International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Biometric Access Control System for Residential Apartments: A Qualitative Inquiry

Janepol G. Ballard[1], Reagan Ricafort[2]

[1,2]AMA University, Quezon City, Philippines
[1]janepol.ballard@ustp.edu.ph
[2]Reagan.ricafort@ama.edu.ph

ABSTRACT

This study explored the development and lived usability of a dual-layer biometric access control system purpose-built for residential apartments in Clarin, Misamis Occidental, Philippines. Adopting a descriptive qualitative design, it foregrounded the perceptions, practices, and concerns of apartment owners, landlords, and renters who interacted with the artifact during field deployment. Data were generated through semi-structured interviews, participant observation, and review of system logs, then examined using framework-guided thematic analysis with the ISO/IEC 25010 quality model as an a priori lens. Five interlocking themes emerged: confidence in dual-factor authentication, relief of keyless living, value of timely payment reminders, friction from environmental and power dependencies, and aspirations for resilient solar-backed operation. Findings affirm the social acceptability and contextual fit of integrated biometric security for low- to mid-income residential settings while surfacing design tensions that condition sustained adoption.

KEYWORDS: Access control system, Thumbprint authentication, Facial recognition, Qualitative inquiry, Residential security.

1. INTRODUCTION

Across the urbanizing provinces of the Philippines, the residential apartment has become the default unit of shelter for families, students and migrant workers who are priced out of detached housing yet unwilling to compromise on safety. Rapid population growth and the steady concentration of livelihood in town centres such as Clarin, Misamis Occidental, have multiplied the number of multi-tenant dwellings while leaving the question of who may pass through a door largely unanswered. In many of these complexes, access is still governed by mechanical locks, duplicated keys and the informal vigilance of a landlord who happens to be at home. Such arrangements are brittle: keys are lost, copied or surrendered when tenancies change, and a single compromised lock can expose every occupant on a corridor. The escalating demand for secure and convenient residential living therefore exposes a widening gap between the protection that tenants expect and the protection that legacy hardware can deliver.

Biometric technology has emerged as a credible response to this gap because it binds the right of entry to the person rather than to a transferable token. Fingerprint and facial recognition replace keys and cards that are easily duplicated or stolen with traits that are difficult to forge and impossible to misplace, offering personalized and tamper-resistant access for apartment occupants [1]. The maturation of inexpensive sensors, single-board computers and cellular messaging modules has, for the first time, placed this class

of protection within reach of property owners who operate at modest scale. Foundational treatments of biometric recognition establish that identification systems succeed or fail not only on algorithmic accuracy but on enrolment quality, environmental robustness and user acceptance [2], a triad that becomes especially consequential when the users are ordinary renters rather than trained operators.

Yet the existing body of deployed systems remains uneven. Much of the early residential and institutional work concentrated on a single function. Investigations of biometric authentication in academic settings demonstrated reliable identity verification but confined themselves to attendance tracking rather than comprehensive premises security [3], [4]. Case studies in apartment complexes confirmed the promise of biometric entry and its usefulness for parental oversight, yet repeatedly noted the absence of integrated notification and an intuitive management interface [5], [6]. Parallel work on dormitory and tenancy management underscored that alert mechanisms such as Short Message Service (SMS) are decisive for security transparency, not peripheral conveniences [7]. Studies of facial and fingerprint locks affirmed that biometric verification substantially reduces unauthorized entry [8], while machine-learning and Internet-of-Things (IoT) integrations improved responsiveness and scalability [9], [10]. These advances, however, were frequently calibrated for institutional or commercial deployment and proved impractical for widespread residential use in low- to mid-income communities, where cost-efficiency and user-oriented design are not optional refinements but conditions of survival [11], [12].

