UNIVERSIDAD NACIONAL DE SAN MARTIN

RCSI
https://revistas.unsm.edu.pe/index.php/rcsi
e-ISSN: 2709-992X

Original article
Artículo orginal
Jul-Dec, 2025

IoT-Based Smart Lock with Real-Time Person Detection Using YOLOv5 and Mobile App Integration

Cerradura inteligente basada en IoT con detección de personas en tiempo real mediante YOLOv5 e integración de aplicaciones móviles

Dick Díaz-Delgado[1]*, Sergio M. Vigil-Ramirez[2], Luis J. Acho-Cachay[2], Brandom R. Tuanama-Chávez[2], Luis A. Rojas-Puerta[2]

[1]Faculty of Systems and Computer Engineering, Universidad Nacional de San Martín, Tarapoto, Peru
[2]Faculty of Engineering and Architecture, Universidad Cesar Vallejo, Tarapoto, Peru

Received: 09 Mar 2025 | **Accepted:** 18 Jul. 2025 | **Published:** 20 Jul. 2025

Corresponding author*: ddiazd@unsm.edu.pe

How to cite this article: Díaz-Delgado, D., Vigil-Ramirez, S. M., Acho-Cachay, L. J., Tuanama-Chávez, B. R. & Rojas-Puerta, L. A. (2025). IoT-Based Smart Lock with Real-Time Person Detection Using YOLOv5 and Mobile App Integration. *Revista Científica de Sistemas e Informática, 5*(2), e1005. https://doi.org/10.51252/rcsi.v5i2.1005

ABSTRACT

This article presents the design and implementation of a smart electronic lock system that integrates Internet of Things (IoT) technologies, computer vision, and multifactor authentication to enhance residential security. The solution is built upon a LilyGo ESP32-S3 microcontroller with an embedded camera and leverages a YOLOv5-based person detection model for real-time monitoring. A mobile application, developed in Flutter and integrated with Firebase, enables secure user interaction, remote access control, and real-time alerts. The system combines three authentication factors: a keypad code, visual detection of authorized individuals, and mobile app verification. Experimental validation with ten participants demonstrated an average detection accuracy of 96%, outperforming comparable systems. The proposed approach stands out for its low cost, modularity, and high adaptability to smart home environments. This research contributes to the development of accessible and robust security solutions using edge AI and distributed architectures.

Keywords: computer vision; IoT security; mobile application; person detection; smart lock

RESUMEN

Este artículo presenta el diseño e implementación de un sistema de cerradura electrónica inteligente que integra tecnologías de Internet de las Cosas (IoT), visión por computador y autenticación multifactor para mejorar la seguridad residencial. La solución se basa en un microcontrolador LilyGo ESP32-S3 con cámara incorporada y utiliza un modelo de detección de personas basado en YOLOv5 para monitoreo en tiempo real. Se desarrolló una aplicación móvil en Flutter, integrada con Firebase, que permite la interacción segura del usuario, el control remoto del acceso y el envío de alertas en tiempo real. El sistema combina tres factores de autenticación: ingreso de clave por teclado, detección visual de personas autorizadas y validación mediante la aplicación móvil. Las pruebas experimentales con diez participantes demostraron una precisión promedio del 96% en la detección de personas, superando soluciones comparables. La propuesta destaca por su bajo costo, modularidad y alta adaptabilidad a entornos domóticos. Esta investigación contribuye al desarrollo de soluciones de seguridad accesibles y robustas, basadas en inteligencia artificial de borde y arquitecturas distribuidas.

Palabras clave: visión por computador, seguridad IoT, aplicación móvil, detección de personas, cerradura inteligente

1. INTRODUCTION

Home security is a basic need that has taken on renewed urgency in today's context of growing urbanization, rising crime rates, and expanding technological availability. The increase in burglaries and unauthorized access to residential spaces has driven the search for solutions that allow users to exercise more effective and personalized control over their domestic environments. In this regard, the Internet of Things (IoT) has enabled the development of new forms of protection through connected systems capable of monitoring, detecting, and responding to suspicious events in real time (Castaño-Gómez et al., 2022).

The development of low-cost microcontrollers, such as the ESP32 or Arduino-compatible platforms, along with the use of open-source technologies, has facilitated the implementation of home automation solutions focused on access control and the management of smart locks (Amaya Fariño et al., 2020). These technologies, when integrated with sensors, communication modules, and mobile applications, enable users to remotely control door locking mechanisms, monitor access logs, receive alerts, and configure authorization levels independently, without relying on intermediaries (Tiwari et al., 2018).

Numerous studies have proposed systems that integrate biometric authentication—such as facial recognition, voice control, or fingerprint scanning—with varying levels of effectiveness. Uddin et al. (2022) implemented a facial authentication system that achieved an accuracy of 92.86% using the Haar Cascade and LBPH algorithms. Meanwhile, Karimi et al. (2020) proposed a dual-authentication solution based on voice commands and facial recognition using the PCA algorithm, demonstrating that the system's performance was highly dependent on factors such as lighting conditions and facial orientation.

However, significant challenges remain regarding integration, interoperability, and cybersecurity. The diversity of communication protocols and the lack of universal standards hinder seamless connectivity between devices from different manufacturers (Lee & Lee, 2021). Moreover, many IoT systems lack robust protection mechanisms against cyberattacks, which poses a risk to user data privacy and integrity (Morales-Nava et al., 2023). The choice of communication protocol also has a direct impact on system performance; for example, Quiñones et al. (2020) demonstrated that MQTT performs better than HTTP in terms of latency and energy consumption in 4G mobile networks.

In response to this scenario, the present article proposes the development of a smart electronic lock based on the ESP32-S3 microcontroller with an integrated camera, combining multifactor authentication with computer vision algorithms and lightweight communication protocols. The system is designed to easily integrate with other IoT devices, be controlled via a mobile application, and generate real-time security alerts. This proposal aims to contribute to the design of accessible, secure, and sustainable solutions for strengthening residential security, following an open, modular, and user-centered approach.

