Jurnal Teknologi dan Manajemen

ISSN (Print) 1693-2285 ISSN (Online) 2808-9995

Research Article

IoT-Based E-Bike Docking Station with RFID Authentication for Smart Campus Mobility

Febyan Dimas Pramanta[1], Nana Sutarna [2], Sonki Prasetya [3]

[1, 2, 3] Politeknik Negeri Jakarta, Jl. Prof. DR. G.A. Siwabessy, Kampus Universitas Indonesia, Depok 16425

ARTICLE INFO

Received :
Accepted :
Published :

KEYWORDS

IoT Architecture; RFID Authentication; Smart Campus; E-Bike Docking Station; Access Control System; Micro-Mobility Infrastructure.

CORRESPONDENCE

E-mail Correspnding Author:
febyan.dimas.pramanta.te24@stu.pnj.ac.id
E-mail Co-Author:
nana.sutarna@elektro.pnj.ac.id
sonki.prasetya@mesin.pnj.ac.id

ABSTRACT

The rapid growth of micro-mobility adoption in campus environments requires secure and scalable infrastructure to regulate shared e-bike usage. Existing RFID-based access systems often rely on locally stored UID verification, limiting real-time access revocation and centralized monitoring capabilities. This study aims to design and evaluate an IoT-based e-bike docking station with centralized RFID authentication to enhance governance, traceability, and operational scalability in smart campus mobility systems. The proposed solution integrates edge-based docking control with cloud-based authentication validation using a layered IoT architecture. The main contribution of this research lies in integrating centralized RFID authentication with electromechanical docking control and real-time logging infrastructure within a unified smart campus framework. Unlike prior works focusing primarily on authentication protocol optimization, this study emphasizes deployable infrastructure-level implementation. The system architecture consists of a NodeMCU ESP8266, MFRC522 RFID reader, relay module, and electric magnetic dock lock connected to a centralized web server through Wi-Fi communication. Authentication requests are transmitted via HTTP protocol and validated at the server level. Performance evaluation was conducted through 100 authentication trials involving authorized and unauthorized access attempts. Authentication accuracy, response time, and communication reliability were quantitatively measured. Experimental results demonstrate 98% authentication accuracy with precision and recall above 98%. The mean response time was 1.12 seconds with a coefficient of variation of 12.5%, indicating stable temporal performance. Communication reliability reached 98% under indoor campus Wi-Fi conditions. These findings confirm that centralized IoT-based RFID validation can provide a practical and scalable solution for secure e-bike docking infrastructure in smart campus environments.

INTRODUCTION

The rapid transition toward sustainable transportation has accelerated the adoption of micro-mobility systems, particularly electric bicycles (e-bikes), in urban and institutional environments. E-bikes offer reduced emissions, improved energy efficiency, and suitability for short-distance travel (Oliveira et al., 2021; Hossein Sabbaghian et al., 2023). Intelligent bike-sharing management supported by Internet of Things (IoT) technologies has demonstrated improvements in operational efficiency and resource allocation (Abdellaoui Alaoui & Tekouabou, 2021). In university campuses, where mobility demand is characterized by dense population distribution and short travel distances, e-bikes are increasingly positioned as practical solutions for sustainable mobility (Luckyardi et al., 2022; Christian et al., 2025).

The smart campus paradigm integrates digital technologies into physical infrastructure to enhance governance, operational efficiency, and sustainability (Musa et al., 2021; Domínguez-Bolaño et al., 2024). IoT-based frameworks emphasize infrastructure observability, centralized supervision, and data-driven decision-making (Neis et al., 2023). Within mobility ecosystems, these principles require controlled access, usage traceability, and infrastructure transparency to ensure accountability and proper governance (Pinto et al., 2023).

Despite increasing adoption, campus e-bike deployment often lacks structured docking infrastructure. Informal parking practices reduce spatial efficiency and complicate supervision (Hossein Sabbaghian et al., 2023). Smart parking systems have been proposed to enhance organization through IoT integration (Fahim et al., 2021; Jabbar et al., 2024), while optimization-based localization approaches improve detection accuracy (Ghorpade et al., 2021). Prototypes using NodeMCU and RFID have demonstrated technical feasibility (Fernandez et al., 2023; Permana & Priatna, 2025). However, these implementations primarily focus on vehicle slot monitoring rather than structured docking systems integrating charging capability and controlled authentication tailored for e-bike ecosystems.