A more specific shortfall concerns integration. IoT applications such as child-safety monitoring illustrate how real-time observation can reassure parents and guardians [13], and broad surveys of biometric authentication catalogue the security and convenience such systems afford [14]. Even so, residential implementations seldom unite biometric entry, parental alerts and centralized monitoring in a single coherent platform; functions that ought to reinforce one another are instead scattered across disconnected devices. A notable gap in the literature is therefore the limited fusion of biometric security with notification and monitoring tools purpose-built for the residential apartment, where usability, affordability and deployment constraints are paramount [15]. The present study addresses this shortfall by developing a unified system that pairs fingerprint authentication at room doors with facial recognition at the main gate, layers SMS notification for both security events and rent reminders, and exposes a web-based dashboard for residents and administrators alike.

Where most prior evaluations reach for numerical scoring, this inquiry deliberately turns toward meaning. The decisive questions in a residential setting are not only whether a sensor matches a print within a tolerance, but how a mother feels about her child entering a building unaccompanied, whether a renter trusts a screen instead of a key, and what a landlord does when the power fails during a brownout. Such questions are answered in narrative, not in means. Accordingly, the study adopts a qualitative orientation that privileges the lived experience, situated judgment and voiced concern of the people who actually inhabit the system. Aligned with Sustainable Development Goal 9 on resilient infrastructure and innovation, the research contributes a contextually grounded account of how integrated biometric security is received, resisted and reimagined in a Philippine residential community, and what that reception implies for the broader project of safe, intelligent and equitable urban living.

2. Review of Related Literature

2.1 Biometric Authentication for Residential Security

The literature converges on the proposition that biometric verification raises the floor of residential security by replacing knowledge- and possession-based credentials with the body itself. Reviews of

biometric authentication for residential security argue that fingerprint and facial traits resist the duplication and transfer that undermine keys and cards, and that the resulting accountability, every entry attributable to a specific person, is as valuable as the prevention of intrusion [1]. The canonical account of biometric recognition adds the necessary caution that no modality is flawless: performance is bounded by sensor quality, enrolment care and the variability of real-world capture conditions, so that a system performing admirably in a laboratory may falter in a dim corridor or a humid stairwell [2]. This tension between promise and condition recurs throughout the residential corpus.

Empirical deployments bear this out. Smart locking systems built on facial biometrics report marked reductions in unauthorized access while exposing usability limitations under variable lighting and movement [8]. IoT facial-recognition door systems implemented on Raspberry Pi hardware demonstrate that affordable single-board computers can host serviceable recognition pipelines at the threshold of a home [10], and machine-learning approaches to face recognition for the smart home further improve discrimination between registered and unregistered faces [9]. Case studies situated directly in apartment complexes confirm both the feasibility of biometric entry and its secondary benefit for parental oversight, since a parent can know with confidence that a child has reached home [5]. Reviews of access control across residential complexes nonetheless temper this optimism, observing that many systems remain costly, single-purpose, or poorly matched to the everyday rhythms of tenants and managers [6], [12].

2.2 Notifications, Rent Reminders and Parental Oversight

A second strand of scholarship insists that security is incomplete without communication. A system that admits the right person but tells no one what has happened forfeits much of its protective value. Work on dormitory management information systems with SMS notification and biometric security shows that timely alerts convert a silent lock into a transparent one, allowing guardians and administrators to act on events as they occur rather than discover them after the fact [7]. The same logic extends from security to tenancy administration. Where rent collection has historically suffered from poor visibility and inconsistent reminders, automated SMS prompts about due dates improve resident engagement and financial transparency, reducing the friction and awkwardness that attend face-to-face collection. The integration of biometric monitoring with child-safety assurance, demonstrated in IoT-based monitoring systems, extends notification into the affective register of parental peace of mind [13]. Taken together, these studies reframe notification not as an accessory but as the connective tissue that makes biometric infrastructure socially legible.

