Design and Implementation of an IoT-Enabled Automatic Token Counting Machine for Metro Systems

Phi Van Lam
Faculty of Electrical and Electronic Engineering, University of Transport and Communications, Hanoi, Vietnam
pvlam@utc.edu.vn (corresponding author)

Tran Thi Lan
Faculty of Electrical and Electronic Engineering, University of Transport and Communications, Hanoi, Vietnam
ttlan@utc.edu.vn

Trinh Luong Mien
Faculty of Electrical and Electronic Engineering, University of Transport and Communications, Hanoi, Vietnam
mientl@utc.edu.vn

Received: 24 January 2026 | Revised: 13 February 2026 and 26 February 2026 | Accepted: 28 February 2026

 DOI: https://doi.org/10.48084/etasr.17737

ABSTRACT

This study presents the design, implementation, and experimental validation of an Internet of Things (IoT)-enabled automatic token counting system based on a synchronized optical–Radio Frequency Identification (RFID) dual-verification architecture. Unlike conventional optical-only systems, which are vulnerable to token overlap and vibration, or RFID-only systems, which suffer from read collisions and duplicate Unique Token Identification (UID) detection, the proposed approach introduces a temporally synchronized validation window in which optical interruption events trigger controlled RFID UID acquisition. This mechanism establishes a deterministic one-to-one mapping between physical token movement and digital identification, significantly improving robustness under high-density batch conditions. The system integrates an ESP32-based embedded controller, opto-electronic sensing, ISO/IEC 14443-compliant passive RFID tags, and a cloud-connected MariaDB database with an ASP.NET monitoring dashboard for real-time supervision and data logging. Design parameters, including motor speed, token spacing, and RFID verification window timing, are analytically justified and experimentally optimized to ensure stable operation. Experimental evaluation conducted with batch sizes of up to 250 tokens demonstrates 100% counting accuracy across repeated trials, with an average throughput of 500 tokens/min and stable real-time data synchronization. A comparative analysis confirms that the proposed synchronized dual-verification strategy improves accuracy, collision robustness, and traceability relative to optical-only, RFID-only, and vision-based approaches while maintaining low implementation costs. The results validate the feasibility and scalability of the proposed architecture for practical metro fare management systems and provide a deployable framework for secure and large-scale Automated Fare Collection (AFC)infrastructures.

Keywords-automatic fare collection; optical–RFID fusion; embedded IoT systems; real-time token counting; smart metro systems; applied transportation engineering

I. INTRODUCTION

Metro networks significantly contribute to sustainable urban mobility, helping to alleviate congestion and reduce emissions. In Vietnam, the Nhon–Hanoi Metro has modernized public transportation, and is expected to serve over 65,000 passengers per day during its initial phase. However, the operational efficiency of such systems relies heavily on accurate AFC. Ticket control and token counting in Vietnamese metro stations are mostly manual, leading to potential errors, time delays, and higher labor costs. These shortcomings highlight the need for a reliable, automated

solution that integrates sensing, computation, and communication for real-time fare management.

Authors in [1] investigated AFC systems in public transportation, emphasizing their importance in improving passenger throughput and operational efficiency. Authors in [2] proposed an efficient anonymous authentication protocol for RFID, which strengthened data privacy and integrity in fare systems. Authors in [3] implemented an Advanced RISC Machine (ARM)-based AFC prototype that demonstrated the feasibility of embedded microcontroller platforms for ticket validation. However, such sensor-based systems often lacked IoT connectivity and cloud integration, limiting centralized monitoring and scalability.

The introduction of RFID and IoT technologies was a great advancement in AFC systems. Authors in [4] highlighted lightweight RFID security mechanisms without extensive cryptography, enabling faster data processing for embedded devices, while authors in [5] developed an RFID-based e-ticketing framework for buses using IoT to automate passenger data collection. Authors in [6] proposed an IoT-based counting system that integrates sensor data for real-time supervision and automatic record synchronization. These studies demonstrated the growing trend toward networked, data-driven AFC architectures.

Beyond sensing and communication, researchers have also addressed system-level optimization and smart data utilization. Author in [7] analyzed IoT-based railway data to improve transport analytics and decision-making efficiency, while authors in [8] integrated blockchain and IoT sensor networks to measure and monitor smart infrastructure, ensuring transparency and reliability. Authors in [9] introduced an IoT-enabled AFC architecture that unified payment, sensing, and monitoring layers into a single integrated system. Authors in [10] further developed a smart ticketing framework integrating RFID, Global Positioning System (GPS), and cloud synchronization, which enhanced scalability and real-time analytics for public transport systems.

Developments in intelligent transportation and fare validation algorithms have further advanced automation and system dependability. Authors in [11] reviewed smart infrastructure and passenger-counting technologies that could complement fare collection automation, and authors in [12] proposed an RFID-based ticketing system tailored for metro operations to enhance throughput and minimize fraud. Authors in [13] investigated real-time fare validation algorithms, addressing latency and synchronization challenges in large-scale AFC deployments. Authors in [14] developed a blockchain-enhanced, privacy-preserving e-ticket system for IoT devices, addressing unlinkability and double-spending detection in large-scale deployments. Moreover, research on blockchain applications in intelligent transportation systems highlights transparency and trust enhancements in IoT-enabled ITS via distributed ledgers [15].

Several enabling technologies for RFID- and IoT-based automated systems have been investigated. Authors in [16] analyzed a compact electrically small antenna incorporating Split-Ring Resonator (SRR) structures for RFID applications, demonstrating improved miniaturization and impedance matching suitable for space-constrained deployments. Authors in [17] addressed RFID reader performance by proposing a miniaturized circularly polarized patch antenna, which enhances polarization tolerance and reading reliability under varying tag orientations. These studies contribute to improving the physical-layer efficiency of RFID systems, which is crucial for reliable identification in automated environments. Beyond antenna and RFID hardware design, IoT-based automated monitoring, control systems for Electrical Conductivity (EC), and pH in NFT-based farms have been utilized. These studies demonstrated effective integration of embedded sensing, microcontroller-based control, and cloud-connected data visualization, highlighting the applicability of IoT architectures for real-time supervision and autonomous operation.

Although these studies validate the feasibility of RFID hardware optimization and IoT-based monitoring frameworks, they primarily focus on individual system components or application-specific domains. The integration of high-throughput object counting, token-level identification, and real-time cloud synchronization in transportation-oriented fare collection systems is relatively unexplored. To address these gaps, the present study proposes a fully integrated IoT-enabled automatic token counting system that synchronizes optical sensing with RFID UID verification, specifically designed to meet the operational requirements of metro-scale fare management.

Despite significant advancements, several limitations are evident in current AFC research. First, many existing solutions focus on isolated subsystems, such as sensing, communication, or data analytics, without integrating the entire hardware–software–IoT pipeline into a unified and deployable platform. Second, most reported prototypes target bus transportation or laboratory-scale experiments, with limited validation under the harsh operational conditions of metro environments characterized by high token density, mechanical vibration, and continuous operation. Third, few systems provide real-time cloud-based monitoring while simultaneously maintaining token-level traceability and effective anti-overlap mechanisms during batch token handling. A qualitative comparison of representative approaches is summarized in Table I.

As shown in Table I, existing AFC token counting approaches exhibit inherent trade-offs. Optical gate systems provide reliable mechanical detection but lack token-level traceability. RFID-only systems enable identification but are vulnerable to read collision and duplicate UID acquisition under dense batch conditions. Vision-based systems can detect overlap events but introduce higher computational complexity and implementation costs. The proposed synchronized optical–RFID fusion mechanism integrates physical passage confirmation with UID-level verification in a deterministic sequence. This architecture ensures token-level traceability, real-time cloud synchronization, and anti-overlap capability simultaneously, while maintaining moderate hardware complexity and practical deployability.