1.2 Related work

The implementation of IoT-based smart locks has evolved significantly in recent years through diverse technological strategies. Most of these efforts can be grouped into three major approaches: biometric and multifactor authentication systems, IoT-integrated architecture with remote control, and embedded security solutions for hardware protection.

A substantial body of work has explored biometric authentication, frequently combining facial recognition, fingerprint scanning, or voice commands to increase security and usability. Systems developed using platforms like Raspberry Pi or Arduino have achieved accuracy levels between 90% and 92.86%, often relying on algorithms such as LBPH, PCA, or Haar Cascade (Ibrahim et al., 2020; Karimi et al., 2020; Krishna et al., 2023; Padhan et al., 2023; Praneeth et al., 2024; Uddin et al., 2022). More recent approaches have introduced multimodal authentication through AI-powered models like HUMBIA and UMBIA, showing increased robustness and efficiency (Vaishnavi et al., 2024, 2025).

Parallel to this, a wide array of proposals has addressed smart lock connectivity and functionality within IoT ecosystems. These systems typically integrate password entry, RFID, mobile applications, and GSM-based alert mechanisms using microcontrollers such as ESP32-CAM or Bolt IoT (Hashim et al., 2023; Morales-Nava et al., 2023; Nagasree Y et al., 2021; PBV et al., 2024; R. S et al., 2022; Tiwari et al., 2018). In some cases, accessibility and remote control were emphasized by implementing mobile apps or Zero UI concepts for gesture-based interaction (Chowdhury Joy et al., 2023; Mahendra et al., 2018).

The security of communication protocols has also been a critical research area. Several works compared HTTP and MQTT performance, confirming that MQTT offers lower latency and energy consumption (Quiñones et al., 2020). Others explored the integration of blockchain, SDN, and biometric encryption schemes to address the interoperability and data privacy challenges faced in heterogeneous IoT environments (Lee & Lee, 2021; Panarello et al., 2018).

Additionally, recent investigations have turned attention to hardware-level security and embedded system protection. Techniques such as logic locking, PUF-based circuit design with FeFETs, and fault injection testing have been applied to prevent reverse engineering and tampering in smart lock platforms (Alves de Abreu et al., 2025; Kar et al., 2024; Kolla et al., 2022; Lojda et al., 2021).

Further contributions have examined novel directions such as explainable AI for password strength assessment (Shreya et al., 2024) and smart locker systems designed for public or medical use (Aggarwal & Sharma, 2022; Chandrappa et al., 2025), underscoring the versatility and cross-domain applicability of smart lock technologies.

Despite this growing body of literature, key challenges persist. Many systems remain limited by high cost, restricted interoperability, or limited edge-processing capabilities. Furthermore, while several works have explored biometric or multifactor authentication, few have proposed lightweight, scalable solutions combining YOLOv5-based visual detection with multifactor logic and real-time app control using a low-cost microcontroller such as the ESP32-S3.

The present study addresses this gap by integrating real-time object detection, distributed processing, and mobile-based system management into a cohesive, accessible, and adaptable architecture for residential intrusion prevention.

2. MATERIALS AND METHODS

The methodological design of this study was structured into three main stages: (1) development of the smart lock hardware, (2) training and deployment of the YOLOv5 person detection model, and (3) implementation of a mobile application for remote system interaction and notification delivery.

2.1 Smart Lock System Architecture

The smart lock system integrates multiple components (Figure 1) coordinated through a LilyGo-Cam ESP32-S3 microcontroller, which handles communication and visual input. The system includes a 4×4 matrix keypad for local password entry, a magnetic sensor to detect forced entries, a PIR sensor for motion detection, and an Arduino Uno for managing keypad input signals. Lock activation is controlled through a relay module powered by a 220V to 18V transformer.

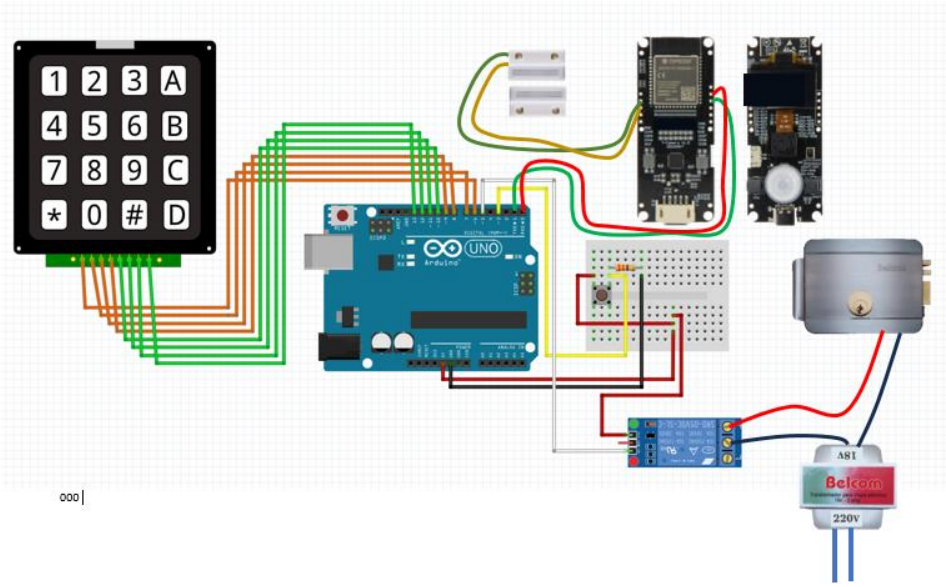

Figure 1. Electronic lock circuit diagram

The overall interaction between the hardware modules is illustrated in the system block diagram (Figure 2). Two authentication modes were implemented: keypad input and mobile app control. If three consecutive incorrect codes are entered, an alert is automatically triggered. This dual-access design improves security and user flexibility.