Access control remains a critical issue in campus mobility infrastructure. Unlike public systems, campus facilities should restrict access to authorized civitas academica. RFID technology provides a cost-effective and rapid authentication mechanism suitable for IoT environments (Gong et al., 2023; Shariq et al., 2021). Lightweight and secure RFID protocols are essential in constrained embedded systems to ensure secure communication without excessive computational overhead (Mudra et al., 2023; Zarbi et al., 2024). Smart card–based authentication architectures further enhance user authorization (Shalannanda et al., 2023). Nevertheless, most studies focus on cryptographic protocol development rather than integration with physical docking infrastructure in operational mobility systems.

From the monitoring perspective, IoT enables real-time telemetry acquisition and centralized supervision of distributed infrastructure (Lobato et al., 2022; Neis et al., 2023). IoT-based monitoring in EV charging stations has enhanced operational transparency and maintenance planning (Iqbal et al., 2024; Syafii et al., 2025). E-bike charging health monitoring approaches further demonstrate diagnostic capability (Jian et al., 2023; Hidayat et al., 2025). Infrastructure-level energy optimization has also been explored to improve system scalability (Balacco et al., 2021). However, these studies emphasize charging efficiency and telemetry rather than secure docking mechanisms with integrated authentication control.

Although research on IoT-enabled charging infrastructure and RFID authentication has progressed significantly (Singh et al., 2024; Bai & Dallasega, 2021), these components are generally treated independently. Charging infrastructure research focuses on energy management and communication performance, while RFID research prioritizes protocol security and computational efficiency. Smart campus studies often remain conceptual and lack deployable micro-mobility infrastructure implementations (Musa et al., 2021; Luckyardi et al., 2022; Domínguez-Bolaño et al., 2024). Consequently, integrated architectures combining physical docking mechanisms, authentication control, and IoT monitoring for campus e-bike systems remain limited.

A clear research gap therefore exists in developing an integrated e-bike docking infrastructure that simultaneously incorporates: (1) a structured physical docking mechanism, (2) secure RFID-based user authentication, and (3) IoT-enabled real-time monitoring within a unified smart campus mobility framework. Existing smart parking solutions do not fully address controlled energy access and docking alignment specific to e-bike ecosystems (Fahim et al., 2021; Fernandez et al., 2023), while charging research rarely embeds authentication mechanisms within the physical infrastructure layer.

To address this limitation, this study proposes the design and implementation of an IoT-based e-bike docking station equipped with RFID authentication tailored for smart campus mobility. The proposed architecture integrates a NodeMCU-based IoT controller, an RFID RC522 authentication module, and a web-based monitoring dashboard providing real-time operational data and usage logs. The novelty of this research lies in the integrated system architecture that unifies docking mechanics, secure user authentication, and IoT telemetry within a deployable campus-focused mobility infrastructure. The contribution of the research is the development and validation of a secure, observable, and scalable e-bike docking system capable of enhancing accountability, operational supervision, and governance of smart campus mobility services.

METHOD

System Design Framework

The proposed IoT-Based E-Bike Docking Station is designed using a distributed Internet of Things (IoT) architecture with centralized authentication control. This architectural approach ensures scalability, traceability, and governance within campus mobility infrastructure, consistent with smart campus implementation models (Domínguez-Bolaño et al., 2024; Neis et al., 2023). By adopting a layered IoT framework, the system separates physical device operations, communication processes, and application-level validation, enabling modular expansion and simplified maintenance.

This study prioritizes secure access control and infrastructure accountability rather than energy-monitoring functionality. The system architecture follows a client-server model where each docking unit operates as an IoT edge node responsible for RFID detection and actuator control, while authentication validation is performed centrally through a cloud-based server. Centralized validation enhances administrative control and reduces the risk of unauthorized access, as recommended in RFID-enabled IoT security frameworks (Gong et al., 2023; Shariq et al., 2021). In contrast to local UID matching stored directly in the microcontroller memory, centralized validation enables real-time access revocation and centralized audit tracking.