TABLE I. COMPARISON OF REPRESENTATIVE AFC TOKEN COUNTING SYSTEMS

System	Counting method	Token-level traceability	Real-time cloud sync	Anti-overlap mechanism
Coin discriminator [18]	Optical break-beam	No	No	Yes
RFID-only system [12]	RFID scan	Yes	No	No
Vision-based system [11]	Camera	No	Yes	Yes
Proposed system	Optical–RFID fusion	Yes	Yes	Yes

To address miscounting in dense-batch AFC token processing, this study presents the design and experimental validation of an IoT-enabled automatic token counting system developed for the Nhon–Hanoi Metro. The proposed architecture synchronizes optical interruption events with RFID UID validation, ensuring deterministic one-to-one correspondence between physical token movement and digital identification. The system is implemented using an ESP32 microcontroller and integrated with a cloud-based MariaDB database and web dashboard for real-time monitoring and logging. The experimental results demonstrate 100% counting accuracy for batch sizes of 200–300 tokens under realistic operating conditions.

The main contributions of this work are: (1) a synchronized optical–RFID dual-verification architecture that enhances counting reliability and token-level traceability, (2) an integrated hardware–software–IoT platform tailored for metro fare management, and (3) experimental validation confirming stable operation and reliable cloud synchronization suitable for practical AFC deployment.

Unlike optical-only, RFID-only, or vision-based approaches, which suffer from overlap errors, UID collisions, or higher complexity, the proposed method binds physical detection to digital identity acquisition. The device is deployed in the metro operator's warehouse and coordination center for backend token inventory verification and inter-station reconciliation; it does not perform passenger counting. By integrating synchronized sensing, embedded control, and IoT supervision into a unified platform, this work provides a practical solution for modern metro fare management.

II. DESIGN AND IMPLEMENTATION

The development follows a top-down engineering approach, starting from system-level requirement analysis and architectural design, followed by hardware–software integration and experimental verification under realistic operating conditions. The primary design objective is to overcome the inherent limitations of conventional single-sensor AFC systems. Optical-based counting mechanisms provide high throughput but are prone to miscounting due to token overlap, mechanical vibration, and unstable feeding conditions. In contrast, RFID-based systems enable token-level identification but suffer from signal collision and repeated UID readings during dense batch handling. To address this important trade-off, the proposed system adopts a dual-verification design philosophy, in which optical sensing and RFID identification are temporally synchronized rather than independently processed. This synchronized architecture ensures a one-to-one correspondence between physical token movement and digital identification, thereby improving counting reliability and traceability.

Based on this design rationale, the system architecture integrates mechanical token transport, synchronized optical–RFID sensing, embedded control, and IoT-based monitoring into a unified platform. The key design parameters of the proposed system were experimentally selected to ensure stable operation and reliable synchronization. The RFID verification window was determined based on the measured traversal time of tokens across the sensing region. A small safety margin was included to accommodate RFID read latency and mechanical variations while preventing duplicate UID acquisition. The mechanical guide channel ensures that tokens move sequentially along a single path, preventing parallel passage through the sensing region. The minimum spacing between tokens was experimentally verified to avoid RFID read collision. The TFT display updates the counting results and UID logs every 1 s. This refresh rate applies only to visualization and does not affect the real-time dual-verification logic executed at the embedded firmware level.

A. The Proposed IoT-Enabled Automatic Token Counting System

The proposed IoT-enabled automatic token counting system is designed to achieve high counting accuracy, token-level traceability, and real-time supervision under practical metro operating conditions. As illustrated in Figure 1, the system architecture is organized around a set of tightly coordinated functional modules that collectively implement a dual-verification counting mechanism, in which optical sensing and RFID identification are synchronized to validate each counting event. The overall system consists of the functional blocks, as depicted in Figure 1. The coordination of these functional blocks results in a high-precision and fully automated token counting system. By synchronizing optical and RFID sensing, the proposed architecture significantly reduces miscounting caused by token overlap, vibration, or dense batch handling, while maintaining full token-level traceability and real-time data transmission. After defining the system architecture, the hardware configuration was designed and validated using SolidWorks. As displayed in Figure 2, the automatic token counting device integrates the following main components:

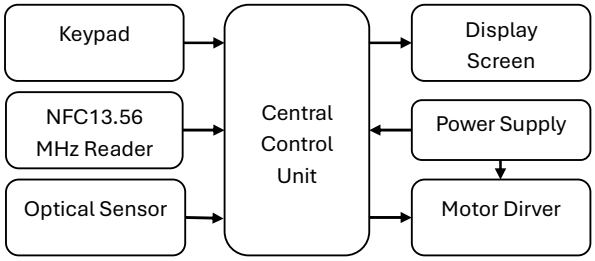

Fig. 1. Architecture of the IoT-enabled automatic token counting system.

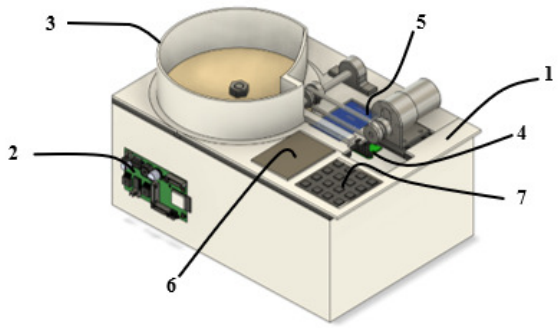

Fig. 2. Proposed IoT-enabled automatic token counting device.

1) Motor Assembly (1)

Motor assembly provides a mechanical drive for token transport, ensuring continuous movement through the sensing area. The DC motor operates at 240 rpm after gearbox reduction, experimentally determined to achieve stable serialized feeding without overlapping or excessive vibration while maintaining adequate throughput. Token tray motion is controlled by dual BTS7960B high-current H-bridge drivers, enabling bidirectional DC motor operation. These drivers provide overcurrent protection, thermal shutdown, and high current capability for stable continuous operation. PWM signals from the ESP32 regulate speed and direction via the IN and EN pins. Pull-down resistors are added to prevent unintended activation due to noise or floating inputs, as demonstrated in Figure 3.

2) Central Control Module (2)

The ESP32 serves as the core processing unit, implementing embedded control, synchronized sensing logic, and IoT communication. It processes sensor data, controls motor operation, manages user inputs and display interaction, and executes the dual-verification mechanism in which optical events trigger RFID UID acquisition. Using its built-in Wi-Fi capability, validated counting results are transmitted to the remote server for real-time monitoring.

3) Token Tray and Motor Structure (3)

The token tray stores the tokens and guides them along a predefined path toward the sensing modules. The tray geometry is optimized to minimize token overlap and mechanical jamming during batch feeding.

4) Token Counting Sensor Module (4)

The token-counting sensor contains an optical emitter–receiver pair that detects token passage via light interruption. Rather than directly incrementing the count, the sensor acts as a temporal trigger for RFID UID verification within a defined detection window. The detection threshold is experimentally calibrated and adjusted during initialization to ensure stable operation under varying ambient lighting conditions and continuous batch processing.

5) RFID Sensor Module (5)

The sensor module reads the UID of each token within the optically defined verification window. Upon optical triggering, the reader acquires the token's unique RFID code, and only UIDs detected within this window are accepted as valid. This synchronized mechanism ensures one-to-one correspondence between physical token passage and digital identification, reducing false multiple readings caused by collision or interference. Logged UID data support traceability and statistical analysis.

6) Display Module (6)

The display module serves as the human–machine interface using a TFT screen to present the preset batch size, current token count, operating mode, and alert notifications. It enables operators to monitor the synchronized counting process and promptly detect abnormal conditions.

7) Data Input Module (Keypad) (7)

The keypad enables secure user authentication and configuration of operational parameters, such as the target batch size. These inputs are processed by the central control unit to initialize and manage the synchronized counting sequence.

This integrated mechanical–electronic architecture provides an efficient and scalable platform for stable, high-accuracy token management. Its modular design supports maintenance and future expansion, while the synchronized optical–RFID mechanism ensures reliable and traceable operation in metro environments.

