DESIGN AND IMPLEMENTATION OF AN AUTHENTICATED LOCKER SYSTEM USING ELECTRONIC IDENTIFIER COIN-OPERATED TIME MANAGEMENT

Geovani L. Pabilona, Cran Leigh Mae A. Salamanca, Christian Glenn O. Bunayog and Rozano A. Pimentel
University of Science and Technology of Southern Philippines, Cagayan de Oro City, Philippines
Corresponding author: geovani.pabilona@ustp.edu.ph

Date of publication: 25 July, 2026

ABSTRACT. *Conventional shared lockers depend on mechanical keys and manual monitoring, creating difficulties in access control, occupancy tracking and time-limited use. This paper describes the design, fabrication and functional demonstration of a 12-compartment smart locker that combines institution-issued QR identifiers, a Raspberry Pi 4 controller, webcam-based decoding, relay-actuated solenoid locks and a 10-peso coin acceptor. The control logic verifies a registered identifier, confirms payment, assigns an available compartment, records occupancy time and requires an additional payment when the configured period is exceeded. Demonstration-level testing showed that the integrated modules executed the intended access sequence under normal indoor conditions; QR obstruction or poor positioning produced occasional decoding delays. The work establishes implementation feasibility only. Authentication accuracy, processing latency, coin-validation accuracy, failure rate, long-term reliability and user acceptance were not quantified because trial logs and validated survey data were not available. The prototype therefore provides a transparent engineering basis for controlled performance testing rather than evidence of operational superiority. Its principal contribution is the integration of QR authentication, coin-based time control, automated allocation and offline operation in a modular campus locker architecture.*

Keywords: access control; coin acceptor; QR code; Raspberry Pi; smart locker; time management

1. INTRODUCTION

Shared lockers are used in universities, libraries, offices, hospitals, transport terminals and recreational facilities. Mechanical keys remain inexpensive, but lost or duplicated keys, manual occupancy records and weak accountability can increase administrative effort. Embedded platforms and electronic identifiers allow authentication, event logging and lock actuation to be combined in one controller. Industrial Internet of Things research likewise emphasizes the integration of sensing, processing and communication for responsive physical systems [1, 2].

Existing electronic lockers use RFID, biometrics, passwords, one-time passwords and networked applications. A QR-based library locker reported by Rahayu et al. demonstrated the feasibility of using QR codes for compartment access [3]. More recent smart-locker work has incorporated multiple authentication modes and IoT monitoring [4], while secure smart-lock and safe-box studies have emphasized key management, transaction integrity and protection of physical assets [5, 6]. User-centered research on automated lockers also shows that accessibility, correct compartment allocation and a dependable interface are central service attributes [7].

These studies demonstrate progress in authentication and remote management, but the reviewed systems do not combine all the features targeted in the present prototype: institution-issued QR identification, offline control, automatic locker assignment, coin validation, configurable occupancy time and overtime charging. The purpose of this study was therefore to design and functionally demonstrate an integrated locker architecture for time-limited campus storage. The study asks whether the fabricated modules can execute the specified workflow under demonstration conditions. It does not claim quantified security, reliability, usability or economic effectiveness.

2. REVIEW OF RELATED TECHNOLOGIES

Authentication alternatives

RFID offers rapid contactless identification but requires a reader and a compatible credential [8]. Biometrics link access to physiological characteristics, yet recognition performance depends on sensor quality, environment and enrolment conditions [9]. QR identifiers can be decoded by commodity cameras and may reduce dedicated credential hardware when an institution already issues printed IDs. A QR-based authentication protocol has also been shown to support practical, low-cost authentication, although static codes must be protected against copying and replay [10]. The QR symbol itself should conform to the current ISO/IEC 18004:2024 specification [11, 12].

Embedded control and software

The Raspberry Pi provides general-purpose input/output, camera support and a Linux-based software environment suitable for coordinating authentication, payment and relay control [13]. OpenCV supplies image-processing functions [14], whereas pyzbar provides Python bindings to the ZBar barcode reader [15]. These tools support rapid prototyping, but their availability alone does not establish system accuracy; performance must be measured under defined lighting, distance, orientation and code-quality conditions.

