Journal of Computation Physics and Earth Science
ISSN: 2776-2521 (online)
Volume 5, Number 2, February 2026, Page 129 - 136
https://journal.physan.org/index.php/jocpes/index

Design and Implementation of a Web-Based RFID-Enabled Library Visitor Attendance and Management System: A Case Study at STMKG

Ahmad Meijlan Yasir[1], Tonny Wahyu Aji[2],
[1,2]Undergraduate Program in Applied of Instrumentation Meteorology, Climatology Geophysics (STMKG)

Article Info

Article history:

Received December 31, 2025
Revised February 28, 2026
Accepted February 28, 2026

Keywords:

Library Management System
RFID
Information System
Digitalization
STMKG

ABSTRACT

This study presents the design and implementation of a web-based, RFID-enabled library visitor attendance and management system as a single-site case study at STMKG. Academic libraries require structured visit data to support service evaluation and institutional reporting, yet manual logbooks often produce inconsistent records and limit timely analysis. To address this issue, the proposed system digitalizes attendance capture through three integrated workflows within one platform: RFID-based identification for cadets, controlled selection for employees, and a structured manual form for public visitors. The system also provides administrative capabilities for monitoring and reporting, including visit statistics dashboards, time-filtered logs with search, and spreadsheet export for routine reporting needs. The implementation adopts a cloud-backed architecture using a modern web application frontend and a managed backend with database persistence and authentication services. Baseline security controls were incorporated to protect administrative functions and reduce automated abuse at public-facing entry points, including access verification, bot protection, and database-level access boundaries. Functional verification through end-to-end scenario testing confirms that the core attendance workflows, reporting features, and security mechanisms operate as intended within the defined scope. The resulting artifact is deployable in STMKG and can be adapted for similar higher-education libraries seeking practical visitor attendance digitalization.

Corresponden Author:

Ahmad Meijlan Yasir,
Undergraduate Program in Applied of Instrumentation Meteorology, Climatology Geophysics (STMKG)
Tangerang, Indonesia
Email: yasirahmad220504@gmail.com

1. INTRODUCTION

Academic libraries routinely collect operational metrics to evaluate services and support institutional benchmarking. One of the most widely used indicators is visitor traffic, often measured as annual gate counts, which reflects the level of physical space utilization within library facilities. Large-scale benchmarking initiatives across higher education institutions use these metrics to compare operational performance and inform strategic planning for library services [1], [2]. Because visitor attendance data directly represent how frequently library spaces are used, these records become an essential evidence base for managerial decision making, including adjustments to service hours, staffing allocation, and infrastructure investment [3], [4]. Consequently, the availability of accurate and structured attendance data is a critical requirement for modern library management.

Despite the importance of this data, many institutions still rely on manual recording procedures or fragmented visitor management practices [1], [2]. Similar conditions were observed at the library of Sekolah Tinggi Meteorologi Klimatologi dan Geofisika (STMKG), where visitor attendance was historically recorded using physical logbooks and a conventional barcode-based system. Such approaches limit data accuracy, create inconsistencies in record formats, and complicate the generation of timely reports required for administrative evaluation [4], [5]. The modernization of operational systems within STMKG is part of a broader institutional effort to improve digital services and optimize user interaction across information platforms [6]. Within this context, the library environment presents a specific operational challenge because the attendance system must simultaneously accommodate three categories of visitors, namely cadets, internal staff, and public visitors. Without a systematic identification mechanism, the process of verifying visitor identity becomes a significant operational bottleneck that reduces service efficiency and reliability [1], [5].

Radio Frequency Identification (RFID) technology has been widely adopted in library environments to support fast and contactless identification of users, thereby reducing congestion at service entry points [7], [8]. However, standalone RFID deployments may introduce new concerns related to data integrity and security. Empirical studies have demonstrated that certain low-frequency RFID cards without encryption mechanisms are vulnerable to cloning attacks using widely available tools such as Proxmark3, highlighting the importance of complementary security mechanisms at the system level [9], [10]. In addition to hardware-related vulnerabilities, web-based attendance endpoints are also exposed to automated abuse by bots that repeatedly submit requests to exploit open interfaces. While many studies in RFID-based library automation focus on communication protocols between the card and the reader, comparatively less attention has been given to end-to-end security architectures that extend protection to the application layer and backend infrastructure.