B. Central Control Module Design

Figure 3 presents the schematic of the central control module, illustrating the electrical connections among the ESP32, motor drivers, power regulators, sensors, and peripheral interfaces. Figure 4(a) shows the 2D PCB layout designed in Altium Designer. The layout separates high-current motor paths from low-voltage signal traces to reduce electromagnetic interference and voltage drop. Motor driver traces are widened and thermally reinforced, while sensor and communication lines are carefully routed to maintain signal integrity. Decoupling capacitors are placed close to the ESP32 and BTS7960B drivers, and optimized ground planes are implemented to suppress noise and improve heat dissipation.

Figure 4(b) presents the assembled PCB model, highlighting the spatial organization of critical components. The ESP32-WROOM-32 module is positioned centrally to balance routing and thermal distribution. The BTS7960B motor drivers are located near the power connectors to minimize resistance and heat accumulation. The system is powered by a 220 VAC supply converted to 24 VDC for the main power rail. The LM2576S-5.0 and AMS1117-3.3 regulators are positioned away from sensitive logic circuits to isolate power regulation. Connector headers are arranged along the PCB edges for modular interfacing, while status LEDs and push buttons remain accessible for diagnostics and manual control. The integrated electrical and mechanical design enhances noise immunity, thermal stability, and manufacturability under continuous operation. By combining synchronized sensing logic, motor control, and IoT communication on a single control board, the module serves as the backbone of the proposed automatic token counting system.

C. Operating Principle of the Automatic Token Counting System

The operating principle of the proposed automatic token counting system is based on a synchronized optical–RFID dual-verification mechanism, which guarantees accurate token counting, token-level traceability, and real-time IoT monitoring. The detailed operational flow is illustrated in Figure 5 and consists of a sequence of deterministic control states managed by the central control module.

1) System Initialization and Parameter Configuration

In this step, the operator enters authentication credentials and the target batch size using the Data Input Module (keypad). These parameters are transmitted to the Central Control Module, where system variables are initialized, counters are reset, and operating thresholds are validated. If the entered batch size is zero or invalid, the system automatically enters a reconfiguration state and prompts the user to re-enter valid parameters.

2) Token Transport and Motion Control

Upon successful initialization, the Central Control Module activates the Tray and Motor Assembly to transport tokens from the storage tray toward the sensing channel. Motor speed and rotation direction are regulated through PWM signals generated by the ESP32 and applied to the BTS7960B motor drivers. This controlled motion ensures uniform token spacing and minimizes mechanical overlap before sensing.

3) Optical Triggering and Event Detection

In this step, each token passing through the sensing channel interrupts the optical beam of the Counting Sensor Module. This interruption is treated as a physical trigger rather than an immediate count increment. Upon detecting a valid optical transition, the Central Control Module timestamps the event and opens a predefined verification time window for identity confirmation.

4) RFID-Based Identity Verification

While the verification window is active, the RFID Sensor Module is enabled to scan for a UID. If a valid UID is detected within the allowed time window, the system confirms the presence of a legitimate token and increments the count by one. The UID is then temporarily buffered to prevent duplicate counting caused by repeated RFID reads. Optical events without corresponding RFID validation are discarded, effectively eliminating false counts due to vibration, token overlap, or mechanical noise.

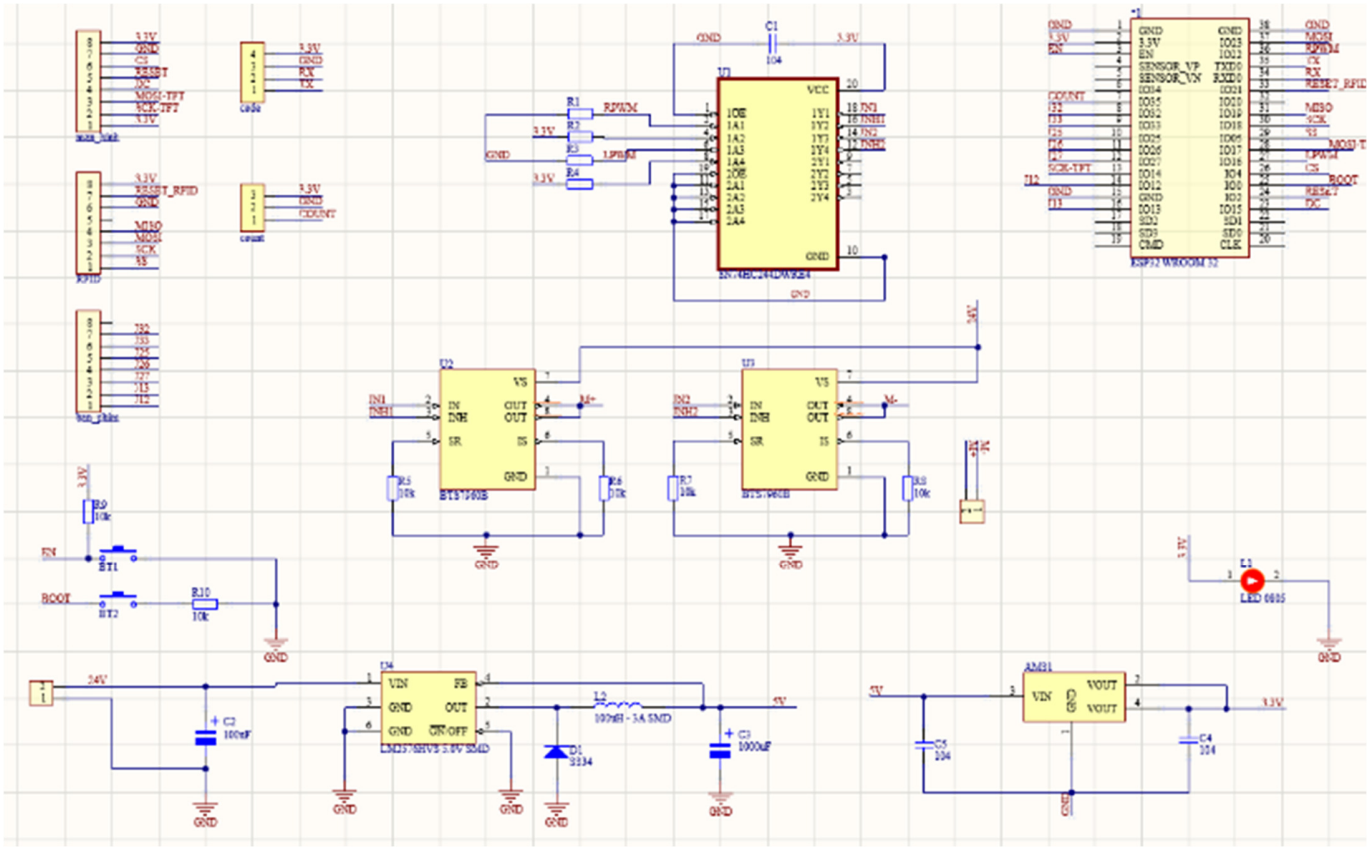

Fig. 3. Schematic of the central control module.