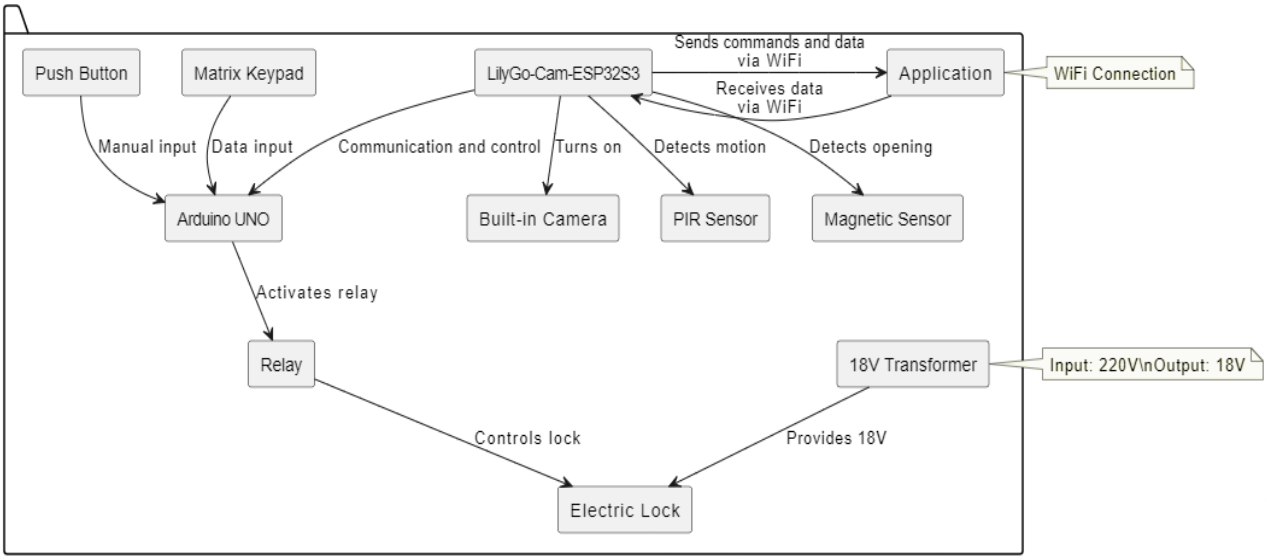

Figure 2. Block diagram of the smart lock operation

The system's operational flow is detailed in the activity diagram (Figure 3), which maps the steps from password input or mobile request to alert generation and lock actuation. This diagram includes motion and tampering detection, ensuring continuous monitoring and responsive control.

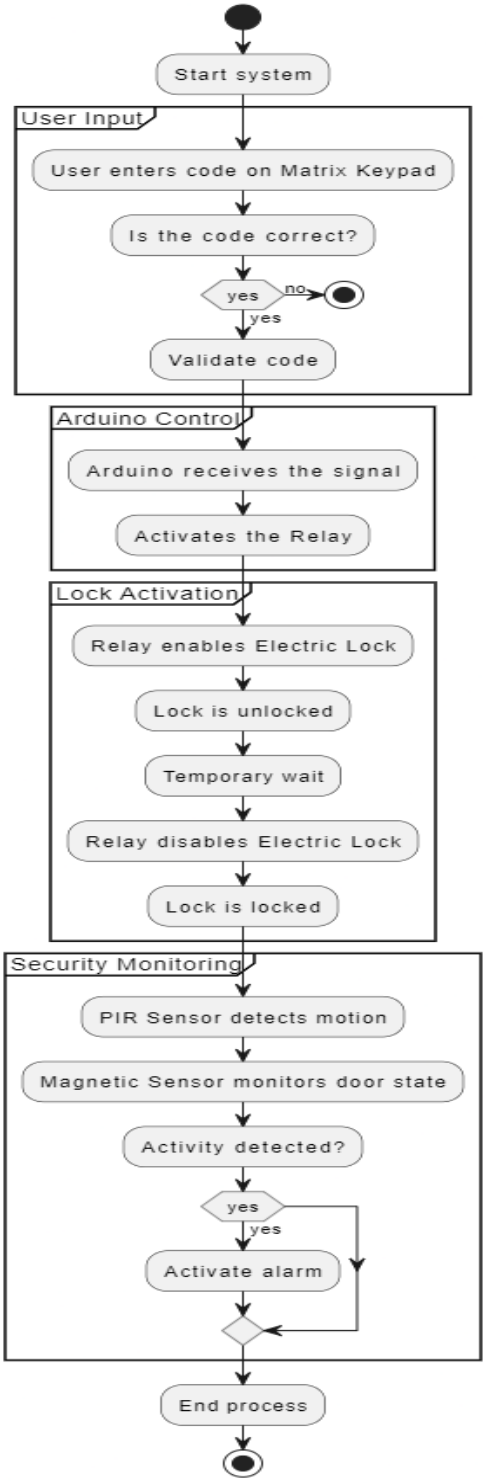

Figure 3. Activity diagram of the smart lock

2.2 YOLOv5 Model Training and Deployment

Person detection was implemented using YOLOv5s, a lightweight convolutional neural network suited for embedded applications. The training process involved the following configuration:

2.2.1 Dataset

A custom dataset of 200 images, annotated with bounding boxes for person detection. The dataset was split 80/20 for training and validation, respectively.

2.2.2 Augmentation

Applied techniques included horizontal flip, brightness shifts, and Gaussian noise to increase model robustness under varying residential conditions.

2.2.3 Hyperparameters

The model was trained over 100 epochs with a batch size of 16, initial learning rate of 0.001, and SGD optimizer. Anchor boxes were recalculated using k-means clustering.

2.2.4 Thresholds

A detection confidence threshold of 0.80 was selected to reduce false positives.

2.2.5 Validation metrics

The model achieved a mAP@0.5 of 94.7% and an F1-score of 0.91 on the validation set.

2.2.6 Deployment

The trained model was converted to TorchScript and deployed via a Flask API hosted on an external server. The ESP32-S3 sends image captures through HTTP requests, and server responses are sent back with detection results.

A visual output of detection during testing is presented in Figure 4, showing accurate person identification by the system.