2.3 Synthesis and the Research Gap

Read as a whole, the literature documents three durable achievements and one persistent omission. It establishes that biometric entry reliably reduces unauthorized access [8]; that affordable hardware can support recognition at the residential threshold [10]; and that SMS notification is essential to security transparency and tenancy management [7]. The omission concerns synthesis. Cloud-based and intelligent access systems for apartment complexes tend toward institutional scale and cost [11], surveys of biometric systems remain general rather than residential [14], and apartment case studies, while valuable, seldom unite entry control, parental alerting and centralized monitoring within one affordable, user-centered platform [15]. Few systems are purpose-built for the residential apartment of a developing region, where the binding constraints are not algorithmic sophistication but power stability, environmental robustness, cost and the patience of non-expert users. It is precisely this integrative and contextual gap, and the qualitative experience of inhabiting a system designed to close it, that the present study addresses.

3. Objectives of the Study

Guided by a qualitative orientation toward experience and meaning, the study pursued three objectives. First, it sought to understand how residents, owners and landlords experienced the effectiveness of existing apartment access arrangements in preventing unauthorized entry and securing occupants, and where those arrangements were felt to fail. Second, it set out to develop and deploy an integrated, secure biometric access control system designed specifically for residential apartments in Clarin, Misamis Occidental, combining fingerprint authentication at room doors with facial recognition at the main gate. Third, it aimed to explore how stakeholders perceived this dual-layer system in everyday use, including their accounts of its real-time SMS notifications for access events and payment reminders, and to surface the concerns, frictions and aspirations that would condition its broader adoption.

4. Methodology

4.1 Research Design

The study employed a descriptive qualitative design embedded within a developmental research effort. The developmental component produced the artifact: using the Agile Software Development Life Cycle, the system was elaborated through iterative cycles of requirements elicitation, prototyping, deployment and refinement, so that field feedback continually reshaped the build rather than arriving only after completion. The qualitative component governed the evaluation. Rather than reduce user response to numerical averages, the study treated stakeholders as knowledgeable informants whose narratives, practices and concerns constitute the primary evidence of how the system performs in situ. Analysis followed reflexive thematic analysis [17], complemented by a directed, framework-guided reading [18] in which the ISO/IEC 25010 system and software quality model [16] supplied an a priori set of analytic categories, namely functional suitability, interaction capability, performance efficiency, usability, reliability and security. This pairing allowed the study to remain open to themes that participants raised unprompted while ensuring systematic coverage of the recognized dimensions of software quality.

4.2 Research Locale and Participants

Fieldwork was conducted in a residential apartment setting in Clarin, Misamis Occidental, Philippines, a locale selected for its growing demand for improved residential security and its representativeness of the low- to mid-income complexes for which the system was intended. Participants were recruited through purposive sampling, the appropriate strategy when the aim is depth of insight from those with direct, relevant experience rather than statistical representativeness. The sample comprised three stakeholder groups whose vantage points differ instructively: apartment owners, who carry investment and liability; landlords, who manage day-to-day operations and rent collection; and renters, who live with the system most intimately. Each participant had first-hand interaction with the technology during its testing and deployment, ensuring that accounts were grounded in use rather than speculation. Demographic profiles were recorded but held separately to preserve confidentiality, in keeping with the sensitivity of biometric and tenancy data.

4.3 Data-Gathering Procedure

Data generation was woven into the deployment itself. Before the trial, participants attended an orientation in which the system's core features, fingerprint scanning at room doors, facial recognition at the gate, SMS notification and the web dashboard, were introduced and demonstrated, and informed consent was secured. During live operation, three complementary techniques were used. Semi-structured interviews, organized around open-ended prompts, invited participants to narrate their experiences of enrolment, daily

entry, notification and any difficulties encountered. Participant observation captured behavior that interviews cannot reach, such as hesitation at a sensor, the improvised use of a phone flashlight in dim light, or the relief of a successful gate match. Review of system artifacts, including access logs and records of recognition attempts, provided a documentary trail against which spoken accounts could be cross-checked. Observational notes were taken contemporaneously to preserve the texture of real-time interaction.