These challenges indicate the need for an integrated system architecture that combines RFID-based identification with a structured web-based visitor management workflow while incorporating practical security controls. A unified system can enforce consistent data validation, store visit records in a centralized database, and provide administrative monitoring capabilities for reporting and analysis. At the same time, protective mechanisms such as bot-abuse mitigation and database-level authorization are necessary to preserve data integrity and system availability when attendance endpoints are publicly accessible.

Therefore, this study aims to design and implement a web-based RFID-enabled library visitor attendance and management system as a single-site case study at STMKG. The proposed system integrates RFID-based identification with a multi-category visitor workflow and centralized reporting features within a cloud-backed architecture. The contributions of this work are threefold. First, the study presents an end-to-end system design that supports RFID-based attendance capture alongside structured workflows for staff and public visitors. Second, it documents an implementation approach that combines a modern web application architecture with database-level authorization and bot-abuse mitigation mechanisms. Third, the study reports functional verification of key system capabilities, including attendance capture workflows, administrative reporting functions, and baseline security controls. The scope of the study is limited to the STMKG library environment, and user acceptance evaluation is outside the scope of this work

2. RESEARCH METHOD

This study follows a design-and-implementation approach, framed as a single-site case study at STMKG. The research output is a deployable software artifact that operationalizes library visitor attendance and management through a web interface and RFID-based identification for cadets, complemented by structured workflows for employees and public visitors. The method is organized into four stages: requirements elicitation, system design, implementation, and functional verification.

2.1. Requirements Elicitation

Requirements were derived from the operational workflow of STMKG library attendance, emphasizing a minimal but complete set of functions to record visits consistently and to support administrative reporting. The resulting functional and security requirements are summarized in Table 1, which is later used to maintain traceability to implemented modules (Section 3.1) and verification scenarios (Section 3.5).

Table 1. Summary of functional and security requirements

ID	Requirement	Operational intent
FR1	Support cadet attendance via RFID by resolving rfid_data to cadets and recording a visit in visitors	Reduce manual entry and standardize cadet identification
FR2	Support employee attendance via controlled selection from employees and record a visit in visitors	Ensure consistent employee records without free-text ambiguity
FR3	Support public visitor attendance via structured form input and record a visit in visitors	Enable standardized capture for external visitors
FR4	Provide RFID registration flow when an RFID is unregistered, with NPT format validation and RFID uniqueness	Preserve data integrity and prevent duplicate identifiers
FR5	Provide admin dashboard for visit statistics and a reporting module with filtering, search, and Excel export	Produce operational summaries and institutional reports efficiently
SR1	Enforce database access boundaries using row-level security: anon limited to lookup and visit insert, admin to management CRUD	Prevent unauthorized reads or edits while keeping attendance usable

ID	Requirement	Operational intent
SR2	Protect landing access with credential verification via landing-verify and bot protection via Turnstile	Reduce unauthorized usage and automated abuse on the attendance endpoint
SR3	Protect admin login with Turnstile validation and lockout after repeated failures	Reduce bot attempts and brute force against admin access

Table 1 reflects the need to accommodate three visitor categories within one platform, while ensuring that reporting and baseline security controls are available for operational deployment at STMKG.

2.2. System Design

The system was designed as a web application connected to a cloud backend, with RFID serving as an identifier input for cadet attendance. The frontend was implemented as a single-page application, while the backend relied on Supabase services, including PostgreSQL for persistence, authentication for administrator access, and Edge Functions for security-critical operations [11]. The core database schema was defined around five main tables: *admins*, *cadets*, *employees*, *rfid_data*, and *visitors*. The *rfid_data* table maps an RFID number to a cadet identifier (NPT), and the visitors table stores a unified visit log across all visitor types, enabling consistent reporting regardless of capture method.

Access control was enforced at the database layer using row-level security policies. In the deployed configuration, unauthenticated clients were restricted to read-only lookups for attendance resolution and were permitted only to insert visit records, while authenticated administrators were granted the CRUD privileges required for management and reporting functions. Security-sensitive flows were designed to minimize client exposure of privileged logic. Specifically, landing access verification was performed through an Edge Function that returns only a boolean validation result without creating a Supabase session on the client, and administrative login was protected with robot verification and lockout controls.