Research gap and contribution

Contemporary systems increasingly employ multi-factor or networked access [4-6]. However, network dependence and complex credential infrastructures may not suit low-cost campus deployments. The present work contributes a locally controlled architecture that joins four functions rarely evaluated together in the reviewed literature: QR-based identity verification, automatic compartment allocation, coin-gated access and time-based overtime control. The contribution is architectural integration and transparent functional demonstration, not a comparative claim of higher security or reliability.

Table 1. : Functional comparison of representative access technologies

Feature	RFID	Biometric	Networked locker	Prototype
Electronic authentication	Yes	Yes	Yes	Yes

QR identifier	No	No	Optional	Yes
Coin-gated access	No	No	Uncommon	Yes
Automatic allocation	Optional	Optional	Common	Yes
Time/overtime control	Optional	Optional	Optional	Yes
Offline core operation	Yes	Yes	Often no	Yes

3. MATERIALS AND METHODS

Research design and scope

A developmental engineering design was used. The work comprised requirements definition, hardware selection, circuit and cabinet integration, software development and functional demonstration of the access sequence. The prototype contained 12 independently controlled compartments. Because the available study record did not include a test log with trial counts or a validated participant dataset, this paper reports observable system behavior only. No human-participant usability scores or inferential statistics are presented.

System architecture

A Raspberry Pi 4 served as the central controller. A webcam captured QR identifiers printed on institution-issued ID cards. The remaining hardware consisted of a programmable coin acceptor, relay module, normally locked solenoid mechanisms, liquid-crystal display, regulated power supply and uninterruptible backup supply. A local database stored registered identifiers, compartment status, transaction state and occupancy time. The modular arrangement allowed each additional compartment to be mapped to a relay channel and database record.

Control sequence

The operating sequence was implemented as follows: (1) capture and decode the QR identifier; (2) compare the decoded value with the local registration database; (3) reject an unregistered identifier or display available compartments for a registered user; (4) receive the user selection; (5) validate the required 10-peso coin; (6) actuate the corresponding relay and solenoid; (7) start the occupancy timer when storage begins; and (8) on retrieval, calculate any overtime charge and withhold unlocking until the required additional payment is validated. This sequence separates identity verification from payment authorization and maintains a local transaction record.

Software implementation

Python modules handled image acquisition, OpenCV preprocessing, pyzbar decoding, database queries, compartment selection, payment signals, timing, relay actuation and display messages. Exception handling returned the interface to a safe waiting state when decoding failed or payment was incomplete. The design used local control for the core access path so that loss of internet connectivity would not prevent ordinary operation.

Functional demonstration procedure

The submitted prototype record documents demonstration of registered-user access, QR decoding under normal indoor lighting, payment-gated unlocking, compartment assignment, timer initiation, overtime-payment logic, retrieval and short-duration backup-power operation. Observations were recorded qualitatively. The record does not state the number of trials, test duration, lighting level, camera distance, coin variants, induced fault conditions or raw event logs. Accordingly, terms such as accuracy, failure rate and long-term reliability are not calculated in this paper.

4. RESULTS

Integrated prototype operation

The 12-compartment prototype executed the intended end-to-end sequence during demonstration. A registered QR identifier initiated compartment selection; validated payment enabled the mapped relay; and the controller initiated timing and recorded the transaction. Retrieval required the same identifier, and the overtime branch requested additional payment when the configured period had been exceeded. These observations show functional integration under the reported conditions but do not establish production-level performance.

Table 2:Reported functional observations and evidentiary limits

Subsystem	Reported observation	Evidence limitation
QR authentication	Registered identifiers were decoded under normal indoor conditions; obstruction or poor positioning caused delays.	No trial count, accuracy, latency or lighting measurements.
Payment	Coin validation was required before locker actuation; overtime logic requested additional payment.	No accepted/rejected-coin matrix or validation error rate.
Allocation and lock	Selected available compartments were mapped to relay-actuated solenoids.	No actuation-time distribution or cycle-endurance test.
Occupancy timer	The timer started after storage and supported an overtime branch during retrieval.	No clock-drift or boundary-condition analysis.
Backup power	The controller remained operational during a temporary interruption.	Interruption duration and battery-load test were not reported.

Authentication behavior

The webcam and decoding pipeline recognized registered identifiers when the code was visible and correctly positioned. Partial obstruction and poor positioning led to observable delays, indicating that camera geometry and code quality should be controlled in a formal experiment. A static printed QR identifier is also susceptible to copying; therefore, deployment should bind the identifier to an account record, restrict duplicate active sessions and consider signed or time-limited tokens for higher-risk use.