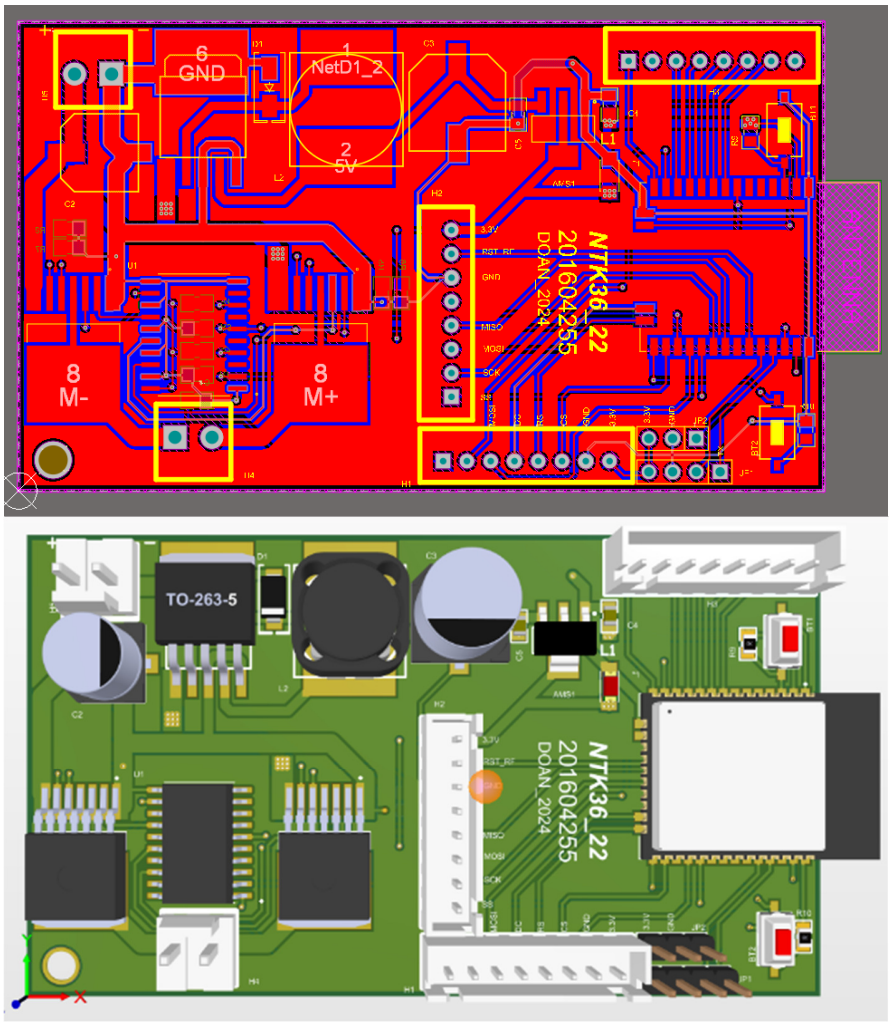

Fig. 4. PCB layout of the central control module: (a) 2D design, (b) 3D assembled board.

5) Batch Completion and Control Decision

In this step, the verified token count is continuously compared against the preset batch quantity stored in the Central Control Module. Once the two values match, the system automatically disables the motor driver, halting token transport and concluding the counting cycle. This closed-loop comparison ensures precise batch-level control without operator intervention.

6) IoT Data Transmission and Visualization

During data transmission, all validated data—including token UIDs, total counts, timestamps, and system status—are transmitted via Wi-Fi to the remote server. The data are stored in a cloud-based MariaDB database and visualized in real time through the ASP.NET web dashboard. This enables remote supervision, historical analysis, and operational auditing of fare collection processes.

7) Result Display and System Reset

The final batch results are displayed on the Display Module, showing the processed quantity, system status, and any warning notifications. The system then transitions to an idle state, ready to accept the next batch command.

8) Fault Handling and Safety Mechanisms

To enhance robustness under real-world operating conditions, multiple fault-handling mechanisms are incorporated. If the RFID module detects an unidentified or defective token, a warning is generated and logged in the system. In the event of mechanical obstruction or token jamming, the control logic automatically initiates a brief reverse rotation of the motor to clear the blockage and restore normal operation. These protective measures ensure continuous and reliable system performance during long-term deployment.

Through this synchronized, state-based operating sequence, the proposed system achieves high counting accuracy, eliminates miscounting caused by sensor ambiguity, and enables real-time IoT supervision. The operating principle demonstrates how the integration of optical triggering, RFID verification, and embedded control logic forms a reliable solution for AFC in metro environments.

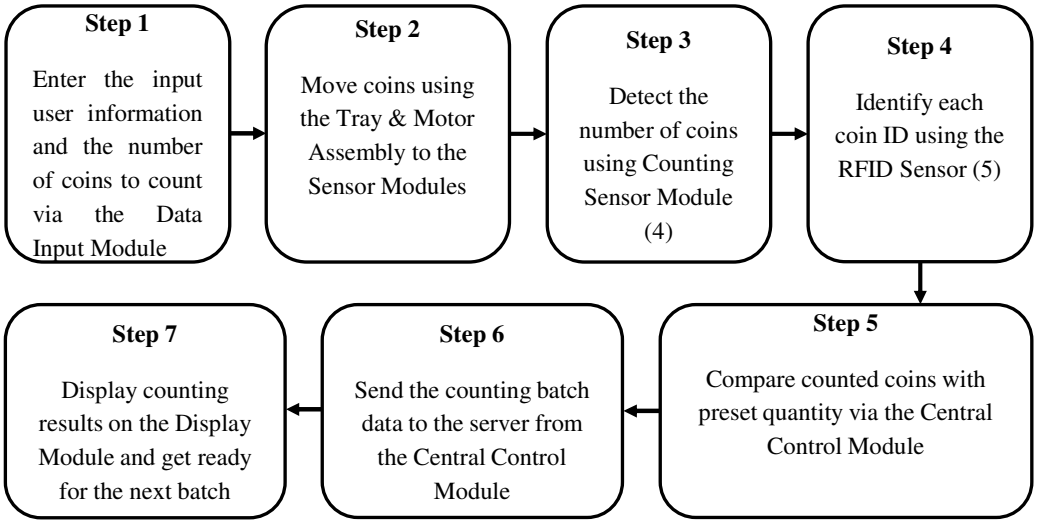

Fig. 5. Activity diagram of the backend RFID metro token detection and counting process.

The proposed system does not perform passenger detection at metro gates. Instead, it is designed for backend batch processing of collected RFID-enabled metro tokens. The system detects and counts physical tokens through synchronized optical and RFID verification before updating the central information system. Algorithm 1 presents the workflow of dual-verification optical–RFID token counting:

```
Algorithm 1: Dual-Verification Optical-RFID Token Counting Algorithm
Input:
Target batch size N_target
Optical sensor signal S_opt
RFID UID stream UID_rfid
Output:
Verified token count N_count
Token UID log
System status flag
Initialization:
Set N_count ← 0
Clear UID buffer and event flags
Validate N_target > 0; if invalid, request reconfiguration
Enable motor drive
Main Control Loop:
while N_count < N_target do
    Monitor optical sensor state S_opt
    if optical beam interruption is detected, then
        Timestamp optical event t_opt
        Open verification window [t_opt, t_opt + ΔT]
        Enable the RFID reader
        if a valid UID is detected within ΔT then
            if UID is not in the recent UID buffer, then
                Increment N_count ← N_count + 1
                Store UID with timestamp
                Update cloud database asynchronously
            end if
        else
            Discard optical event (false trigger)
        end if
        Disable the RFID reader
    end if
end while
Batch Completion:
1. Disable motor drive
2. Transmit final batch data to the cloud server
3. Display the counting result and the system status
Fault Handling:
if RFID UID is unreadable or duplicated, then
    Trigger warning and log event
end if
if motor stall or mechanical obstruction is detected, then
    Reverse motor rotation for a predefined duration
    Resume normal operation
end if
```

The verification window ΔT was empirically selected to accommodate mechanical vibration and RFID read latency while preventing duplicate detection.

D. Database Management Interface

Figure 6 illustrates the structure of the online database implemented using MariaDB, which serves as the data storage, synchronization, and management layer of the proposed IoT-enabled automatic token counting system. The database acts as

a centralized repository that receives validated token data from the embedded control module via Wi-Fi, ensuring real-time consistency between physical counting operations and cloud-based monitoring. MariaDB was selected due to its high transaction throughput, open-source flexibility, and compatibility with IoT-oriented web frameworks. In the proposed system, database interaction is event-driven: only verified token events, confirmed by the dual optical–RFID mechanism, are transmitted and committed to the database. This design prevents false records caused by sensor noise, communication retries, or duplicated RFID reads.

