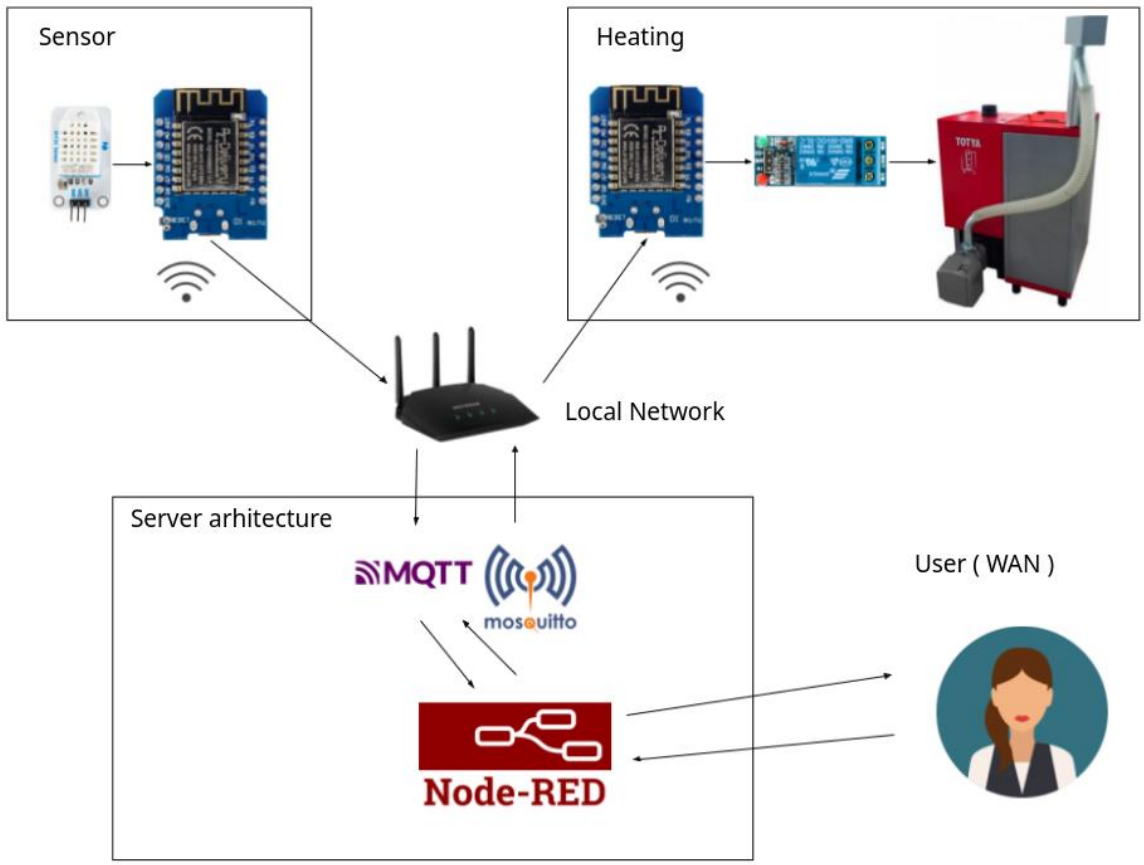

Figure 1. Schematic architecture of the heating control system

The system follows a structured methodology to ensure reliability and security. During deployment, IoT devices were connected in a simulated environment to facilitate data exchange and validate heating control commands via MQTT. Security testing involved penetration testing techniques such as brute-force attacks, packet sniffing, and denial-of-service simulations to assess vulnerabilities. Performance evaluation measured

DOI: https://doi.org/10.14232/analecta.2025.1.38-44

the impact of security measures on system performance, focusing on latency, response times, and error rates. Furthermore, continuous monitoring of security logs and network activity allowed for the detection of anomalies and unauthorized access attempts.

By combining robust hardware, secure communication protocols, and proactive security measures, the system is designed to mitigate risks while maintaining operational efficiency. This integrated approach ensures that the heating control system remains both functional and resilient, making it suitable for deployment in critical infrastructure environments.