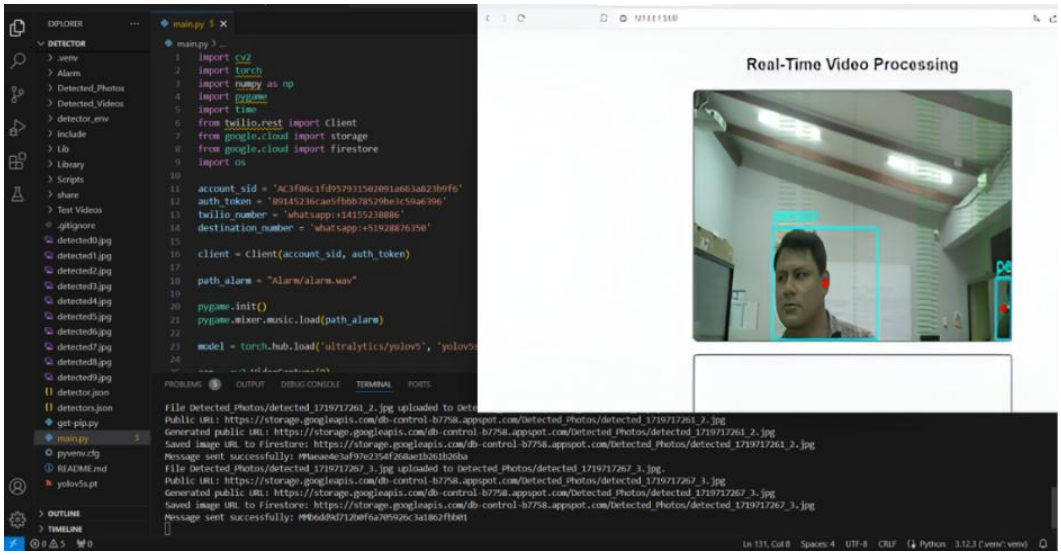

Figure 4. Performance Evaluation of the YOLOv5 Model

2.3 System Hardware Implementation and Configuration

The assembled components during testing are shown in Figure 5. The ESP32-S3 manages camera operations and app communication, while the Arduino Uno processes keypad inputs. The magnetic and PIR sensors enable real-time alerts for intrusion or tampering. All devices communicate reliably under the power regulation of the transformer, ensuring safe and stable operation.

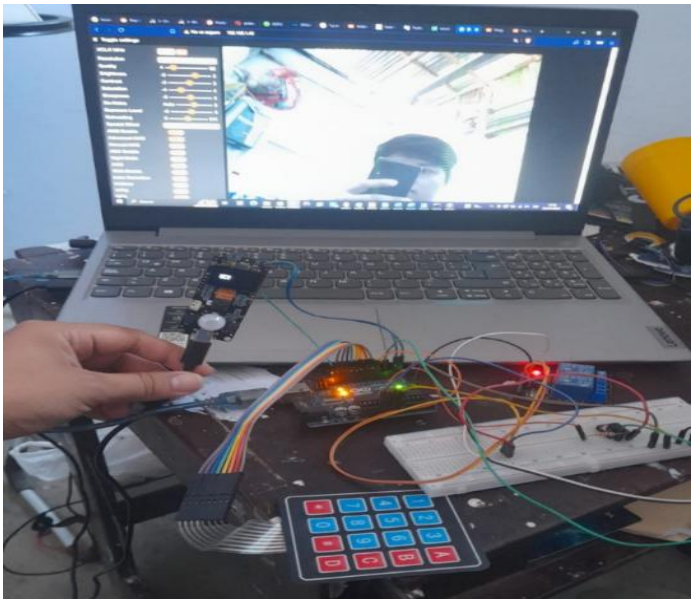

Figure 5. Configuration and recognition tests

2.4 Mobile Application and Interface Design

The Flutter-based mobile application provides user interaction with the system. It includes remote lock/unlock control, status monitoring, and intruder alert reception via Firebase Cloud Messaging. Firebase Authentication ensures secure user login, while captured images and logs are stored in Firestore and Firebase Storage. A role-based user system distinguishes between administrators and standard users.

The app's workflow, from login to alert reception, is summarized in the activity diagram (Figure 6), which ensures intuitive navigation and system awareness for the user.