1) Database Schema and Data Organization

All operational data are organized under the schema "nguyentrankhai_dulieu", which contains a relational table designed to support traceability, batch-level management, and efficient querying. The table consists of five primary fields:

a) ID

ID acts as the primary key of the table, uniquely identifying each transaction record. The AUTO_INCREMENT attribute ensures sequential indexing, facilitating efficient storage, retrieval, and chronological ordering of batch operations.

b) HoVaTen (Name)

This field stores the name or identifier of the system operator associated with each counting session. The VARCHAR data type provides flexibility for user identification while maintaining compact storage and fast query performance.

c) SoLuongLay (Quantity Taken)

Quantity taken records the total number of tokens processed during a complete batch operation. This value is computed by the embedded controller based on verified optical–RFID events and transmitted to the server only after batch completion, ensuring consistency between local and cloud counters.

d) XuID (Token ID)

This field contains the list of unique RFID identification codes corresponding to all verified tokens within a batch. The MEDIUMTEXT data type is selected to accommodate variable-length UID lists while preserving data integrity for auditing and traceability purposes.

e) ThoiGianLay (Pickup Time)

Pickup time Logs the timestamp associated with each counting session. This field enables chronological tracking, performance analysis, and operational auditing, which are essential for long-term supervision of fare collection activities.

2) Data Synchronization and Transaction Flow

During system operation, the ESP32 microcontroller transmits validated counting data to the server through an asynchronous HTTP-based interface. Data packets are generated only after successful dual-verification and batch completion, reducing unnecessary network traffic and preventing partial or inconsistent records. Upon reception, the server-side application inserts the data into the MariaDB table as a single transaction, ensuring atomicity and consistency. This database-centric architecture enables real-time visualization of system status through the web dashboard while maintaining a reliable historical record for statistical analysis and system optimization. By decoupling physical sensing from cloud storage and enforcing verification at the embedded level, the proposed database interface enhances robustness, scalability, and transparency in AFC systems.

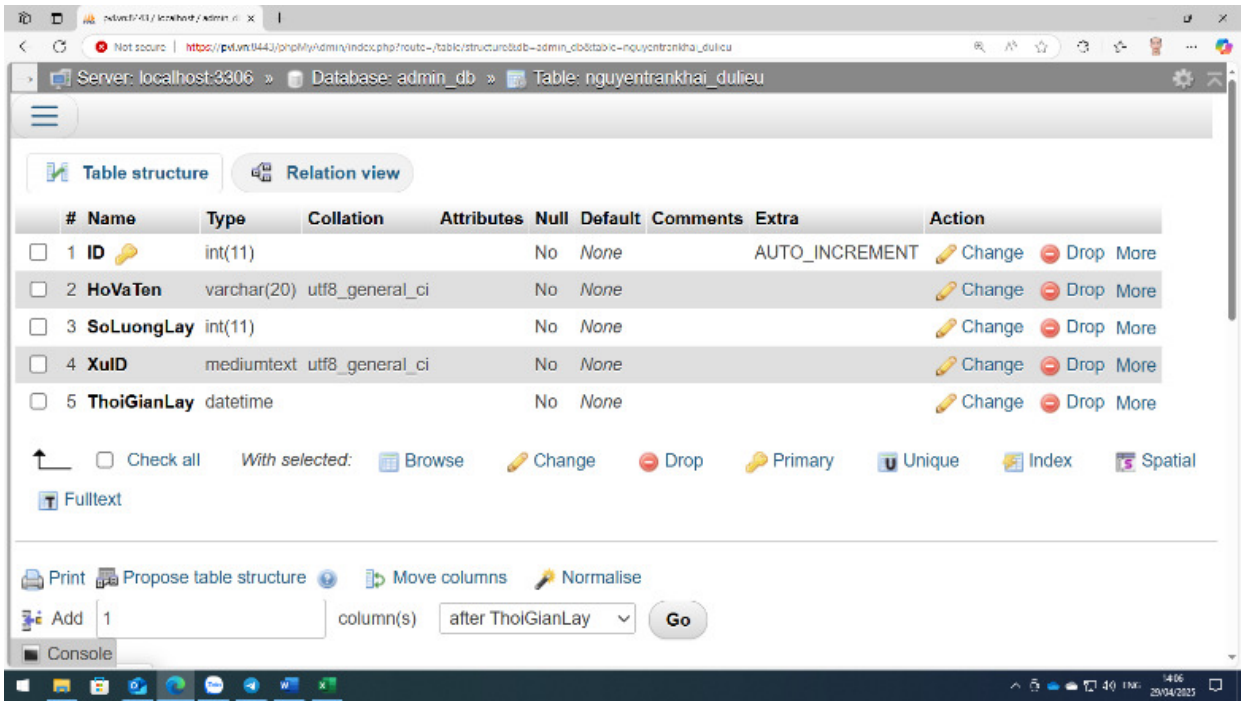

Fig. 6. Online database design on MariaDB.

This relational database design ensures both scalability and data integrity by enforcing structured storage and transaction-level consistency for verified counting events. Leveraging MariaDB's SQL-based architecture, the system maintains seamless compatibility with cloud servers, web-based dashboards, and IoT middleware layers. Validated data transmitted from the embedded control module are automatically inserted as atomic records, retrieved for analytical processing, and visualized through the web interface to support real-time supervision. The MariaDB-based backend provides a reliable and structured data management infrastructure that complements the dual-verification counting mechanism. By supporting real-time data logging, operator traceability, and synchronized cloud integration, the proposed database architecture enhances operational transparency and efficiency. Moreover, this design establishes a scalable foundation for/enables future expansion toward large-scale smart transportation and intelligent fare management systems.

E. Web-Based Monitoring Interface

Figure 7 presents the web-based monitoring interface developed using C#, ASP.NET, and Microsoft Visual Studio 2015. This interface functions as the visualization and supervision layer of the proposed IoT-enabled automatic token counting system, enabling real-time interaction between operators, cloud data, and embedded hardware. The primary role of the web interface is to retrieve verified counting data from the MariaDB backend and present them in a structured, human-readable format. Operational data transmitted from the embedded control module are stored in the cloud database and dynamically synchronized with the web dashboard, providing up-to-date system status without requiring direct physical access to the device.