The architectural decision to use centralized HTTP-based validation rather than offline UID comparison is motivated by three considerations: (1) real-time revocation capability, allowing administrators to immediately disable lost or compromised RFID cards; (2) centralized audit logging, ensuring complete traceability of docking usage; and (3) scalability for multi-docking deployment across campus environments without manual configuration on each unit.

The overall layered system architecture of the proposed IoT-based E-Bike Docking Station is illustrated in Figure

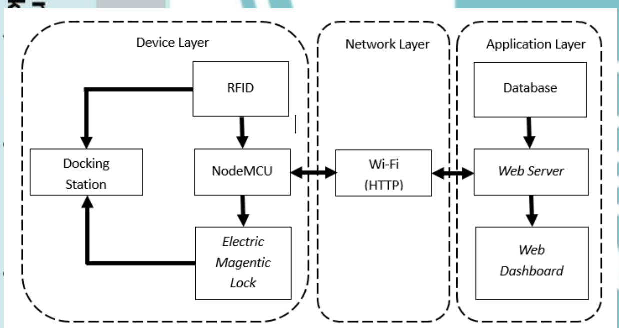

Fig. 1. Layered Architecture of IoT-Based E-Bike Docking Station with RFID Authentication

As shown in Figure 1, the architecture is divided into three logical layers. The Device Layer consists of the RFID reader (MFRC522), NodeMCU ESP8266 microcontroller and electric magnetic dock lock. These components collectively function as an edge node responsible for user identification and physical docking control. The RFID reader captures the user's unique identifier (UID), which is processed by the NodeMCU and transmitted for server-side validation. Upon receiving an authorization response, the NodeMCU activates or deactivates the relay controlling the magnetic dock mechanism.

The Network Layer handles wireless communication using the built-in Wi-Fi module of the ESP8266. HTTP protocol is employed for authentication request and response exchange between docking units and the central server. This approach balances implementation simplicity and system reliability for campus-scale deployment, as commonly adopted in IoT-based smart infrastructure systems (Neis et al., 2023).

The Application Layer comprises the authentication API, centralized database, and web-based administrative dashboard. The server validates UID requests against the registered user database and records access logs for monitoring and governance purposes. The web dashboard provides real-time system visibility, including access history and docking activity. This layered separation ensures modular system design, enhances scalability, and supports incremental deployment across multiple docking stations within the campus mobility ecosystem.

RFID Authentication and Control Algorithm

The RFID authentication mechanism represents the operational core of the proposed docking system. Unlike standalone access systems that rely on locally stored UID matching, this research adopts a centralized server-side validation model to ensure real-time authorization control and centralized logging (Gong et al., 2023; Zarbi et al., 2024). This design improves traceability and enables dynamic access revocation within campus mobility infrastructure.

The system operates using a request–validation–actuation paradigm. The RFID reader continuously monitors for card detection. Once a card is tapped, the unique identifier (UID) is extracted and transmitted to the NodeMCU controller. The microcontroller constructs an HTTP request containing the UID, docking station ID, and timestamp, and forwards it to the centralized authentication server. The server validates the UID against the registered database and generates a binary response indicating either authorization (VALID) or rejection (INVALID). Based on this response, the relay control state is updated to release or maintain the docking lock.

The operational workflow of the proposed RFID authentication and docking control mechanism is illustrated in Figure 2.