Payment and time-control behavior

The payment module acted as an authorization condition rather than as the identity credential. This separation allowed the system to reject access when payment was absent and to request a further payment after overtime. Nevertheless, successful demonstrations cannot be described as accurate payment validation without testing genuine and invalid coins across repeated trials. Revenue sustainability likewise requires a cost model covering fabrication, maintenance, electricity, component replacement and utilization rates.

Reliability and usability

The integrated modules communicated sufficiently to complete the reported workflow. This finding is appropriately described as short-term functional operation, not continuous reliability. Similarly, informal favorable comments cannot substitute for a validated usability study. The qualitative labels used in earlier summaries, such as accurate, high and stable, are therefore omitted. A subsequent evaluation should report participants, sampling, instrument validation, descriptive statistics and test conditions.

5. DISCUSSION

The prototype extends QR-based locker access [3] by joining identity verification with payment and configurable occupancy control. Relative to multi-authentication and networked designs [4-6], local processing reduces dependence on connectivity but transfers security responsibility to the device, database and physical enclosure. The contribution is thus a different design trade-off rather than evidence that the prototype is more secure or convenient. The design also highlights the distinction between functional verification and performance evaluation. Demonstrating that a QR code can unlock a selected compartment answers whether the programmed sequence works in a test setting. Establishing authentication accuracy requires repeated registered and unregistered attempts under controlled lighting, distance, angle, obstruction and print-quality conditions. Payment accuracy requires a matrix of valid, invalid and counterfeit inputs; reliability requires cycle and duration testing; and usability requires a validated instrument administered to a defined sample.

The next evaluation stage is recommended to first quantify the engineering performance identified in Table 3. Philippine technology-education research demonstrates the value of explicit models and adequately reported samples. For example, Branzuela Jr., San Diego and Namoco used multiple regression to determine the relative contribution of learner and contextual factors to Computer-Aided Designing performance [16]. Although the outcome in that study differs from locker performance, its analytical logic is applicable: the dependent variable and its predictors must be defined, measured with defensible indicators and tested using a method appropriate to the research questions. For the locker, technical outcomes should include authentication success, response time, payment-validation performance and recovery from power or communication faults.

After the prototype meets predefined technical thresholds, its acceptance among intended users may be evaluated through the Technology Acceptance Model (TAM). Davis identified perceived usefulness and perceived ease of use as central determinants of technology acceptance [17]. In a closely related Philippine electro-mechanical education context, Esquinas and Namoco applied TAM to evaluate a programmable pedagogical mobile robot through perceived ease of use, perceived usefulness and behavioral intention [18]. This framework is directly applicable to the current study on smart locker. Perceived usefulness may be represented by faster locker allocation, reduced dependence on physical keys, transparent time monitoring and convenient temporary storage. Perceived ease of use may cover QR positioning, clarity of display instructions, coin insertion, compartment identification and retrieval. Behavioral intention may assess willingness to use the locker again or recommend it for campus deployment. Because a locker also handles identity and personal property, perceived security and trust should be examined as external variables rather than assumed from TAM alone. A future study may test whether perceived ease of use predicts perceived usefulness and whether both constructs predict behavioral intention, using an adapted instrument subjected to content validation, pilot testing, reliability analysis and construct validation.

Table 3. Minimum protocol for a subsequent quantitative evaluation

Domain	Required measurement	Recommended report
Authentication	Registered/unregistered trials across lighting, distance, angle and obstruction	Success, false acceptance/rejection, latency and 95% confidence intervals
Payment	Valid and invalid coin trials, including repeated insertions	Acceptance/rejection matrix and error rate
Locking	Repeated open-close cycles and power interruptions	Response time, failures per cycle and recovery behavior
Usability	Defined user sample and validated TAM-based instrument measuring perceived usefulness, perceived ease of use and behavioral intention; include perceived security/trust as external variables	Sampling and respondent profile; item sources; content and construct validity; reliability coefficients; descriptive results; and tested TAM relationships
Security	Threat model and attempts involving copied QR identifiers and database access	Observed vulnerabilities, controls and residual risks

6. CONCLUSION

A 12-compartment QR-authenticated, coin-operated locker was designed and functionally demonstrated using a Raspberry Pi 4, webcam, coin acceptor, relays, solenoid locks, local database, display and backup supply. The prototype executed the intended sequence of identity verification, compartment selection, payment authorization, timed occupancy, overtime handling and retrieval under the reported demonstration conditions. These observations support implementation feasibility but do not quantify authentication accuracy, payment accuracy, failure rate, long-term reliability, security improvement or user acceptance. The next stage should follow the controlled protocol proposed in Table 3 and should report complete raw-test summaries and validated participant data. Subject to that evaluation and appropriate security hardening, the modular architecture may provide a basis for cost-conscious campus storage applications.