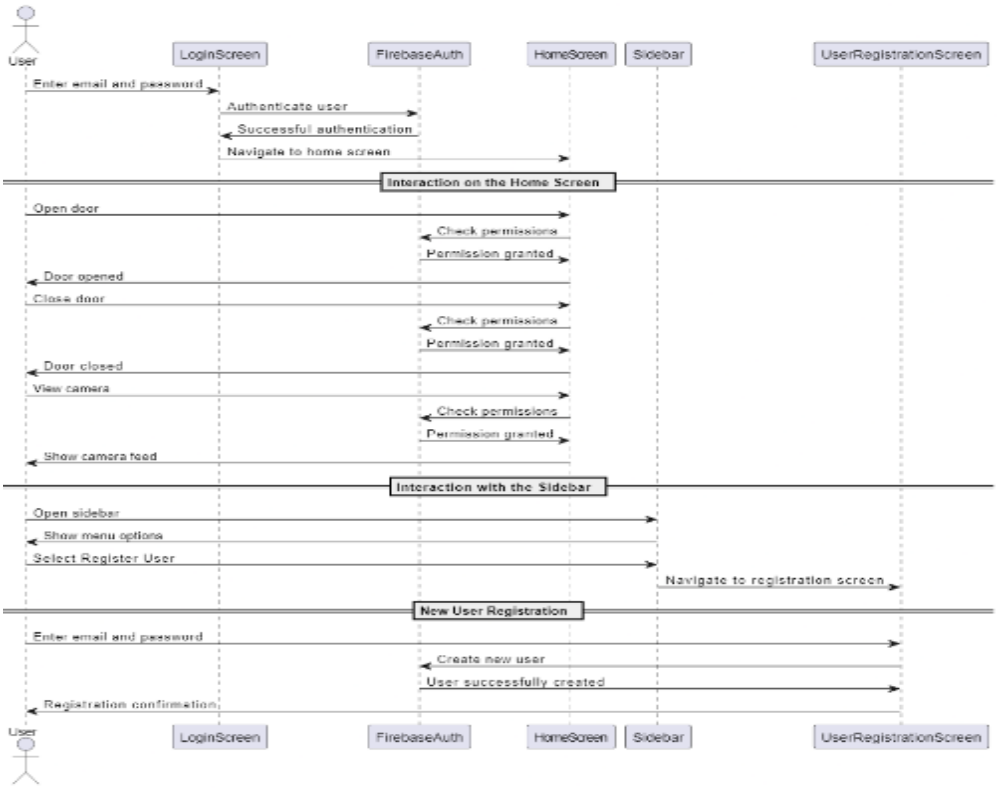

Figure 6. Activity diagram of the application process

The final user interface flow is shown in Figure 7, demonstrating step-by-step transitions including unlocking the door, receiving visual alerts, and accessing log data.

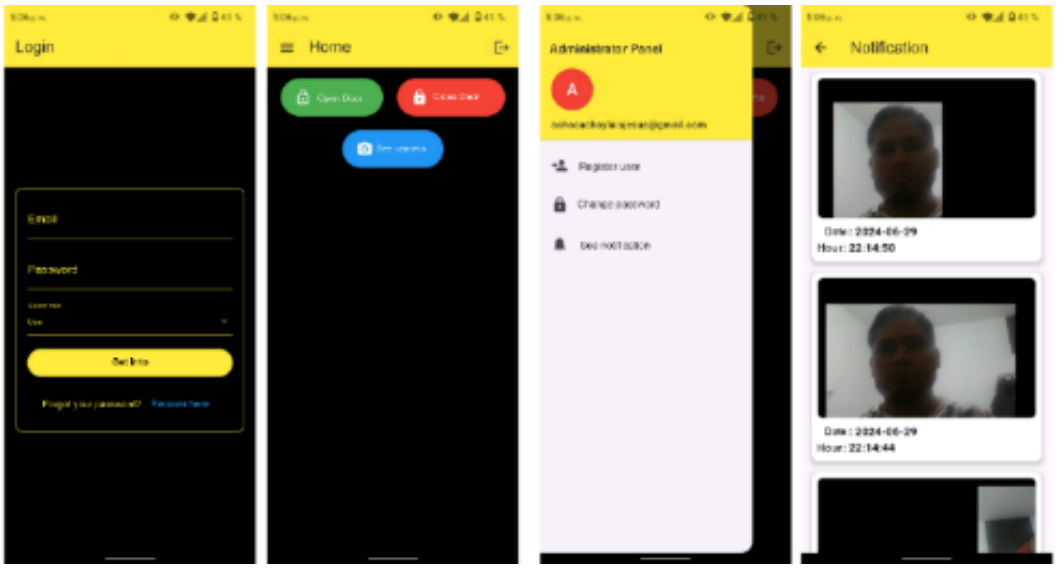

Figure 7. Operational workflow of the smart lock system

2.5 Experimental Procedure

System performance was evaluated through real-world trials involving 10 participants. Each subject approached the door and was recorded during 10 detection events under varied lighting conditions. Each detection attempt was logged and compared with the ground-truth presence. True positives, false positives, and accuracy rates were recorded and analyzed.

Additionally, scenarios involving incorrect password attempts and sensor-triggered intrusions were simulated to validate system response time, app notifications, and lock behavior under stress.

2.6 Design Justification

The choice of YOLOv5s balanced model performance with embedded system constraints, while offloading inference to a server allowed for high-accuracy detection without compromising ESP32-S3 performance. The use of multifactor authentication—via keypad, visual detection, and app validation—enhances security, and Firebase infrastructure supports scalable data handling and notification delivery.

3. RESULTS AND DISCUSSION

The results of this study highlight both the operational capabilities and methodological limitations of the proposed smart lock system. The mobile application (Figure 8) proved to be an essential component of the system, offering users a seamless interface to unlock the door remotely, receive real-time alerts, and monitor activity through captured images. The app's responsiveness was consistent under standard Wi-Fi conditions, with low latency observed between detection events and alert reception. Its architecture, based on Firebase services, allowed for role-based access management and ensured that future integration of features such as mobile-based biometrics could be implemented with minimal structural changes.

The visual alert process is illustrated in Figure. When an unrecognized person is detected with a confidence threshold of 80% or higher, the system automatically captures an image, which is sent to the server for inference and then stored in Firebase Storage. A push notification is immediately delivered to the user via Firebase Cloud Messaging. This streamlined process allows the user to verify the alert in real time and determine whether the detected individual represents a potential threat. The integration of computer vision, real-time alerting, and cloud-based image storage enhances the system's utility in domestic security scenarios.