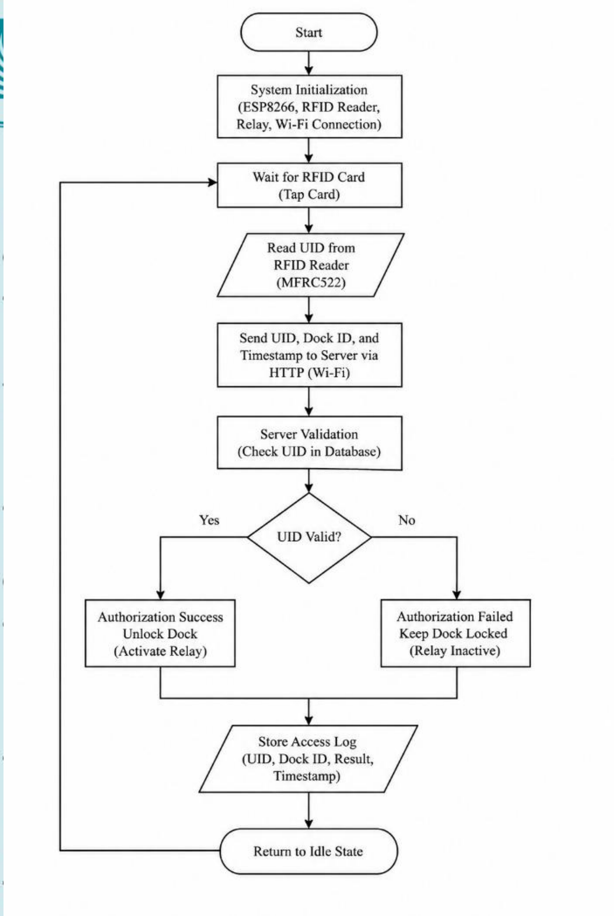

Fig. 2.RFID Authentication and Docking Control Flowchart

As shown in Figure 2, the authentication process begins when an RFID card is detected by the reader. The UID is then transmitted to the centralized server for validation. Based on the validation result, the system either unlocks the docking mechanism or denies access while maintaining the lock state. All authentication activities are recorded in the database before the system returns to idle state for the next authentication cycle.

To formally describe the operational behavior, the authentication logic is modeled as a finite state machine (FSM). The system transitions from idle state (waiting for RFID input) to UID detection, followed by server validation, and finally to either access granted (dock unlocked) or access denied (dock locked) state. After completing the actuation process, the system automatically returns to idle state. This state-based representation ensures deterministic behavior and simplifies debugging and scalability analysis.

Dock unlocking is governed by a binary relay control function. Let S_v denote the server validation result and R denote the relay state. The relay is activated (R = 1) if S_v indicates a valid user, and deactivated (R = 0) otherwise. To prevent unintended prolonged unlocking, a timeout policy is implemented. The relay remains active only within a predefined unlock duration (t_unlock), after which it automatically resets to locked condition. This time-based restriction enhances operational safety and maintains controlled access duration.

By delegating authentication to the centralized server, the system mitigates risks such as unauthorized UID duplication and delayed access revocation. Moreover, centralized logging enables comprehensive tracking of docking usage. The authentication structure remains compatible with lightweight IoT security practices suitable for embedded devices while allowing future integration of stronger encryption mechanisms if required.

Experimental Setup and Performance Evaluation

To evaluate the operational performance of the proposed IoT-based e-bike docking station, experimental validation was conducted under controlled campus simulation conditions. The prototype docking unit consisted of a NodeMCU ESP8266, MFRC522 RFID reader, relay module, and electric magnetic dock lock, connected to a centralized web server through a campus Wi-Fi network. Authentication logs were stored in a MySQL database and visualized via a web-based administrative dashboard.

Testing was performed using both registered and unregistered RFID cards to simulate authorized and unauthorized access scenarios. Each authentication cycle included RFID tap detection, UID transmission to the server, server-side validation, relay actuation decision, and activity logging. A total of 100 authentication attempts were conducted to assess system accuracy and responsiveness.

Authentication accuracy (A) was defined as:

$$A = \left(\frac{Correct\ Authorization}{Total\ Attempts}\right) \times 100\% \qquad (1)$$

This metric evaluates the correctness of server validation and docking actuation response. The authentication response time (T_response) was measured from the moment the RFID card was tapped until the magnetic dock lock was released or denied. The mean response time was calculated as:

$$T\_mean = (\Sigma\ T\_response)\ /\ N \qquad (2)$$

where N represents the total number of trials. The response time encompasses RFID reading delay, network transmission latency, server processing duration, and relay actuation time. Maintaining a response time below two seconds was considered acceptable for smooth campus mobility operation.

Communication reliability (R_comm) was evaluated as the ratio between successful server responses and total authentication requests:

$$R\_comm = \frac{Successful\ Server\ Responses}{Total\ Requests} \quad (3)$$

This metric reflects Wi-Fi communication stability between the docking node and centralized server.

Testing was conducted in an indoor campus environment with Wi-Fi signal strength ranging between –55 dBm and –65 dBm, without artificial network interference. The evaluation framework provides quantitative validation of authentication reliability, response latency, and communication stability of the proposed RFID-based docking control architecture..