4.4 Instruments

The principal instrument was a researcher-developed interview and observation guide structured around the six ISO/IEC 25010 quality characteristics, which served less as a scoring rubric than as a conversational scaffold ensuring that each dimension of quality was addressed while leaving room for unanticipated concerns. Open-ended items probed how the system met expectations, how intuitive its interface felt, how quickly it responded, how dependable it proved across repeated use, and how secure participants believed their data and premises to be. The guide was paired with an observation protocol that directed attention to capture conditions, recovery from failed attempts, and the spontaneous workarounds users devised. Because the instrument was developed specifically for this study and a formal pilot validation was not separately conducted, trustworthiness was pursued through the procedural safeguards described below rather than through psychometric calibration.

4.5 Data Analysis

Transcribed interviews, observational notes, and log excerpts were analyzed through the six phases of thematic analysis: familiarization through repeated reading; generation of initial codes; collation of codes into candidate themes; review of themes against the full data set; definition and naming of themes; and the production of the analytic narrative reported here [17]. The ISO/IEC 25010 dimensions functioned as deductive anchor codes within a framework matrix, while inductive codes were admitted freely so that participant-driven concerns, most notably power dependency and environmental sensitivity, could rise to thematic prominence even though they cut across several quality categories [18]. Coding proceeded manually to keep the analyst close to the data, and the resulting themes were refined iteratively until they offered a coherent and faithful account of the corpus.

4.6 Trustworthiness of the Inquiry

Rigour was established against the four criteria for naturalistic inquiry [19]. Credibility was supported by triangulating interviews, observation and system logs, so that claims rested on convergent evidence rather than a single source, and by member-checking key interpretations with participants during the deployment. Transferability was served by thick description of the locale, the participants and the system, enabling readers to judge the applicability of findings to comparable residential settings. Dependability was pursued through a documented audit trail of design decisions, coding choices and analytic moves, consistent with the procedural transparency expected of qualitative research [20]. Confirmability was protected by grounding every theme in concrete data extracts and by reflexive attention to the researchers' dual role as system developers, a position that lends technical insight but demands vigilance against advocacy.

4.7 Ethical Considerations

Participation was voluntary and predicated on informed consent obtained before involvement. Given that the system processes fingerprint, facial and tenancy data, the study adhered strictly to confidentiality and data-protection standards: biometric templates and personal information were handled as sensitive, access to records was restricted, and demographic identifiers were stored apart from interview data. Participants were assured that they could withdraw at any time without consequence, and the evaluation was conducted

in accordance with recognized ethical guidelines for research involving human participants.

4.8 Scope and Delimitation

The inquiry concerns the development and qualitative evaluation of a biometric access control system for residential apartments in Clarin, Misamis Occidental, designed for small- to medium-scale settings. The system provides dual-layer authentication through facial recognition and fingerprint scanning together with SMS notification for rent reminders and access events. Its benefits are conditioned by recognized limitations: reliance on stable electrical power, the possibility of biometric inaccuracies under adverse physical or environmental conditions, and comparatively higher initial hardware costs. The system is not intended for large-scale deployment without further adaptation, and it requires ongoing maintenance to sustain performance and user satisfaction. The study makes no claim to statistical generalizability; its contribution is the depth and contextual fidelity characteristic of qualitative research.

5. The Developed System: Design and Architecture

Before turning to participant experience, it is necessary to describe the artifact that occasioned it, since the meanings stakeholders made were inseparable from the concrete devices they encountered. The system is organized as two cooperating subsystems, one governing room doors and one governing the main gate, unified by a shared notification channel and a web-based management interface.