2.3. System Implementation

The artifact was implemented using a modern web stack to support maintainability and deployment simplicity. The frontend was built with React and TypeScript, while integration with backend services was handled through the Supabase JavaScript client and Edge Functions. Three visitor attendance workflows were implemented on the landing interface: (1) RFID-based cadet attendance using a lookup chain from rfid_data to cadets, followed by insertion into visitors; (2) employee attendance via dropdown selection sourced from employees; and (3) public visitor attendance via a structured form. If an RFID number is not registered, the system redirects to a registration page where the RFID number is prefilled and an NPT format constraint is enforced at the database layer to preserve data consistency.

Administrative functions were implemented under a protected route group, including login, dashboard statistics, master data management for cadets and employees, visit reporting with time filters and search, and spreadsheet export. The system includes bot protection through Cloudflare Turnstile on both landing verification and admin login, with server-side validation performed by the verify-turnstile Edge Function. Deployment was designed for a cloud-native setup where the web frontend can be hosted on Vercel and backend services operate within Supabase.

2.4. Functional Verification

Verification was limited to functional testing of critical end-to-end scenarios as a checklist, without user acceptance evaluation. The scenarios in Table II cover landing access verification, the three attendance paths, the unregistered RFID registration path, administrative reporting and export, and core security controls aligned with Table 1.

Table 2. Functional testing scenarios and outcomes

ID	Test scenario	Expected outcome
FT1	Landing verification with credentials and Turnstile	Access to attendance workflows is granted only after valid verification
FT2	RFID attendance with registered RFID and existing cadet	Visit record is inserted into visitors with type cadets, then redirected to welcome page
FT3	RFID attendance with unregistered RFID	User is redirected to /register with RFID number prefilled
FT4	Employee attendance submission	Visit record is inserted into visitors with type employee, then redirected to welcome page
FT5	Public visitor attendance submission	Visit record is inserted into visitors with type public, then redirected to welcome page
FT6	Admin login with username resolution, Turnstile, and lockout policy	Successful login requires Turnstile; repeated failures trigger lockout behavior
FT7	Dashboard and report retrieval	Admin can view statistics and query visit logs using filters and search

ID	Test scenario	Expected outcome
FT8	Export visit report to Excel	System generates an Excel file containing the visit log with required columns

Table 2 is referenced in Section 3.5 to report verification coverage and to demonstrate alignment with the requirements in Table 1.

3. RESULT AND DISCUSSION

3.1. Results of Requirements Analysis

The requirements analysis identified a minimal set of capabilities needed to operationalize visitor attendance at the STMKG library while producing structured outputs for administration. Functionally, the system must support three visitor categories within a single, consistent logging model: cadets recorded through RFID-based identification, employees recorded through controlled selection to avoid ambiguous free-text entries, and public visitors recorded through a structured manual form. To ensure operational continuity, an RFID enrollment path is also required when an RFID number is not yet registered, including identifier validation to preserve data consistency.

From the administrative perspective, the requirements emphasize monitoring and reporting rather than complex workflows. The system must provide a dashboard that summarizes visit trends, and a reporting module that supports time-based filtering, search, and export to spreadsheet format to enable routine institutional reporting. These features ensure that visit records are not only captured but also transformed into usable summaries without manual recapitulation.

Security requirements were defined as baseline controls appropriate for a publicly reachable attendance endpoint. The system must restrict administrative functions to authenticated users and include bot-abuse mitigation at public-facing verification and login steps. In addition, database-layer access boundaries are required to ensure that unauthenticated usage is limited to attendance-related lookups and visit record insertion, while administrative data management remains restricted. Table 3 summarizes the finalized functional and security requirements that guide the implementation discussed in subsequent sections.