RESULT AND DISCUSSION

The experimental validation was conducted to evaluate authentication reliability, response latency, communication robustness, and operational stability of the proposed IoT-based e-bike docking station. A total of 100 authentication trials were performed under campus Wi-Fi conditions, consisting of 60 authorized and 40 unauthorized access attempts.

Authentication Performance

The authentication results are summarized using a confusion matrix representation in Table 1.

Table 1. Authentication Confusion Matrix

Actual / Predicted	Authorized	Unauthorized
Authorized	59	1 (False Reject)
Unauthorized	1 (False Accept)	39

Based on Table 1, the following performance metrics were computed:

$$Accuracy = \frac{TP + TN}{Total} = \frac{59 + 39}{100} = 98\%$$

$$Precision = \frac{TP}{TP + FP} = \frac{59}{59 + 1} = 98.33\%$$

$$Recall = \frac{TP}{TP + FN} = \frac{59}{59 + 1} = 98.33\%$$

$$Specificity = \frac{TN}{TN + FP} = \frac{39}{39 + 1} = 97.5\%$$

The results indicate balanced authentication performance with minimal bias toward acceptance or rejection. The false reject event was primarily attributed to temporary network delay exceeding the timeout threshold during UID transmission. The false accept case occurred during a brief database synchronization interval, highlighting the importance of transactional integrity in centralized validation architectures.

Compared to RFID-based lightweight IoT authentication frameworks such as Gong et al. (2023) and Zarbi et al. (2024), which reported reliability within 97–99%, the proposed system achieves comparable accuracy while integrating physical electromechanical docking control and centralized logging mechanisms.

Response Time Statistical Analysis

Authentication response time was measured from RFID tap detection until magnetic dock release or denial. The statistical summary is presented in Table 2.

Table 2. Response Time Statistics

Parameter	Value
Minimum	0.79 s
Maximum	1.65 s
Mean	1.12 s
Standard Deviation	0.14 s
Variance	0.0196

The relatively small standard deviation indicates stable temporal performance across trials. The coefficient of variation (CV) was calculated as:

$$CV = \frac{\sigma}{\mu} = \frac{0.14}{1.12} = 12.5\%$$

A CV below 15% confirms acceptable temporal consistency for real-time access control systems.

Most authentication events were completed within 1.0–1.3 seconds, while the maximum observed value (1.65 s) was associated with temporary network congestion. Importantly, all response times remained below the predefined operational threshold of 2 seconds, ensuring smooth user interaction within campus mobility scenarios. Neis et al. (2023) reported IoT smart campus latency typically within 1–2 seconds, aligning with the observed mean latency of 1.12 seconds in this study.

Communication Reliability

During testing, 98 out of 100 authentication requests were successfully validated by the server. Communication reliability was therefore calculated as:

$$R_{comm} = \frac{98}{100} = 98\%$$

The two failed transmissions were attributed to short-duration Wi-Fi signal degradation within the –55 dBm to –65 dBm range. However, the implemented retry mechanism ensured automatic recovery without system freeze or hardware reset.

Although HTTP-based communication was selected for simplicity rather than protocol optimization, the achieved reliability demonstrates that event-driven request–response communication is sufficient for RFID-based docking authentication in campus-scale deployment.

Comparative Analysis with Related Works

Figure X presents the comparative performance analysis between the proposed system and related RFID-based IoT authentication studies. While Gong et al. (2023) and Zarbi et al. (2024) primarily focused on cryptographic optimization of RFID authentication protocols, the present study integrates authentication logic with physical docking control and centralized infrastructure governance.

Despite employing a lightweight HTTP-based validation approach rather than enhanced RFID cryptographic schemes, the achieved authentication accuracy (98%) remains within the same performance range reported in prior IoT authentication research. Furthermore, compared to smart parking implementations that primarily emphasize occupancy detection (Fahim et al., 2021), the proposed architecture enforces deterministic electromechanical docking release through identity validation.

In contrast to EV charging monitoring studies that focus on energy telemetry and optimization (Iqbal et al., 2024), this work addresses secure access governance within micro-mobility infrastructure. The integration of RFID authentication, relay-based docking actuation, and centralized logging constitutes the primary practical contribution of this research.