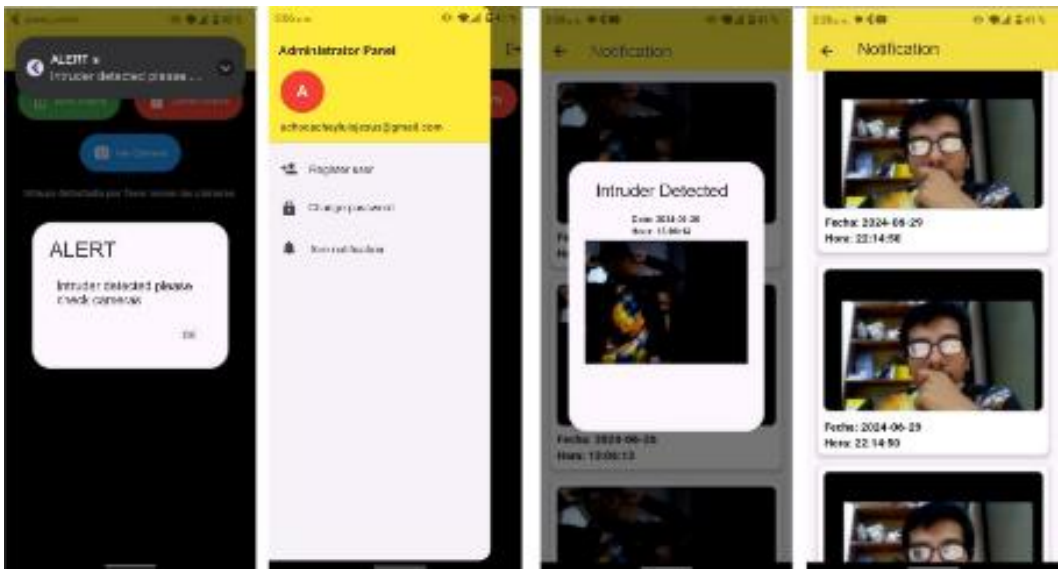

Figure 8. Intruder alert process

Despite its strengths, the evaluation of detection accuracy reveals certain limitations. The system was trained on a dataset of only 200 labeled images, which restricts its ability to generalize under complex and varied conditions such as different lighting, postures, or facial occlusions. Figure 9 presents the overall accuracy, which reached an average of 96% in controlled conditions. However, the model may be susceptible to overfitting due to the limited diversity of the training data.

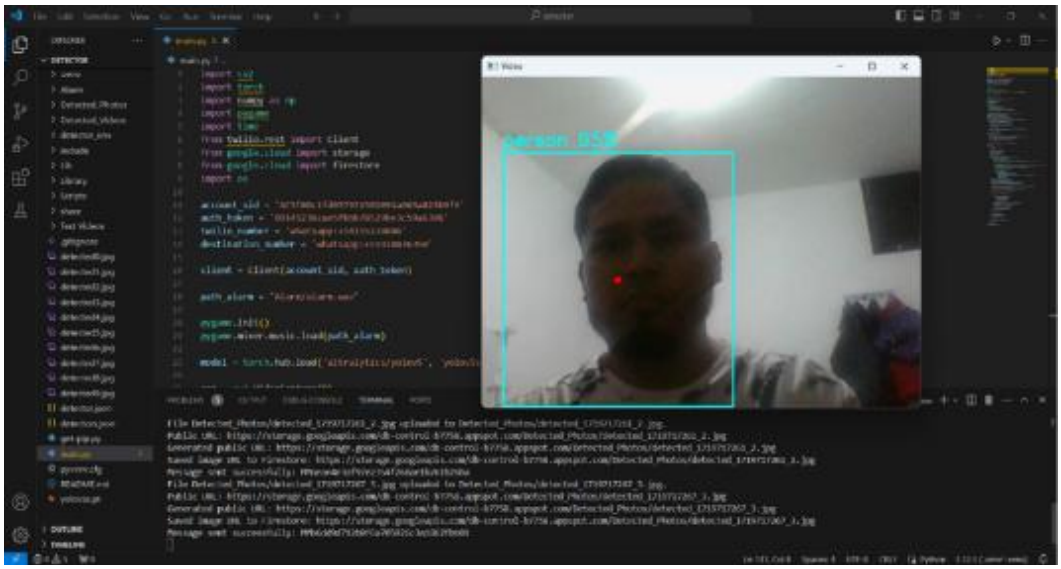

Figure 9. Intruder detector accuracy percentage

To assess detection performance, 10 participants performed 10 trials each. Table 1 shows that six users achieved 100% detection accuracy, while the remaining four recorded one false positive,

resulting in 90% accuracy. While the high success rate is encouraging, the lack of statistical indicators such as standard deviation, confidence intervals, and confusion matrices limits the analytical rigor of the results. Including such metrics in future assessments would enable a more reliable evaluation of model performance across broader scenarios.

Table 1. Performance of the person detection system during individual tests

Subject ID	Number of Attempts	True Positives	False Positives	Detection Accuracy (%)
Subject 01	10	10	0	100
Subject 02	10	10	0	100
Subject 03	10	9	1	90
Subject 04	10	9	1	90
Subject 05	10	10	0	100
Subject 06	10	9	1	90
Subject 07	10	10	0	100
Subject 08	10	9	1	90
Subject 09	10	10	0	100
Subject 10	10	10	0	100

To calculate the accuracy, we used the following formula:

$$Accuracy = \left(\frac{Correct\ detections}{Total\ attempts}\right) x100$$

The average system accuracy was calculated by summing the individual accuracies and dividing by the number of participants.

$$Average\ Accuracy = \left(\frac{100 + 100 + 90 + 90 + 100 + 90 + 100 + 90 + 100 + 100}{10}\right)$$

$$Average\ Accuracy = \left(\frac{960}{10}\right)$$

$$Average\ Accuracy = 96\%$$

When compared to existing smart lock systems, the proposed solution demonstrates favorable performance. As shown in Table 2. Comparative accuracy of person detection algorithms used in smart locks, Uddin et al. (2022) achieved 92% accuracy using Haar Cascade, and Derbali (2025) reported 92.86% using a hybrid DeSGCBQNN model. The 96% achieved by our system using YOLOv5s and OpenCV exceeds these benchmarks. This improvement may be attributed to the adoption of a real-time object detection model with a strict confidence threshold, which helps reduce false positives. However, it is important to note that many of the compared studies used larger public datasets or incorporated multimodal biometric authentication, enhancing their robustness. Our system, by contrast, relies solely on visual detection and a relatively small, customized dataset. These factors must be considered when drawing conclusions from comparative analysis.

Table 2. Comparative accuracy of person detection algorithms used in smart locks

Author	Model	Precision (%)
Derbali (2025)	Distributed Encoder Shannon Gaussian Correntropy Bayesian Q-Neural Networks (DeSGCBQNN)	92.86
Uddin et al. (2022)	Haar Cascade	92
Proposed model	YOLOv5, OpenCV	96

The final assembled prototype (Figure 10) integrates all system components, including the ESP32-S3 microcontroller, camera, keypad, sensors, relay, and power module. During testing, the prototype performed reliably in detecting intruders, triggering alerts, and enabling both manual and remote unlocking. However, the prototype has yet to be validated under real-world deployment conditions involving unstable internet connections, environmental interference, or tampering attempts. Future work should include stress testing to evaluate the system's resilience and to ensure operational integrity in practical environments.