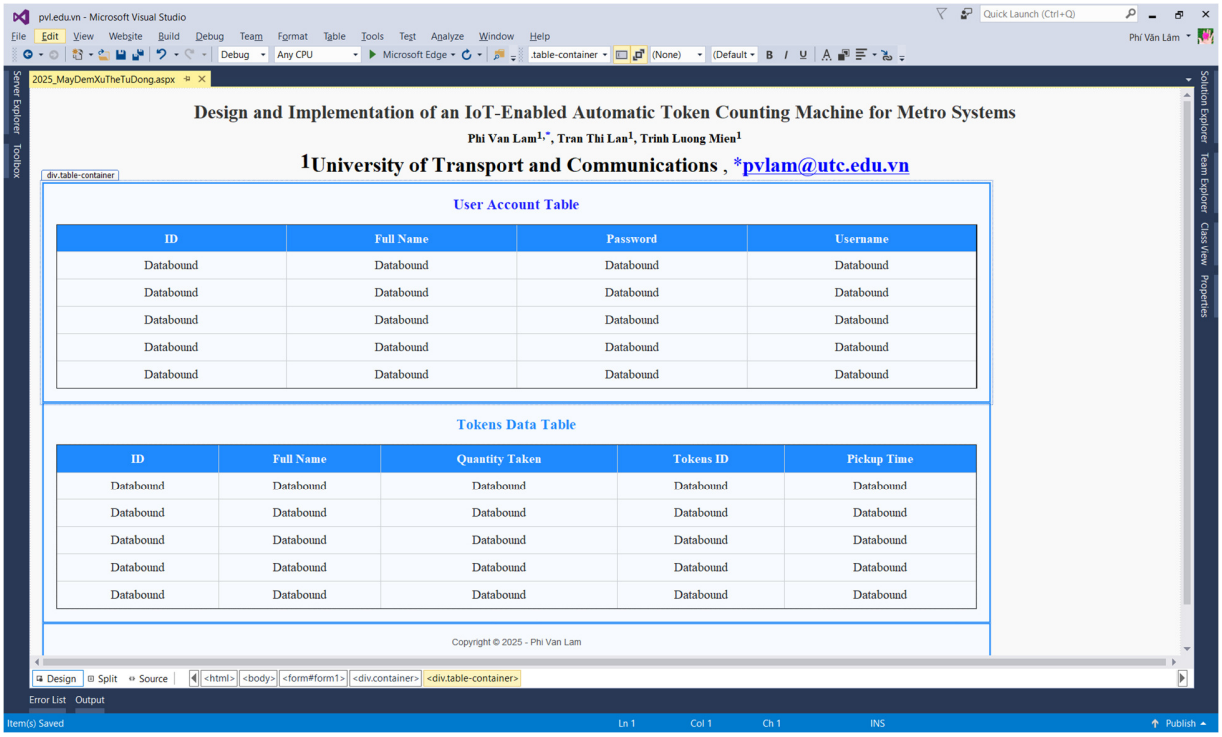

Fig. 7. Web-based monitoring interface.

1) User Management Interface

The first component of the dashboard is the User Account Table, which manages operator authentication and access control. This table displays authorized users responsible for system operation and supervision. The information presented in the table includes the following fields:

- ID: A unique identifier automatically generated by the database.
- Full Name: The registered name of the system operator.
- Username: The login identifier used for system access.
- Password: An encrypted credential used for authentication and security.

The user management interface is implemented using ASP.NET data-binding mechanisms, allowing controlled Create, Read, Update, and Delete (CRUD) operations through structured SQL queries or Entity Framework services. This functionality ensures secure access management and traceability of system usage. The proposed system operates within the metro operator's station control center for backend verification of token quantity and integrity during inter-station handover processes. The deployment environment is physically restricted to authorized personnel. RFID communication occurs at short range within an enclosed mechanical processing unit,

reducing the feasibility of external sniffing or interception. At the network level, communication between the embedded controller and the central server is secured using HTTPS with TLS encryption, ensuring the confidentiality and integrity of transmitted data. Device authentication mechanisms are implemented to prevent unauthorized access and data injection. Operational data is stored in a MariaDB database with role-based access control and restricted user privileges. The database is not directly exposed to external networks; all interactions occur through secured server-side APIs with input validation and authentication checks.

These transport-layer encryption and database-layer protection mechanisms mitigate risks, such as eavesdropping, data tampering, and unauthorized access, thereby enhancing the cybersecurity effectiveness of the proposed system for practical metro deployment.

2) Real-Time Token Monitoring Interface

The Tokens Data Table is the second component of the dashboard. It provides real-time visualization of operational data collected from the automatic token counting device. Each record corresponds to a completed counting batch and includes:

- ID: The transaction index associated with each counting session.
- Full Name: The operator responsible for the session.
- Quantity Taken: The total number of verified tokens processed.
- Token ID: The list of RFID-based unique identifiers corresponding to verified tokens.
- Pickup Time: The timestamp generated when data are committed to the database.

This table is dynamically synchronized with the backend database, allowing newly inserted records to be displayed automatically without manual refresh. The real-time update mechanism enables operators and administrators to monitor system performance, detect anomalies, and review historical data for auditing and operational analysis.

3) Role in the IoT Architecture

Within the overall system architecture, the web-based dashboard operates as a cloud-level supervisory interface, decoupled from low-level hardware control. By separating embedded decision-making from cloud visualization, the system maintains deterministic real-time behavior at the device level while offering scalable, remote monitoring capabilities at the application level. Through this web-based monitoring interface, the proposed system achieves transparent operation, user accountability, and centralized supervision, reinforcing its suitability for deployment in modern metro fare collection environments and other large-scale intelligent transportation systems.

Both data tables are integrated within a unified ASP.NET-based web interface, designed using standard HTML and CSS to ensure a clear, organized, and responsive layout across different display environments. The web application provides real-time interaction with the backend database, allowing operators and administrators to supervise system operation and access historical records without direct access to the embedded hardware.

The ASP.NET framework facilitates efficient communication between the web interface and the MariaDB backend through standardized data access layers, supporting both structured SQL transactions and object-relational mapping. This architecture ensures low-latency data synchronization, reliable transaction handling, and scalability for multi-user access in cloud-based environments.

The developed web interface completes the IoT architecture of the proposed automatic token counting system by providing real-time monitoring, user authentication, and historical data tracking. The seamless integration of the embedded device, cloud database, and web-based supervisory layer establishes an effective and extensible framework suitable for deployment in metro fare collection systems and future large-scale intelligent transportation applications.

III. EXPERIMENTAL IMPLEMENTATION AND RESULTS

Figure 8 presents the experimental implementation of the proposed IoT-enabled automatic token counting system, including the developed hardware prototype and the corresponding user interface during operation. The prototype was developed to experimentally validate the complete system architecture, illustrated in Figure 1, encompassing mechanical token handling, synchronized optical–RFID sensing, embedded control logic, and cloud-based monitoring. The experimental setup validates not only the mechanical feasibility of the device, but also the effectiveness of the proposed dual-verification counting mechanism and its real-time data synchronization capabilities under realistic operating conditions. The prototype integrates all functional subsystems into a single deployable unit suitable for metro station environments.

A. Prototype Hardware Implementation

Figure 8(a) shows the developed experimental prototype of the IoT-enabled automatic token counting device: The main components of the prototype are:

- Token Storage Tray: Positioned at the top of the device, the tray stores a batch of tokens prior to processing. Token transport is driven by a DC motor through a belt–pulley mechanism, which provides controlled and continuous feeding toward the sensing channel while minimizing overlap and jamming.
- Central Control Unit: Located beneath the storage tray, this module integrates the ESP32-WROOM-32 microcontroller and associated power and driver circuits. It executes the dual-verification counting algorithm, regulates motor speed and direction, processes sensor data, and manages wireless communication with the cloud server.
- Sensor Modules: The optical counting sensor and RFID reader are installed sequentially along the token pathway. The optical sensor generates physical trigger events

corresponding to token passage, while the RFID module reads unique token identifiers for identity verification and traceability.

Fig. 8. Experimental prototype of the IoT-enabled automatic token counting device: (a) top view, (b) display screen.

- Input Keypad: A 4×4 matrix keypad is mounted on the front panel, allowing operators to enter authentication credentials and configure batch parameters, including the target number of tokens.
- Display Unit: A TFT LCD screen located adjacent to the keypad provides real-time feedback on system status, counting progress, batch results, and warning notifications during operation.

The compact integration of mechanical, electronic, and human–machine interface components enables stable operation and direct observation of system behavior during experimental evaluation.

Figure 8(b) presents the real-time operational interface displayed on the embedded screen during experimental testing. The interface provides live visualization of key system parameters, including operator authentication status, predefined batch size, verified token count, and the dynamically updated list of RFID-based unique identifiers. A connectivity indicator confirms active wireless communication with the remote database, ensuring that verified data are synchronized with the cloud in real time.