Table 3. Finalized Functional and Security Requirements

ID	Requirement	Rationale
FR1	Record cadet attendance via RFID by resolving RFID to a cadet identifier and logging the visit	Automate identification and reduce manual entry errors
FR2	Record employee attendance via controlled selection and log the visit	Ensure consistent internal visitor records
FR3	Record public visitor attendance via structured manual form and log the visit	Provide standardized capture for external visitors
FR4	Provide RFID registration for unregistered RFID numbers with identifier validation and uniqueness checks	Maintain data integrity and prevent duplicate identifiers
FR5	Provide an admin dashboard for visit statistics and a reporting module with time filtering, search, and spreadsheet export	Enable routine monitoring and institutional reporting
SR1	Enforce database-layer access boundaries so unauthenticated clients are limited to necessary lookups and visit insertion	Prevent unauthorized access while keeping attendance usable
SR2	Require access verification at the attendance entry point and apply bot protection	Reduce unauthorized use and automated abuse
SR3	Protect admin login with bot protection and lockout after repeated failures	Reduce brute-force attempts against admin access

These requirements establish a complete but bounded scope for an operational attendance system, where data capture, reporting, and baseline security controls are treated as first-class design objectives.

3.2. System Architecture and Design

The implemented system adopts a web-and-cloud architecture where a browser-based single-page application performs visitor-facing attendance capture and administrative management, while Supabase provides the backend services for persistence, authentication, and server-side security logic. The architecture also integrates Cloudflare Turnstile for bot protection, validated server-side using an Edge Function.

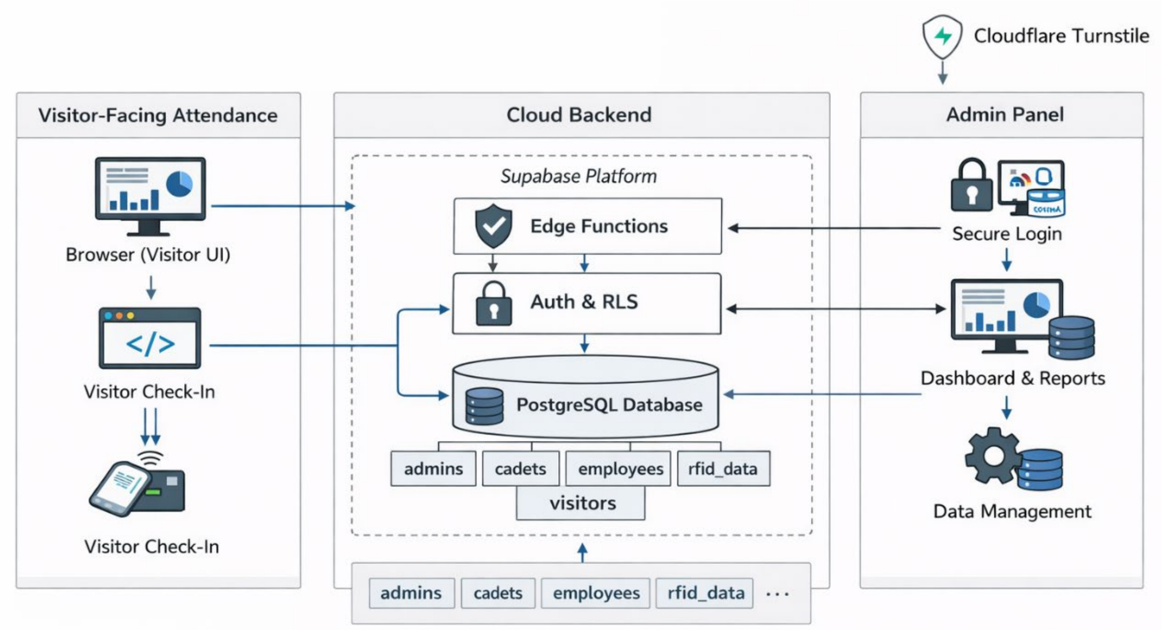
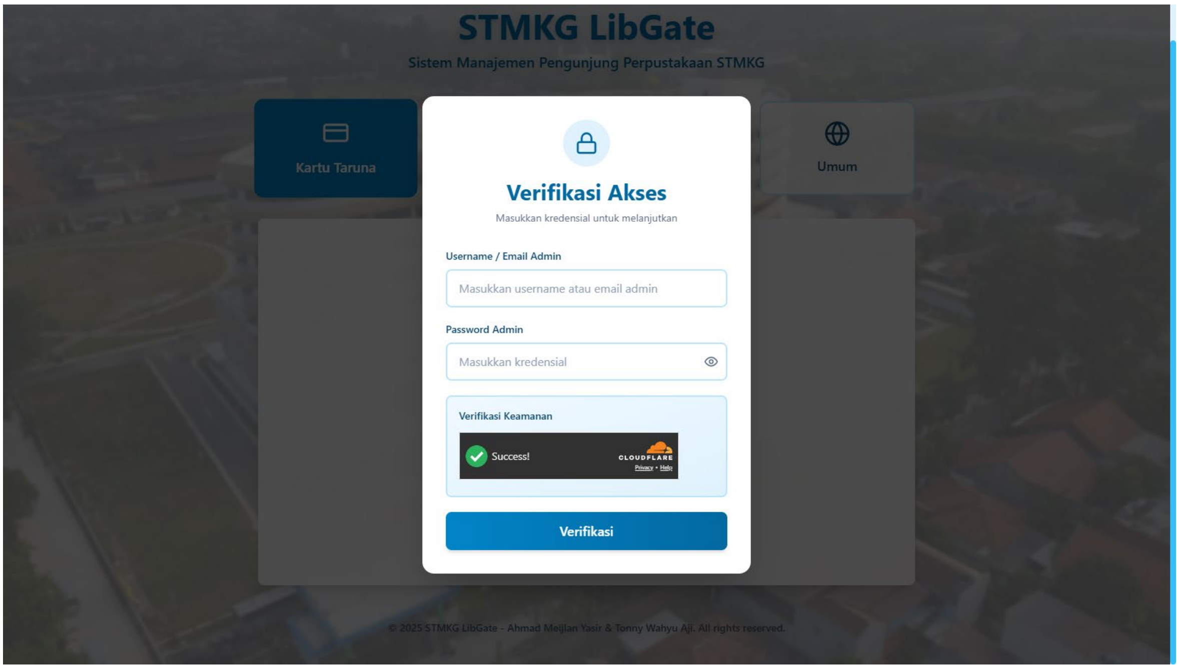