Overall, the experimental findings confirm that centralized RFID authentication integrated with lightweight IoT hardware achieves high reliability (98%), stable response latency (~1.12 s), and consistent communication performance. The minor performance deviations observed were primarily network-induced rather than algorithmic, indicating that further improvement should focus on network optimization rather than redesigning authentication logic. These results validate the feasibility of deploying the proposed system within campus-scale mobility infrastructure.

CONCLUSION

This study proposed and experimentally validated an IoT-based e-bike docking station with centralized RFID authentication for smart campus mobility infrastructure. The system adopts a distributed edge-to-cloud architecture in which each docking unit functions as an IoT node while authentication validation is performed through a centralized server. This architecture enhances administrative control, enables real-time access revocation, and supports scalable multi-docking deployment.

Experimental results demonstrate that the proposed system achieves 98% authentication accuracy, with precision and recall values exceeding 98%, indicating balanced performance in both acceptance and rejection scenarios. The mean authentication response time was measured at 1.12 seconds, with a coefficient of variation of 12.5%, confirming stable and responsive operation under campus Wi-Fi conditions. Communication reliability reached 98%, demonstrating that HTTP-based request–response architecture is sufficient for event-driven access control applications.

Compared to prior RFID-based IoT authentication studies that primarily focus on protocol optimization, this research integrates authentication logic with electromechanical docking control and centralized logging infrastructure. The results confirm that lightweight IoT hardware combined with centralized validation provides a practical and scalable solution for secure micro-mobility infrastructure governance within smart campus environments.

Future work may focus on enhancing communication resilience, integrating stronger encryption mechanisms, and extending the system toward multi-node deployment with load-balanced server architectures to further improve reliability and scalability.

Author Contribution: All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.
Funding: This research received no external funding.
Acknowledgment: The author teamwould like to express our deepest gratitude to all those who have contributed to the completion of this research. Our sincere appreciation goes to Polytechnic STMI Jakarta for providing the facilities and support necessary for this project..
Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

Abdellaoui Alaoui, E. A., & Tekouabou, S. C. K. (2021). Intelligent management of bike sharing in smart cities using machine learning and Internet of Things. *Sustainable Cities and Society, 67*, 102702. https://doi.org/10.1016/j.scs.2020.102702

Balacco, G., Totaro, V., & Piccinni, A. F. (2021). Pumps as turbine for energy recovery in water distribution networks: A case study for e-vehicle charging stations. *Sustainability,* 13(4), 1847. https://doi.org/10.3390/su13041847

Christian, H., Yusuf, Y. G., & Ainul, R. D. (2025). An IoT-enabled bicycle access and monitoring system with geo-fence-based location restriction. *IJEEEMI, 7*(4), 619–629. https://doi.org/10.35882/ijeeemi.v7i4.123

Domínguez-Bolaño, T., Pérez-Castillo, R., Piattini, M., & García, F. (2024). An IoT system for a smart campus: Challenges and solutions illustrated over several real-world use cases. *Internet of Things, 26*, 101099. https://doi.org/10.1016/j.iot.2024.101099

Fahim, A., Hasan, M., & Chowdhury, M. A. (2021). Smart parking systems: Comprehensive review based on various aspects. *Heliyon, 7*(5), e07050. https://doi.org/10.1016/j.heliyon.2021.e07050

Fernandez, S., Erwadi, Y., & Erlangga, F. (2023). Smart parking system model analysis with NodeMCU and IoT-based RFID. *JUITA: Jurnal Informatika, 11*(1). https://doi.org/10.30595/juita.v11i1.16908

Ghorpade, S. N., Zennaro, M., & Chaudhari, B. S. (2021). GWO model for optimal localization of IoT-enabled sensor nodes in smart parking systems. *IEEE Transactions on Intelligent Transportation Systems,* 22(2), 1217–1224. https://doi.org/10.1109/TITS.2020.2964604

Gong, Y., Zhang, Y., Li, X., & Xue, G. (2023). An adaptive, lightweight, secure, and efficient RFID-based authentication scheme for IoV. *Sensors, 23*(11), 5198. https://doi.org/10.3390/s23115198