TABLE II. PICKUP SESSION CONSISTENCY BETWEEN RECORDED QUANTITY AND DATABASE-LOGGED TOKEN IDS

ID	Quantity taken	Token count	Status
18	8	8	✓ Match
19	9	9	✓ Match
20	15	15	✓ Match
21	6	6	✓ Match
22	6	6	✓ Match
23	5	5	✓ Match
24	50	50	✓ Match
25	12	12	✓ Match
26	5	5	✓ Match
27	20	20	✓ Match
28	50	50	✓ Match
29	60	60	✓ Match
30	70	70	✓ Match
31	80	80	✓ Match
32	25	25	✓ Match
33	35	35	✓ Match
34	45	45	✓ Match
35	55	55	✓ Match
36	68	68	✓ Match
37	86	86	✓ Match
38	30	30	✓ Match
39	32	32	✓ Match
40	40	40	✓ Match
41	56	56	✓ Match
42	50	50	✓ Match
43	33	33	✓ Match

During operation, the embedded control logic continuously compares the verified token count with the preset batch value. Any abnormal conditions, such as token absence, mechanical obstruction, or unreadable RFID identification, trigger an automatic alert and initiate a corrective motor reverse sequence

to clear potential jams. This closed-loop behavior validates the effectiveness of the proposed control strategy under non-ideal operating conditions.

For experimental evaluation, a set of customized RFID-enabled tokens was fabricated and encoded with unique identifiers compliant with the ISO/IEC 14443 standard (13.56 MHz passive tags). These tokens were used to assess counting accuracy, identification reliability, and resistance to read collisions during batch processing. Across all experimental trials, the system consistently demonstrated correct token feeding, synchronized optical–RFID verification, and reliable data transmission to the online server.

Figure 9 shows the corresponding web-based monitoring interface, which enables authorized users to remotely supervise counting sessions through a secure HTTPS browser connection. Access to the dashboard requires authenticated login credentials, and all data transactions between the server and client are protected using TLS encryption. The dashboard dynamically retrieves and displays updated records from the MariaDB database via secured server-side APIs, ensuring controlled access without direct public exposure of the database. The experimentally recorded Quantity Taken values exhibit a strict one-to-one correspondence with the number of stored RFID identifiers, confirming that every physically counted token is uniquely identified and logged without duplication or data loss.

Overall, the experimental results confirm the effectiveness of the proposed IoT-enabled automatic token counting system. The combination of synchronized optical triggering, RFID-based identity verification, secure HTTPS-based communication, and cloud database supervision achieves accurate counting, full traceability, protected data transmission, and reliable real-time monitoring. These results validate the feasibility of deploying the proposed system in practical metro operational environments and demonstrate its scalability for intelligent transportation applications.

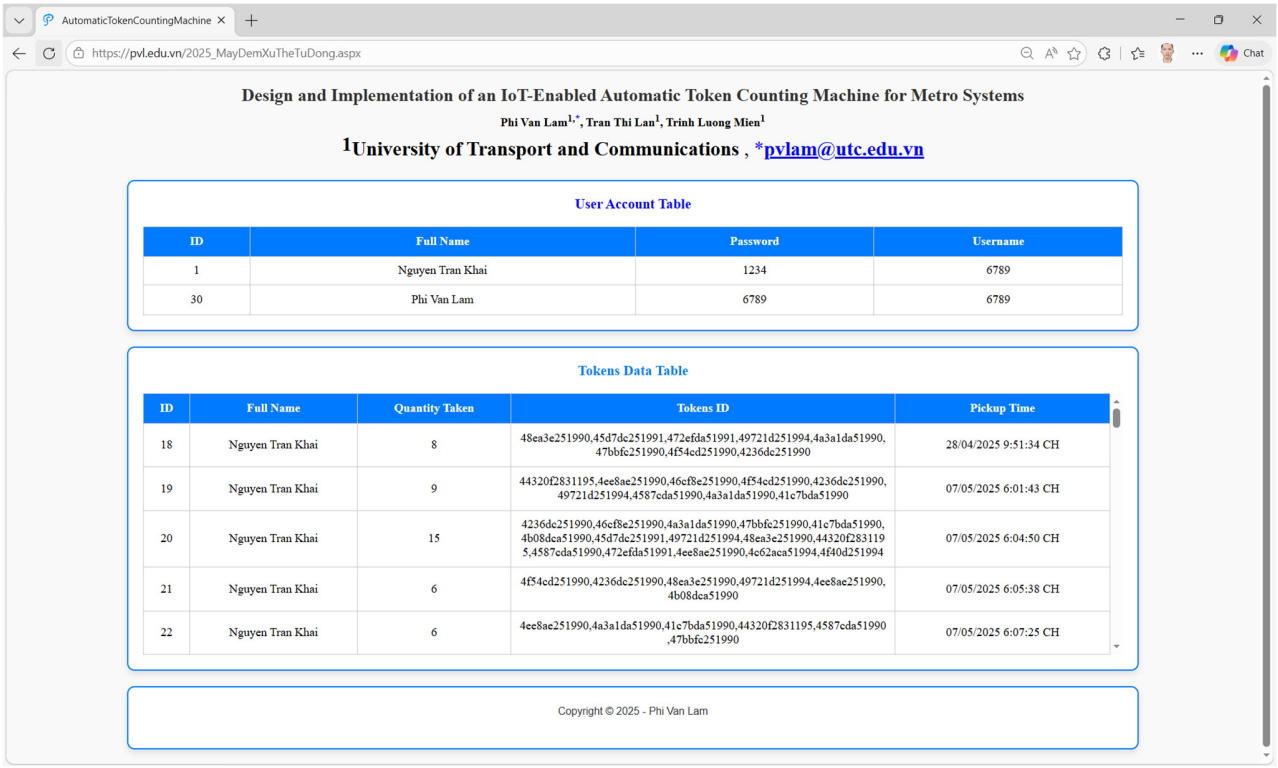

Fig. 9. Online monitoring interface.

To provide clearer quantitative insights into the evaluation scope, Table II summarizes the testing range, number of sessions, and token quantity intervals used during validation. Pickup sessions from ID 18 to ID 43 are covered. For each session, the recorded quantity exactly matches the number of detected token IDs, demonstrating 100% counting consistency across the tested range (5–86 tokens per session). These results confirm the effectiveness and reliability of the proposed synchronized optical–RFID verification mechanism under varying pickup volumes.

The real-time operation of the deployed prototype is illustrated in Figure 10. The embedded interface displays detected token IDs, counted quantity, and system status during pickup sessions, confirming stable field operation and reliable synchronization with the online monitoring platform exhibited in Figure 9.

The current study presents a complete design-to-implementation workflow integrating mechanical construction, embedded electronics, and IoT-based supervision into a unified automatic token counting platform. The proposed dual-

verification architecture, synchronizing optical triggering with RFID-based identity confirmation, ensures accurate counting, full token-level traceability, and reliable real-time database synchronization. Experimental validation demonstrates stable operation under continuous load and preserves data integrity between the embedded device and the cloud-based supervisory interface.

ingMachine ×

ovl.edu.vn/2025_MayDemXuTheTuDong.aspx

33	Nguyen Tran Khai	35	473b0d251990,46aaee251990,48ea3e251990,447e5c251991,4363bc251991,4cf33d251990,4bf58ca51990,49441d251994,431e5da51990,45d7dc251991,4b62ed251994,48af9da51990,46423da51990,44320f2831195,4ee8ae251990,4236dc251990,4362fd251995,4d895e251990,4e24fda51990,441fcca51990,484ebc251990,41c7bda51990,4396eda51991,4b366c251990,486b6f2831190,46bf6da51990,42a15da51995,4569d251995,4a3a1da51990,4f772d251990,47971d251991,47bbfc251990,4b936e251994,4ef15e251994,4288cca51990	26/02/2026 9:05:14 SA

Fig. 10. Real-time operation of the deployed token counting prototype.

IV. CONCLUSION

This study proposed and experimentally validated an Internet of Things (IoT)-enabled automatic token counting system based on a synchronized optical–Radio Frequency Identification (RFID) dual-verification architecture. By deterministically synchronizing physical token detection with RFID-based Unique Token Identification (UID) acquisition, the system ensures one-to-one correspondence between mechanical movement and digital identification, effectively mitigating duplicate reads and overlap-related miscounting.