Fig. 1. High-level system architecture and component interactions

At the data layer, the design uses a unified visit log to support consistent reporting across all visitor types. The schema is organized around five core tables: admins, cadets, employees, rfid_data, and visitors, where rfid_data maps RFID numbers to cadet identifiers (NPT) and visitors stores the final visit record used for analytics and reporting. This design reduces fragmentation and allows the reporting module to operate over a single visit dataset regardless of the capture method.

3.3. Results of Requirements Analysis

The system was implemented as two main surfaces: a visitor-facing landing interface and an admin panel. The landing interface is the operational entry point and supports three attendance modes after a mandatory access verification step. The admin panel provides secured access to dashboards and data management modules, including master data maintenance for cadets and employees and visit reporting with export.


STMKG LibGate

Sistem Manajemen Pengunjung Perpustakaan STMKG

Verifikasi Akses

Masukkan kredensial untuk melanjutkan

Username / Email Admin

Masukkan username atau email admin

Password Admin

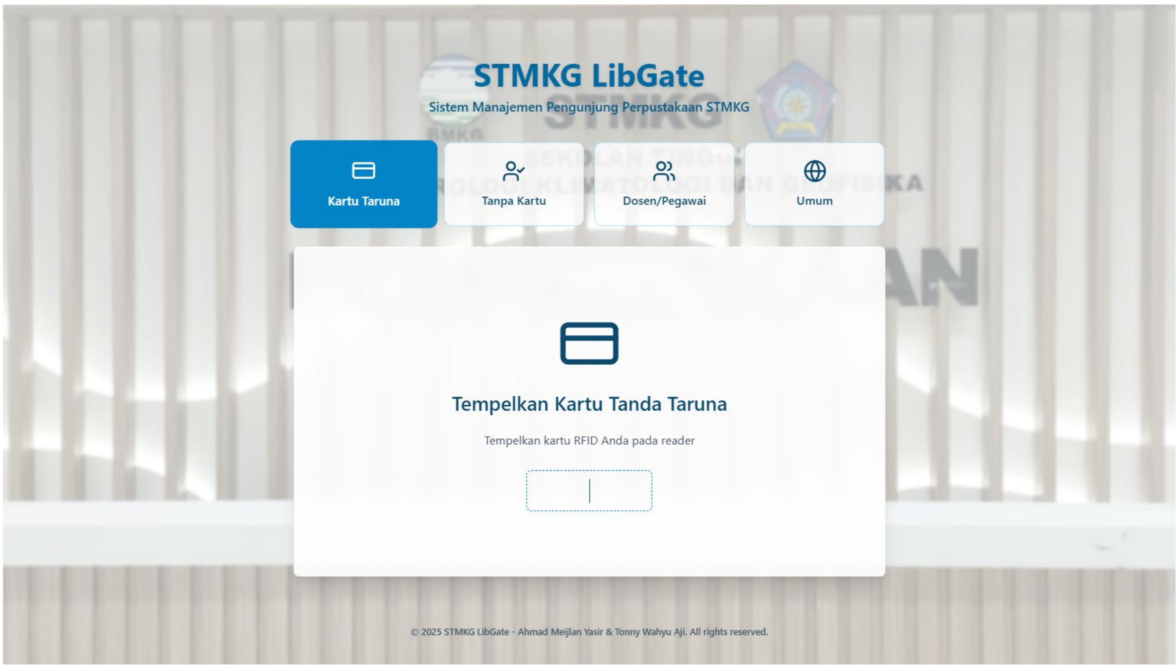
Masukkan kredensial

Verifikasi Keamanan

✓ Success! CLOUDFLARE Privacy • Help

© 2025 STMKG LibGate - Ahmad Meijlan Yasir & Tonny Wahyu Aji. All rights reserved.

Fig. 2. Access verification form

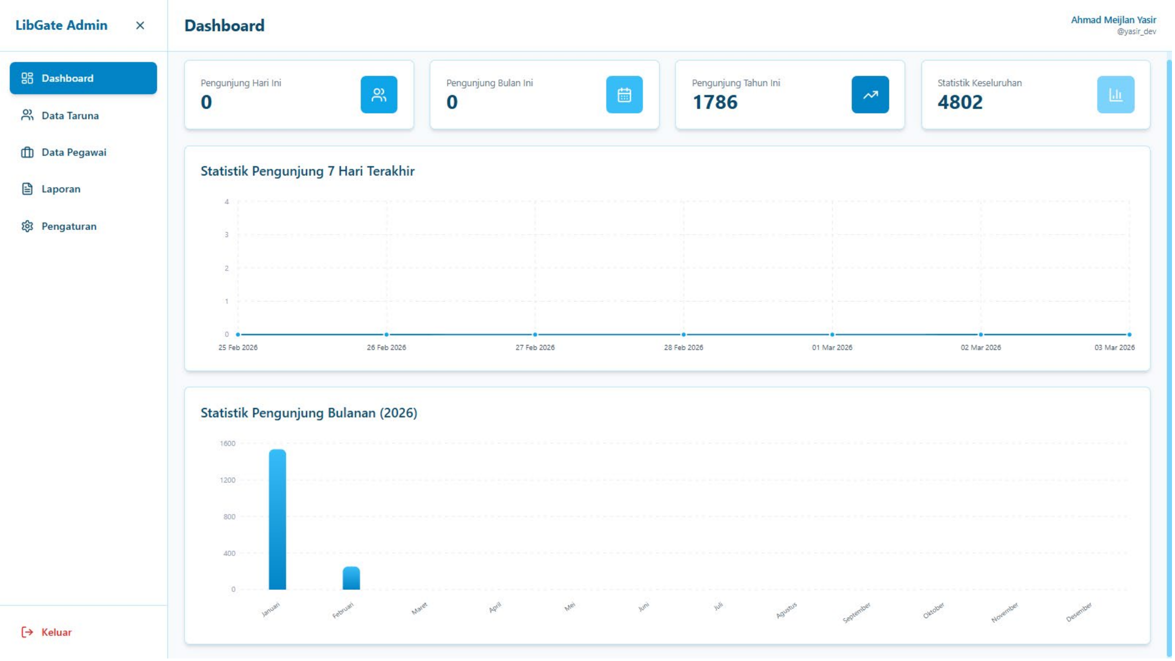


Tempelkan Kartu Tanda Taruna

Tempelkan kartu RFID Anda pada reader

© 2025 STMKG LibGate - Ahmad Meijlan Yasir & Tonny Wahyu Aji. All rights reserved.