2.1. System Architecture and Components

The proposed heating control system consists of three key components:

- **Temperature Sensor Module:** Incorporates an ESP8266 microcontroller and a DHT22 sensor to capture temperature data in real time, transmitting it to a central server.
- **Heating Control Module:** Features an ESP8266 microcontroller connected to a relay switch that toggles the heating system based on received instructions.
- **Central Management Server:** A Linux-based server running Mosquitto MQTT broker and Node-RED, responsible for processing sensor data, making decisions, and transmitting control commands.

MQTT, a lightweight messaging protocol, is utilized for efficient communication between these modules [3]. However, the absence of inherent security features necessitates additional protective measures to prevent cyber intrusions. Given the importance of heating systems in critical infrastructure, any security breach could lead to disruptions with severe consequences.

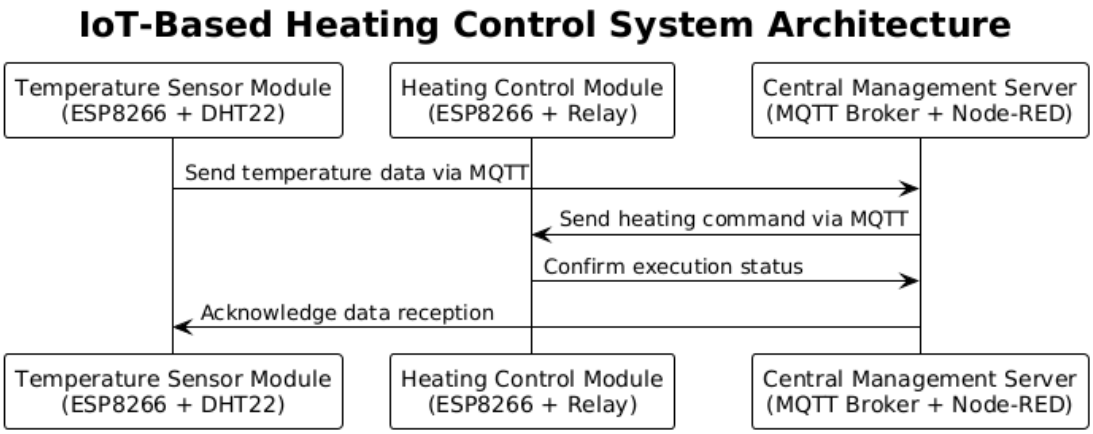

Figure 2. System Components and Communication

DOI: https://doi.org/10.14232/analecta.2025.1.38-44

2.2. Security Challenges in IoT-Based Heating Systems

Due to limited computational capabilities, IoT devices often lack essential security protections [4]. Some of the most common vulnerabilities in critical infrastructure heating systems include:

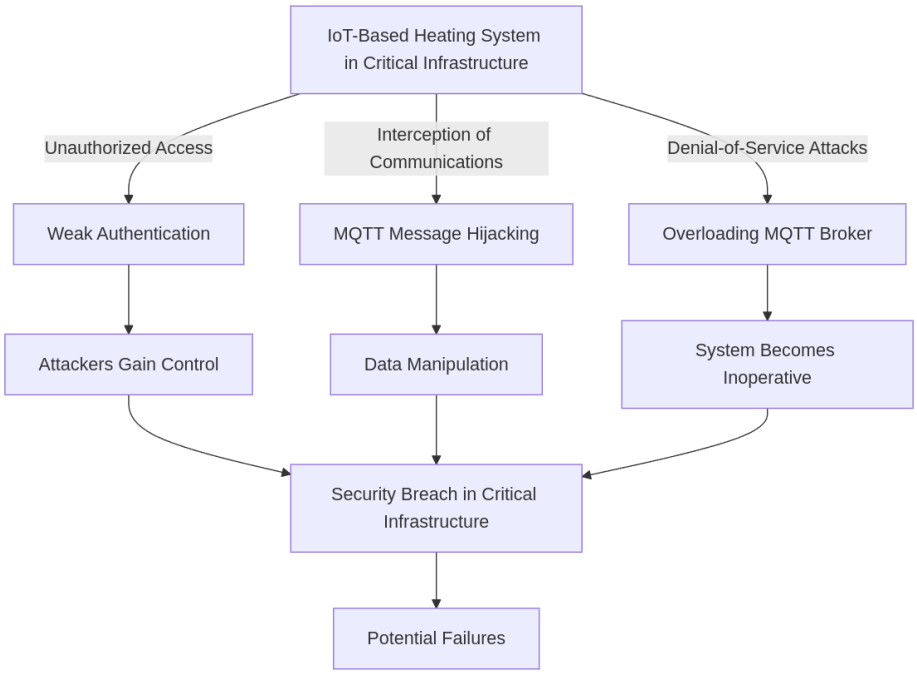

Figure 3. Security Challenges in IoT-Based Heating Systems

- **Unauthorized Access:** Weak authentication mechanisms can enable malicious actors to seize control of heating systems [5]. Without robust access controls, attackers may infiltrate the network and manipulate operations.
- **Interception of Communications:** Cybercriminals can intercept MQTT messages, modifying commands or manipulating sensor data [6]. In critical infrastructure, this could lead to cascading failures affecting large populations.
- **Denial-of-Service (DoS) Attacks:** A flood of requests can overwhelm the MQTT broker, rendering the system inoperative [7]. A DoS attack on a critical facility's heating system during winter could result in catastrophic failure.

The 2016 Mirai botnet attack exemplifies the dangers of unsecured IoT devices, as millions of compromised devices were leveraged to execute large-scale cyberattacks [8]. Critical infrastructure systems must implement strong security frameworks to prevent similar incidents.

DOI: https://doi.org/10.14232/analecta.2025.1.38-44

2.3. Implementing Security Measures

To fortify the system against potential threats, the following measures were applied:

- **Enhanced Authentication:** Implemented MQTT username-password authentication and Access Control Lists (ACLs) to restrict unauthorized access [9].
- **Data Encryption:** Integrated Transport Layer Security (TLS) to encrypt MQTT messages, safeguarding communications from interception [10].
- **Firmware Integrity Verification:** Deployed cryptographic hashing techniques to ensure firmware updates remain unaltered by unauthorized parties [11].
- **Network Segmentation:** Created an isolated VLAN for IoT devices, limiting exposure to external threats [12].
- **Intrusion Detection Mechanisms:** Monitored network activity for anomalies, enabling real-time detection of suspicious behavior [13].

Each of these measures contributes to a multi-layered security approach, strengthening resilience against cyber threats in critical infrastructure settings.

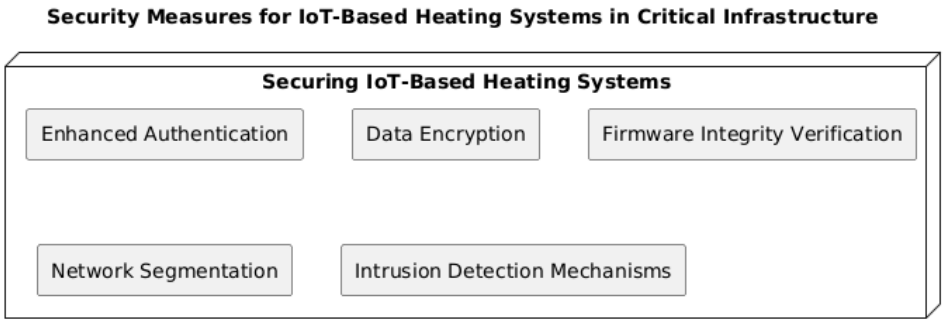

Figure 4. Security Measures

DOI: https://doi.org/10.14232/analecta.2025.1.38-44

3. RESULTS AND DISCUSSION

Implementing security enhancements led to substantial improvements in system protection. Testing demonstrated that TLS encryption significantly mitigated data interception risks, while ACL-based authentication effectively prevented unauthorized access [14]. Additionally, network segmentation minimized the impact of breaches by containing threats within a designated environment.