Figure 10. Prototype of the electronic lock

CONCLUSIONS

The development of a smart electronic lock based on IoT and computer vision, as presented in this study, demonstrates the feasibility of integrating low-cost hardware with AI-based person detection and mobile app functionality to improve residential security. The system effectively combines a keypad, YOLOv5s-based visual detection, and mobile app verification as part of a multifactor authentication mechanism. Experimental tests showed an average detection accuracy of 96%, confirming the system's potential compared to similar solutions in the literature.

However, the study presents important methodological limitations. The person detection model was trained on a relatively small dataset (200 images), which may not capture the full diversity of real-world scenarios, including different lighting conditions, occlusions, or complex facial angles. Moreover, although ten users participated in the validation phase, the absence of statistical significance testing (e.g., standard deviation, confidence intervals) limits the generalizability of the results. The system was also tested under controlled lab conditions, and its behavior in dynamic, real-life environments remains unvalidated.

Future work should directly address these constraints. First, expanding the dataset with more diverse and labeled images—ideally from public sources—will help improve generalization. Second, incorporating statistical analyses during testing will provide a stronger basis for performance evaluation. Third, testing the system in realistic residential settings with network fluctuations, physical tampering, and environmental interference will allow for more accurate assessment of robustness and usability. Lastly, the proposed architecture could be extended by

integrating lightweight biometric modalities (e.g., voice or gait recognition), as well as exploring edge-based inference to reduce dependency on cloud services.

By acknowledging these limitations and proposing focused future directions, this study provides a technically sound foundation that can be iteratively enhanced. The proposed system represents a promising step toward accessible, scalable, and adaptive smart security solutions for domestic environments.

FINANCING

The author did not receive sponsorship to carry out this study-article.

ACKNOWLEDGMENTS

Sincere thanks to Universidad César Vallejo for providing an adequate space in the Fab Lab area and all the necessary facilities to carry out this research. Their support has been fundamental for the development of this work.

CONFLICT OF INTEREST

There is no conflict of interest related to the subject matter of the work.

AUTHORSHIP CONTRIBUTION

Conceptualization, data curation, formal analysis, investigation, and visualization were carried out by Dick Diaz-Delgado, Sergio M. Vigil-Ramirez, Luis J. Acho-Cachay, Brandom R. Tuanama-Chávez, and Luis A. Rojas-Puerta. Methodology was developed by Dick Diaz-Delgado, Sergio M. Vigil-Ramirez, and Luis J. Acho-Cachay. Acquisition of funds and project administration were managed by Dick Diaz-Delgado. Resources were provided by Dick Diaz-Delgado, Brandom R. Tuanama-Chávez, and Luis A. Rojas-Puerta. Software development was conducted by Luis J. Acho-Cachay and Brandom R. Tuanama-Chávez. Supervision and validation were the responsibility of Dick Diaz-Delgado. Writing – original draft and writing – review and editing were also performed by Dick Diaz-Delgado.

REFERENCES

Aggarwal, S., & Sharma, S. (2022). Voice Based Secured Smart Lock Design for Internet of Medical Things: An Artificial Intelligence Approach. *2022 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*, 1–7. https://doi.org/10.1109/WiSPNET54241.2022.9767113

Alves de Abreu, B., Paim, G., Alrahis, L., Flores, P., Sinanoglu, O., Bampi, S., & Amrouch, H. (2025). On the Efficacy and Vulnerabilities of Logic Locking in Tree-Based Machine Learning. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *72*(1), 180–191. https://doi.org/10.1109/TCSI.2024.3457541

Amaya Fariño, L., Tumbaco Reyes, A., Roca Quirumbay, E., Villón González, T., Mendoza Morán, B., & Reyes Quimís, Á. (2020). El IoT aplicado a la Domótica. *Revista Científica y Tecnológica UPSE*, *7*(1), 21–28. https://doi.org/10.26423/rctu.v7i1.490

Castaño-Gómez, M., López Echeverry, A. M., & Villa Sánchez, P. A. (2022). Revisión del uso de tecnologías y dispositivos IoT en los sistemas de seguridad física. *Ingeniería y Competitividad*, *24*(1). https://doi.org/10.25100/iyc.v24i1.11034

Chandrappa, S., Prithviraj, H, A. P., I S, R., R, M. S. K., & R, S. S. (2025). Smart Locker 2.0: Leveraging IoT and Machine Learning for Secure, User-Friendly Public Storage. *2025 International Conference on Artificial Intelligence and Data Engineering (AIDE)*, 696–700. https://doi.org/10.1109/AIDE64228.2025.10987522

Chowdhury Joy, M. H., Karim, M. M. A., Choudhury, A. H., Razin, M., & Ahmed, S. N. M. (2023). An IoT Based Smart Vault Security and Monitoring System with Zero UI. *2023 3rd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, 95–100. https://doi.org/10.1109/ICREST57604.2023.10070057

Derbali, M. (2025). Facial authentication based smart door lock system and anomaly detection using machine learning architectures integrated with IoT. *Research Square Preprint*. https://doi.org/10.21203/rs.3.rs-3247506/v1

Hashim, K., Qasim, H., Hamzah, A., Hasan, O., & Al-Jadiri, M. (2023). Door lock system based on internet of things and Bluetooth by using Raspberry Pi. *Bulletin of Electrical Engineering and Informatics*, *12*(5), 2753–2762. https://doi.org/10.11591/eei.v12i5.5134

Ibrahim, S., Shukla, V. K., & Bathla, R. (2020). Security Enhancement in Smart Home Management Through Multimodal Biometric and Passcode. *2020 International Conference on Intelligent Engineering and Management (ICIEM)*, 420–424. https://doi.org/10.1109/ICIEM48762.2020.9160331