7. REFERENCES

[1] Xu, L. D., He, W. and Li, S., "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, 10(4): 2233–2243 (2014). https://doi.org/10.1109/TII.2014.2300753

[2] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M., "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, 17(4): 2347–2376 (2015). https://doi.org/10.1109/COMST.2015.2444095

[3] Rahayu, Y., Afif, L. and Soh, P. J., "Design and development of smart lock system based QR-Code for library locker at Faculty of Engineering, Universitas Riau," *SINERGI*, 26(3): 379–384 (2022). https://doi.org/10.22441/sinergi.2022.3.013

[4] Alzhrani, A. A., Balfaqih, M., Alsenani, F., Alharthi, M., Alshehri, A. and Balfagih, Z., "Design and implementation of an IoT-integrated smart locker system utilizing facial recognition technology," *Engineering, Technology & Applied Science Research*, 14(4): 16000–16010 (2024). https://doi.org/10.48084/etasr.7737

[5] Sethuraman, S. C., Mitra, A., Li, K. C., Ghosh, A., Gopinath, M. and Sukhija, N., "Loki: A physical security key compatible IoT based lock for protecting physical assets," *IEEE Access*, 10: 112721–112730 (2022). https://doi.org/10.1109/ACCESS.2022.3216665

[6] Alothman, B., Joumaa, C., Alotaibi, A., Alotaibi, B., Almutairi, B., Aldhafairi, A. and Khan, M., "Development of an electronic smart safe box using private blockchain technology," *Applied Sciences*, 12(13): 6445 (2022). https://doi.org/10.3390/app12136445

[7] Ciesla, M., "Perceived importance and quality attributes of automated parcel locker services in urban areas," *Smart Cities*, 6(5): 2661–2679 (2023). https://doi.org/10.3390/smartcities6050120

[8] Finkenzeller, K., *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*, 3rd ed., John Wiley & Sons, Chichester, U.K. (2010).

[9] Jain, A. K., Ross, A. and Prabhakar, S., "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1): 4–20 (2004). https://doi.org/10.1109/TCSVT.2003.818349

[10] Liao, K. C. and Lee, W. H., "A novel user authentication scheme based on QR-Code," *Journal of Networks*, 5(8): 937–941 (2010). https://doi.org/10.4304/jnw.5.8.937-941

[11] DENSO WAVE Incorporated, "QR Code essentials," *QRcode.com*. https://www.qrcode.com/en/ (accessed 4 August 2026).

[12] International Organization for Standardization, *ISO/IEC 18004:2024 Information Technology—Automatic Identification and Data Capture Techniques—QR Code Bar Code Symbology Specification*, ISO, Geneva, Switzerland (2024).

[13] Upton, E. and Halfacree, G., *Raspberry Pi User Guide*, 4th ed., John Wiley & Sons, Chichester, U.K. (2016).

[14] Bradski, G., "The OpenCV library," *Dr. Dobb's Journal of Software Tools*, 25(11): 120–125 (2000).

[15] Natural History Museum, *pyzbar: Python Wrapper for ZBar Barcode Reader*. https://github.com/NaturalHistoryMuseum/pyzbar (accessed 4 August 2026).

[16] Branzuela Jr., N. F., San Diego, A. L. and Namoco, S. O., "A multiple regression analysis of the factors affecting academic performance of Computer-Aided Designing students during flexible learning program in Philippine state universities," *Science International (Lahore)*, 34(6): 525–530 (2022).

[17] Davis, F. D., "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, 13(3): 319–340 (1989). https://doi.org/10.2307/249008

[18] Esquinas, E. A. S. and Namoco, S. O., "The utilization of TAM to evaluate the acceptability of the programmable pedagogical mobile robot in electro-mechanical course," *Science International (Lahore)*, 35(3): 231–234 (2023).