Simulated cyberattacks further validated system security. Unauthorized access attempts were consistently blocked, proving the effectiveness of authentication and encryption measures. Furthermore, rate-limiting mechanisms on the MQTT broker successfully defended against DoS attacks.

Long-term performance monitoring revealed that security logs played a vital role in identifying potential vulnerabilities. These logs provided a detailed account of login attempts, configuration changes, and network activity, allowing administrators to preemptively address security gaps. In critical infrastructure, continuous monitoring and threat intelligence are crucial for proactive security measures.

4. CONCLUSION

While IoT-based heating control systems offer efficiency and convenience, they also present significant cybersecurity risks, particularly in critical infrastructure. This study demonstrates that implementing TLS encryption, access control measures, and intrusion detection mechanisms enhances system security. Future research will focus on integrating artificial intelligence-driven threat detection to further strengthen cybersecurity frameworks [15].

Security awareness among users is another key aspect of defense. Many breaches occur due to weak passwords and failure to apply software updates. Combining advanced security technologies with user education will ensure a more robust system against evolving cyber threats. For critical infrastructure, adherence to industry standards and regulatory frameworks is essential to maintain security and reliability.

Future enhancements could incorporate renewable energy sources and fuzzy logic-based control strategies, as seen in [16] , to further optimize energy efficiency.

REFERENCES

[1] J. Simon, Z. Čović, and D. Dobrilović, “The Web of Things and Database Management Systems,” *Analecta Tech. Szeged.*, vol. 10, no. 2, pp. 61–68, Jun. 2016, doi: 10.14232/analecta.2016.2.61-68.
[2] R. H. Weber, “Internet of Things – New security and privacy challenges,” *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, Jan. 2010, doi: 10.1016/j.clsr.2009.11.008.
[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Commun. Surv. Tutor.*, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.
[4] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015, doi: 10.1016/j.comnet.2014.11.008.

[5] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.
[6] M. S. Hossain and G. Muhammad, "Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring," *Comput. Netw.*, vol. 101, pp. 192–202, Jun. 2016, doi: 10.1016/j.comnet.2016.01.009.
[7] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Gener. Comput. Syst.*, vol. 82, pp. 761–768, May 2018, doi: 10.1016/j.future.2017.08.043.
[8] M. Antonakakis *et al.*, "Understanding the Mirai Botnet," in *26th USENIX Security Symposium (USENIX Security 17)*, Vancouver, BC: USENIX Association, Aug. 2017, pp. 1093–1110. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis
[9] S. N. Firdous, Z. Baig, C. Valli, and A. Ibrahim, "Modelling and Evaluation of Malicious Attacks against the IoT MQTT Protocol," in *2017 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 Data (SmartData)*, Exeter: IEEE, Jun. 2017, pp. 748–755. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.115.
[10] A. Bashir and A. Hussain Mir, "Securing Communication in MQTT enabled Internet of Things with Lightweight security protocol," *EAI Endorsed Trans. Internet Things*, vol. 3, no. 12, p. e1, Oct. 2017, doi: 10.4108/eai.6-4-2018.154390.
[11] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017, doi: 10.1016/j.jnca.2017.04.002.
[12] C. M. Medaglia and A. Serbanati, "An Overview of Privacy and Security Issues in the Internet of Things," in *The Internet of Things*, D. Giusto, A. Iera, G. Morabito, and L. Atzori, Eds., New York, NY: Springer New York, 2010, pp. 389–395. doi: 10.1007/978-1-4419-1674-7_38.
[13] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 78, pp. 544–546, Jan. 2018, doi: 10.1016/j.future.2017.07.060.
[14] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: threats and challenges," *Secur. Commun. Netw.*, vol. 7, no. 12, pp. 2728–2742, Dec. 2014, doi: 10.1002/sec.795.
[15] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013, doi: 10.1016/j.comnet.2012.12.018.
[16] Simon, J., & Sánta, R. (2023). "Energy efficient smart home heating system using renewable energy source with fuzzy control design. Decision Making: Applications in Management and Engineering", 6(2), 948-974, Sep. 2023, doi: 10.31181/dmame622023825.