Kar, A., Chauhan, Y. S., & Amrouch, H. (2024). Innovations in Hardware Security: Leveraging FeFET Technology for Future Opportunities. *2024 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, 457–460. https://doi.org/10.1109/APCCAS62602.2024.10808824

Karimi, K., Kabrane, M., Hassan, O., & Krit, S. (2020). Secure Smart Door Lock System based on Arduino and Smartphone App. *Journal of Advanced Research in Dynamical and Control Systems*, *12*(1), 407–414. https://doi.org/10.5373/jardcs/v12sp1/20201088

Kolla, S., Sk, A., Veeramachaneni, S., & Sk, N. M. (2022). Logic Locking Designs at Transistor Level for Full Adders. *2022 IEEE International Symposium on Smart Electronic Systems (iSES)*, 289–292. https://doi.org/10.1109/iSES54909.2022.00065

Krishna, M. Y. S., Arya, A., Ansari, S., Awasya, S., Sushakar, J., & Uikey, N. (2023). Real Time Door Unlocking System using Facial Biometrics based on IoT and Python. *2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, 1–5. https://doi.org/10.1109/SCEECS57921.2023.10063142

Lee, J. Y., & Lee, J. (2021). Current Research Trends in IoT Security: A Systematic Mapping Study. *Mobile Information Systems*, *2021*(1), 8847099. https://doi.org/10.1155/2021/8847099

Lojda, J., Panek, R., Podivinsky, J., Cekan, O., Krcma, M., & Kotasek, Z. (2021). Testing Embedded Software Through Fault Injection: Case Study on Smart Lock. *2021 IEEE 22nd Latin American Test Symposium (LATS)*, 1–6. https://doi.org/10.1109/LATS53581.2021.9651770

Mahendra, S., Sathiyanarayanan, M., & Vasu, R. B. (2018). Smart Security System for Businesses

using Internet of Things (IoT). *2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT)*, 424–429. https://doi.org/10.1109/ICGCIoT.2018.8753101

Morales-Nava, R., Sosa Sales, A., Jiménez-Echeverría, J. R., Enríquez Díaz, J. M., & Barreto De La Cruz, J. L. (2023). Implementación de un control de acceso en cerradura eléctrica con base al reconocimiento facial y huella dactilar para elevar el nivel de seguridad en los hogares. *Ciencia Latina Revista Científica Multidisciplinar*, *7*(3), 5976–5991. https://doi.org/10.37811/cl_rcm.v7i3.6602

Nagasree Y, L. V., Rupa, Ch., Dharmika, B., Nithin, T. G., & Vineela, N. (2021). Intelligent Secure Smart Locking System using Face Biometrics. *2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)*, 268–273. https://doi.org/10.1109/RTEICT52294.2021.9573869

Padhan, D. G., Varma, S. N., C, V., Divya, M., Manasa, S., & Pakkiraiah, B. (2023). Home Security System Based on Facial Recognition. *2023 IEEE 3rd International Conference on Sustainable Energy and Future Electric Transportation (SEFET)*, 1–6. https://doi.org/10.1109/SeFeT57834.2023.10244798

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT Integration: A Systematic Survey. *Sensors*, *18*(8). https://doi.org/10.3390/s18082575

PBV, R. R., Sonaleo Mandapati, V., Pilli, S. L., Lahari Manojna, P., Chandana, T. H., & Hemalatha, V. (2024). Home Security with IOT and ESP32 Cam—AI Thinker Module. *2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS)*, 710–714. https://doi.org/10.1109/ICC-ROBINS60238.2024.10533960

Praneeth, D., Rekha Sree, T., Viswanatha, V., & Abhiram Sai, M. (2024). AI Enabled Home Security System Using Object Detection and Face Recognition with Haar Cascade Algorithm. *2024 International Conference on Recent Advances in Science and Engineering Technology (ICRASET)*, 1–6. https://doi.org/10.1109/ICRASET63057.2024.10895751

Quiñones, M. F., Pachar Bravo, H. P., Martínez-Curipoma, J., Quiñones, L., & Torres, R. (2020). Developing and evaluation of an IoT mobile gateway for 4G LTE networks. *Enfoque UTE*, *11*(4), 16–26. https://doi.org/10.29019/enfoqueute.v11n4.634

R. S, N., Venkatasamy, R., Dhanraj, J. A., Aravinth, S., Balachandar, K., & N, Dhamodharan. (2022). Design and Development of IOT based Smart Door Lock System. *2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT)*, 1525–1528. https://doi.org/10.1109/ICICICT54557.2022.9917767

Shreya, K., Divakarla, L. P., Kumar, K. J., & Vishwas, H. N. (2024). Fortifying Digital Security: A Machine Learning and Explainable AI Framework for Password Strength Assessment. *2024 8th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, 1358–1364. https://doi.org/10.1109/ICECA63461.2024.10800823

Tiwari, S., Thakur, S., Shetty, D., & Pandey, A. (2018). Smart Security: Remotely Controllable Doorlock. *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 979–984. https://doi.org/10.1109/ICICCT.2018.8473161

Uddin, K. M. M., Shahela, S. A., Rahman, N., Mostafiz, R., & Rahman, M. M. (2022). Smart Home

Security Using Facial Authentication and Mobile Application. *International Journal of Wireless and Microwave Technologies (IJWMT)*, *12*(2), 40–50. https://doi.org/10.5815/ijwmt.2022.02.04

Vaishnavi, T., N, N., Archana, T., Murali Kishanlal, M. S., Jayasankar, S., & Rahul, D. (2025). Hybrid Unified AI-Based Biometric Authentication: A Low-Power, High-Security Scheme. *2025 International Conference on Emerging Smart Computing and Informatics (ESCI)*, 1–6. https://doi.org/10.1109/ESCI63694.2025.10987946

Vaishnavi, T., Rekha, N, N., M, D., Giri, P., & Kanan, M. (2024). Unified AI-Based Biometric Authentication: A Low-Power, High-Security Solution. *2024 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*, 1–8. https://doi.org/10.1109/ICSES63760.2024.10910877