Hidayat, M. N., Nugroho, A., Munir, A. F., & Putri, R. I. (2025). Internet of things (IoT) based monitoring system for hybrid powered e-bike charging station. *International Journal of Power Electronics and Drive Systems,* 16(1), 243–250. https://doi.org/10.11591/ijpeds.v16.i1.pp243-250

Hossein Sabbaghian, M., Llopis-Castelló, D., & García, A. (2023). A safe infrastructure for micromobility: The current state of knowledge. *Sustainability, 15*(13), 10140. https://doi.org/10.3390/su151310140

Iqbal, S., Alshammari, N. F., Shouran, M., & Massoud, J. (2024). Smart and sustainable wireless electric vehicle charging strategy with renewable energy and Internet of Things integration. *Sustainability, 16*(6), 2487. https://doi.org/10.3390/su16062487

Jabbar, W. A., Tiew, L. Y., & Ali Shah, N. Y. (2024). Internet of things enabled parking management system using long range wide area network for smart city. *Internet of Things and Cyber-Physical Systems, 4*, 82–98. https://doi.org/10.1016/j.iotcps.2023.09.001

Jian, X., Yang, L., Li, Y., Chen, Y.-C., & Xue, G. (2023). SingMonitor: E-bike charging health monitoring using sound from power supplies. *Applied Sciences, 13*(5), 3087. https://doi.org/10.3390/app13053087

Lobato, E., Costa, A., & Medeiros, A. (2022). A monitoring system for electric vehicle charging stations: A prototype in the Amazon. *Energies, 16*(1), 152. https://doi.org/10.3390/en16010152

Luckyardi, S., Hurriyati, R., Disman, & Dirgantari, P. D. (2022). A systematic review of the IoT in smart university: Model and contribution. *Indonesian Journal of Science and Technology, 7*(3), 529–550. https://doi.org/10.17509/ijost.v7i3.51476

Mudra, G., Cui, H., & Johnstone, M. N. (2023). Survey: An overview of lightweight RFID authentication protocols suitable for the maritime Internet of Things. *Electronics,* 12(13), 2990. https://doi.org/10.3390/electronics12132990

Musa, M., Ismail, M. N., & Md Fudzee, M. F. (2021). A survey on smart campus implementation in Malaysia. *JOIV: International Journal on Informatics Visualization,* 5(1), 51–56. https://doi.org/10.30630/joiv.5.1.434

Neis, P., Warch, D., & Hoppe, M. (2023). Testing and evaluation of low-cost sensors for developing open smart campus systems based on IoT. *Sensors, 23*(20), 8652. https://doi.org/10.3390/s23208652

Oliveira, F., Teixeira, J., & Sousa, A. (2021). A survey of technologies and recent developments for sustainable smart cycling. *Sustainability,* 13(6), 3422. https://doi.org/10.3390/su13063422

Permana, A. A., & Priatna, R. (2025). Smart bike parking station menggunakan RFID berbasis Internet of Things. *Telekontran,* 13(2). https://doi.org/10.34010/telekontran.v13i2.16089

Shalannanda, A., Sulaeman, B., & Sutanto, A. (2023). Smart card-based access control system using isolated many-to-many authentication scheme. *Journal of ICT Research and Applications,* 17(2). https://doi.org/10.5614/itbj.ict.res.appl.2023.17.2.8

Shariq, M., Singh, K., Bajuri, M. Y., Pantelous, A., Ahmadian, A., & Salimi, M. (2021). A secure and reliable RFID authentication protocol using Schnorr digital cryptosystem for IoT-enabled healthcare in COVID-19 scenario. *Sustainable Cities and Society, 75*, 103354. https://doi.org/10.1016/j.scs.2021.103354

Singh, A. R., et al. (2024). Electric vehicle charging technologies, infrastructure, and challenges: A review. *Journal of King Saud University – Engineering Sciences*. https://doi.org/10.1016/j.jksues.2024.04.001

Syafii, S., et al. (2025). Enhancing electric vehicle charging stations by integrating IoT technology

(Raspberry Pi-based monitoring). *Journal of Sustainable Development of Energy, Water and Environment Systems*. https://www.sdewes.org/jsdewes/pid13.0609

Zarbi, N., Alzahrani, B. A., & Elhoseny, M. (2024). Toward designing a lightweight RFID authentication protocol for constrained environments. *IET Communications*. https://doi.org/10.1049/cmu2.12794