Fig. 3. Main page for visitor attendance



Pengunjung Hari Ini: 0
Pengunjung Bulan Ini: 0
Pengunjung Tahun Ini: 1786
Statistik Keseluruhan: 4802

Fig. 3. Administrator panel

For reporting, the admin module includes time-window filtering, search, pagination, and Excel export with relevant columns such as timestamp, visitor name, visitor type, and cadet-derived fields when available. These features operationalize the reporting requirement without requiring manual recapitulation from paper logs.

3.4. RFID Integration

RFID integration is implemented as an identifier-driven workflow for cadet attendance. On RFID input, the system queries rfid_data to resolve the RFID number into an NPT, then queries cadets to obtain cadet details, and finally inserts the visit into visitors with type cadets. When an RFID number is not registered or the NPT cannot be resolved to an existing cadet record, the system redirects to /register with the RFID number prefilled to support controlled enrollment.

Data integrity for RFID enrollment is supported by database constraints, including NPT format validation and uniqueness constraints on both NPT and RFID number. This design reduces common failure modes of manual logging, such as inconsistent identifiers and duplicate entries, while preserving a manual path for non-cadet visitor types.

3.5. Functional Testing Results

Functional verification was conducted as scenario-based end-to-end checks aligned with Table I requirements. Each scenario validated both the user-visible behavior and the expected database state changes. The outcomes are summarized in Table 4.

Table 4. Functional Testing Outcomes

Scenario ID	Scenario (summary)	Result
FT1	Landing verification with credentials and Turnstile	Pass
FT2	RFID attendance with registered RFID and existing cadet	Pass
FT3	RFID attendance with unregistered RFID redirects to /register	Pass
FT4	Employee attendance submission via dropdown	Pass
FT5	Public visitor attendance submission via form	Pass
FT6	Admin login with Turnstile and lockout policy	Pass
FT7	Dashboard and report retrieval under authenticated admin	Pass
FT8	Export report to Excel	Pass

The results indicate that the minimal operational feature set in Table 1 is supported end-to-end, including the attendance capture paths, reporting workflow, and baseline protections required for deployment. No user acceptance evaluation is reported in this study, and the verification is restricted to functional correctness under the defined scenarios.

3.6. Security Mechanisms

Security controls are implemented at both the application and database layers. First, administrative identity is handled exclusively through Supabase Auth, while the system supports username-based login by resolving the username to an email via an Edge Function (resolve-admin-email) that uses service-role privileges. This avoids exposing the admins table to unauthenticated clients, consistent with the RLS configuration.

Second, the visitor-facing attendance endpoint is protected by a landing verification gate. The landing-verified Edge Function performs credential verification and returns only a boolean validation response, without creating a Supabase session on the client, and a per-browser trusted state is stored locally to reduce repeated prompts on the same device. Bot protection is applied to both landing verification and admin login using Cloudflare Turnstile, with server-side token validation performed by the verify-turnstile Edge Function. Finally, rate limiting and lockout behavior are enforced after repeated failures to reduce brute-force attempts against the verification and login flows.

At the database layer, row-level security policies enforce clear boundaries between unauthenticated attendance usage and authenticated administrative management. Unauthenticated clients are limited to lookup access for resolving attendance inputs and are permitted only to insert visit records, while authenticated administrators receive CRUD permissions consistent with management and reporting functions. This layered design supports the operational requirement of a publicly usable attendance interface while maintaining controlled access to administrative capabilities and sensitive data.

4. CONCLUSION

This paper presented the design and implementation of a web-based, RFID-enabled library visitor attendance and management system as a case study at STMKG. The system was developed to replace fragmented manual recording with a consistent digital workflow that supports three visitor categories within a unified visit log. Cadet attendance is captured through RFID-based identification, while employee visits are recorded through controlled selection and public visits through a structured manual form. Administrative functions were implemented to transform visit records into actionable outputs, including a statistics dashboard, report filtering and search, and spreadsheet export to support routine institutional reporting.