Experimental trials using 250 RFID-enabled tokens across repeated batch runs demonstrated stable serialized feeding at 240 rpm, consistent counting accuracy, and reliable real-time database synchronization, with no duplicated or missing records observed. These results confirm the robustness and practical feasibility of the proposed synchronization mechanism under continuous operation. Compared with optical-only or RFID-only approaches, the proposed architecture enhances counting reliability and token-level traceability while maintaining practical implementation costs using widely available embedded and RFID components. Secure data handling is ensured through controlled database access and protected HTTPS-based communication mechanisms suitable for operational deployment.

Future work will focus on large-scale field validation under full metro operational conditions, improved mechanical robustness, strengthened secure communication mechanisms, integration with existing Automated Fare Collection (AFC) infrastructure, and the application of advanced data analytics and predictive maintenance models to enhance long-term operational efficiency.

ACKNOWLEDGMENT

This research was supported by the University of Transport and Communications under project T2025-DT-003.

DATA AVAILABILITY STATEMENT

The online monitoring interface developed for the automatic token counting system is publicly available at https://www.pvl.edu.vn/2025_MayDemXuTheTuDong.aspx.

REFERENCES

[1] M. Bieler, A. Skretting, P. Budinger, and T.-M. Gronli, "Survey of Automated Fare Collection Solutions in Public Transportation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 14248–14266, Sep. 2022, https://doi.org/10.1109/TITS.2022.3161606.

[2] M. Chen and S. Chen, "An Efficient Anonymous Authentication Protocol for RFID Systems Using Dynamic Tokens," in *IEEE 35th International Conference on Distributed Computing Systems*, Columbus, OH, USA, Jun. 2015, pp. 756–757, https://doi.org/10.1109/ICDCS.2015.94.

[3] T. C. Thanuja and S. R. Vakare, "Automated Fare Collection System Using ARM," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 6, no. 6, pp. 4535–4542, Jun. 2017.

[4] S. Karthikeyan and M. Nesterenko, "RFID Security Without Extensive Cryptography," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, Alexandria, VA, USA, Nov. 2005, pp. 63–67, https://doi.org/10.1145/1102219.1102229.

[5] M. S. Malkar, M. Mundada, A. Patil, G. Phatak, S. Vaidya, and A. Salunke, "Automated Bus e-Ticketing Service," *International Journal of Advanced Research in Science, Communication and Technology*, vol. 4, no. 2, pp. 281–284, Jan. 2024, https://doi.org/10.48175/IJARSCT-15245.

[6] A. A. Ajmi and M. Jose, "IoT Based Counting System," *Journal of Xidian University*, vol. 15, no. 8, pp. 375–381, 2021.

[7] S. Sudhakaran, R. Maheswari, and V. Kanchana Devi, "An Improvised Analysis of Smart Data for IoT-Based Railway System Using RFID," *Automatika*, vol. 65, no. 1, pp. 361–372, Jan. 2024, https://doi.org/10.1080/00051144.2023.2295141.

[8] N. Ma, A. Waegel, M. Hakkarainen, W. W. Braham, L. Glass, and D. Aviv, "Blockchain + IoT Sensor Network to Measure, Evaluate and Incentivize Personal Environmental Accounting and Efficient Energy Use in Indoor Spaces," *Applied Energy*, vol. 332, Feb. 2023, Art. no. 120443, https://doi.org/10.1016/j.apenergy.2022.120443.

[9] K. S. Gill, A. Sharma, V. Anand, and S. Gupta, "Automated Fare Collection System for Public Transport Using Intelligent IoT Based System," in *International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering*, Chennai, India, Jan. 2023, pp. 1–7, https://doi.org/10.1109/ICECONF57129.2023.10083627.

[10] S. Sandra, C. Subarna, L. Parameshwari, B. Pallapu, and U. Chaitanya, "IoT-Based Automatic Ticketing System for Public Transportation Using RFID, GPS and Android Integration," *Journal of Emerging Technologies and Innovative Research*, vol. 12, no. 3, pp. 757–762, Mar. 2025.

[11] A. Radovan, L. Mršić, G. Đambić, and B. Mihaljević, "A Review of Passenger Counting in Public Transport Concepts with Solution Proposal Based on Image Processing and Machine Learning," *Eng*, vol. 5, no. 4, pp. 3284–3315, Dec. 2024, https://doi.org/10.3390/eng5040172.

[12] C. Furtado and J. Rebello, "RFID Based Metro Train Ticketing System," *International Journal of Science Technology & Engineering*, vol. 3, no. 9, pp. 619–622, Mar. 2017.

[13] M. ElZeweidy and B. Sayed, "Smart Ticketing System in Metro Rail Using RFID Tag," *Journal of the ACS Advances in Computer Science*, vol. 13, no. 1, pp. 11–19, Jun. 2022, https://doi.org/10.21608/asc.2023.171571.1010.

[14] Y. Zhan, F. Yuan, R. Shi, G. Shi, and C. Dong, "PriTKT: A Blockchain-Enhanced Privacy-Preserving Electronic Ticket System for IoT Devices," *Sensors*, vol. 24, no. 2, Jan. 2024, Art. no. 496, https://doi.org/10.3390/s24020496.

[15] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, and U. Biswas, "Blockchain for Intelligent Transportation Systems: Applications, Challenges, and Opportunities," *IEEE Internet of Things Journal*, vol. 10, no. 21, pp. 18961–18970, Nov. 2023, https://doi.org/10.1109/JIOT.2023.3277923.

[16] N. K. Majji, V. N. Madhavareddy, G. Immadi, N. Ambati, and S. M. Aovuthu, "Analysis of a Compact Electrically Small Antenna with SRR for RFID Applications," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12457–12463, Feb. 2024, https://doi.org/10.48084/etasr.6418.

[17] K. Mekki, O. Necibi, C. Boussetta, and A. Gharsallah, "Miniaturization of Circularly Polarized Patch Antenna for RFID Reader Applications," *Engineering, Technology & Applied Science Research*, vol. 10, no. 3, pp. 5655–5659, Jun. 2020, https://doi.org/10.48084/etasr.3445.

[18] M. N. Prabhakaran and A. Sampath, "Prototype Designing of Coin Based Sensing Water Filling System," *International Journal of Engineering Research & Technology*, vol. 5, no. 22, pp. 1–4, 2017.

AUTHORS PROFILE

Phi Van Lam received his B.E. and M.E. degrees in electrical and electronic engineering from the University of Transport and Communications, Hanoi, Vietnam, in 2011 and 2014, respectively. He received his Ph.D. degree in physics, electrical, and computer engineering from Yokohama National University, Yokohama, Japan, in 2019. His current research interests include robotics, AI, control theory, motion control, Internet of Things (IoT), and Intelligent Transport Systems (ITS).

Tran Thi Lan was born in Haiphong, Vietnam, in 1988. She received her B.S. and M.S. degrees in telecommunication engineering from the University of Transport and Communications, Hanoi, Vietnam, in 2011 and 2013, respectively. She received her Ph.D. degree in computer, physics, and electrical engineering from Yokohama National University, Yokohama, Japan. She is now a lecturer at the University of Transport and Communications. Her current research interest is the design of antennas for wireless communication systems.

Trinh Luong Mien received his PhD degree at the Russian University of Transport (RUT MIIT). He is Associate Prof. Dr., Head of Lab, Head of Department Cybernetics, Vice Dean of Faculty Electrical-Electronic Engineering, University Transport and Communications. His area of research includes the development of intelligent control algorithms (Fuzzy, AI, ML) for the technological and manufacturing processes in industry and transportation (IIoT, Scada/DCS). He has interest and expertise in a variety of research topics related to control and automation of machines and production lines in industry and transportation, especially intelligent control for electric vehicles, electric trains, Robotics, UAV networks, IIoT, and Scada/DCS systems.