Beyond attendance capture, the implementation emphasizes deployable baseline security appropriate for a publicly reachable attendance endpoint. Administrative capabilities are restricted to authenticated users, bot-abuse mitigation is applied to the entry verification and login flows, and database-layer access boundaries are enforced to separate unauthenticated attendance usage from privileged management operations. Functional verification confirmed that critical end-to-end scenarios, including the three attendance paths, RFID registration for unregistered cards, reporting and export, and the essential security mechanisms, operate as intended within the defined scope.

The primary contribution of this work is a practical, end-to-end artifact that can be adopted in STMKG and adapted to similar higher-education libraries that require reliable attendance capture and structured reporting. The study is limited to a single institutional environment and does not include user acceptance evaluation, so broader generalization should be approached cautiously. Future work may incorporate usability and acceptance studies, multi-site replication, integration with institutional academic information systems, and longitudinal analysis of visit data to further support evidence-based library service improvements.

REFERENCE

[1] S. Mitha and M. Omarsaib, ‘Emerging Technologies and Higher Education Libraries: A Bibliometric Analysis of the Global Literature’, *Libr. Hi Tech*, vol. 43, no. 2–3, pp. 1248–1270, 2024, doi: 10.1108/lht-02-2024-0105.

[2] S. Nakaziba and P. Ngulube, ‘Harnessing Digital Power for Relevance: Status of Digital Transformation in Selected University Libraries in Uganda’, *Collect. Curation*, vol. 43, no. 2, pp. 33–44, 2024, doi: 10.1108/cc-11-2023-0034.

[3] K. Banleman, B. K. Dukper, and L. D. Banleman, ‘Evaluation of Academic Library Services and Programs in Ghana: Insight From the Sd Dombo University of Business and Integrated Development Studies’, *Int. J. Appl. Res. Soc. Sci.*, vol. 6, no. 1, pp. 89–105, 2024, doi: 10.51594/ijarss.v6i1.734.

[4] K. N. Igwe and A. S. Sulyman, ‘Smart Libraries: Changing the Paradigms of Library Services’, *Bus. Inf. Rev.*, vol. 39, no. 4, pp. 147–152, 2022, doi: 10.1177/02663821221110042.

[5] A. A. Adewojo and O. P. Monjolaoluwa, ‘Smart Library Environments: IoT and Automation for Next-Generation Services’, *Bus. Inf. Rev.*, 2025, doi: 10.1177/02663821251384884.

[6] T. W. Aji *et al.*, ‘Redesign of User Interface and Experience with Brand Identity Enhancement for the STMKG Website through WordPress Implementation’, *J. Comput. Phys. Earth Sci.*, vol. 5, no. 1, 2025, doi: 10.63581/JoCPES.v5i1.15.

[7] S. Saha and M. Roknuzzaman, ‘Library Practitioners’ Perceptions on the Applications of IoT in University Libraries of Bangladesh’, *Libr. Manag.*, vol. 45, no. 1/2, pp. 141–156, 2024, doi: 10.1108/lm-07-2023-0072.

[8] S. M. Wagner, M. Ramkumar, G. Kumar, and T. Schoenherr, ‘Supporting Disaster Relief Operations Through RFID: Enabling Visibility and Coordination’, *Int. J. Logist. Manag.*, vol. 35, no. 6, pp. 1681–1712, 2024, doi: 10.1108/ijlm-12-2022-0480.

[9] H. A. Abdulghani, N. A. Nijdam, and D. Konstantas, ‘Analysis on Security and Privacy Guidelines: RFID-Based IoT Applications’, *Ieee Access*, vol. 10, pp. 131528–131554, 2022, doi: 10.1109/access.2022.3227449.

[10] M. I. Khan, H. Tahir, M. I. Jobiullah, A. R. A. Khan, S. A. Begum, and I. Hafeez, ‘Enhancing IoT Security: A Lightweight Cloning Approach for RFID/NFC Access Control Systems’, *CDF*, vol. 52, no. 2, pp. 231–248, 2023, doi: 10.48047/qy0g4n52.

[11] A. M. Yasir *et al.*, ‘Comparative Performance Analysis of Firebase Realtime Database and Supabase Using Multi-Method Testing Approaches’, in *2025 5th International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS)*, 2025, pp. 303–308. doi: 10.1109/ICE3IS66769.2025.11281116.