5.1 Door Entrance with Thumbprint Access

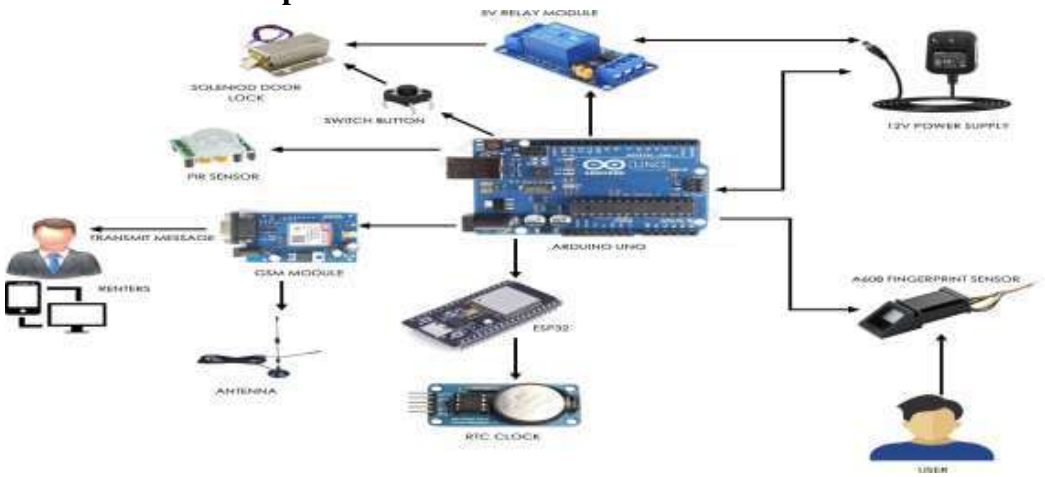

Figure 1. Door entrance with thumbprint access.

Figure 1 illustrates the architecture of the biometric access control installed at the room door. The subsystem is built on an Arduino Uno microcontroller that coordinates a set of sensors and modules. An A608 fingerprint sensor serves as the primary means of authentication, admitting only registered users by actuating a solenoid door lock through a 5V relay module powered from a 12V supply. A passive infra-red (PIR) sensor detects motion at the premises and allows the lock to remain disengaged for legitimate movement, while a manual switch button provides a backup means of release. A real-time clock (RTC) module timestamps each access for the log, and an ESP32 module furnishes Wi-Fi connectivity for data exchange. A GSM module with antenna transmits alert messages to renters' mobile devices, including real-time notifications of payment due dates. In combination, these components translate a verified fingerprint into a physical act of admission while leaving an auditable trace of every entry.

5.2 Gate Entrance with Facial Recognition

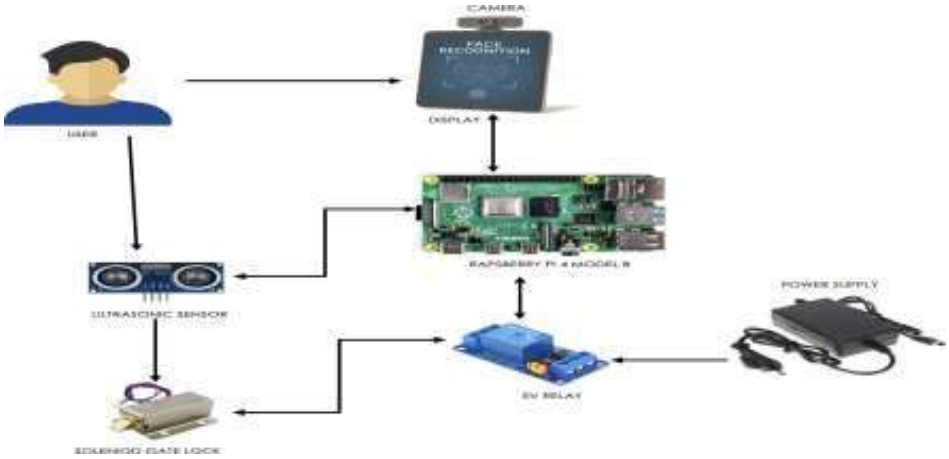

Figure 2. Gate entrance with facial recognition.

Figure 2 depicts the facial-recognition gate lock, which uses a Raspberry Pi 4 Model B as its central processing unit. A camera captures the approaching user's face, and a recognition routine analyses facial features, the configuration of the eyes, nose, and overall facial structure, to authenticate the individual against the registered dataset, displaying the outcome on a screen. Upon successful verification, the Raspberry Pi energizes a 5V relay module that drives a solenoid gate lock, granting entry. An ultrasonic sensor detects a user's presence from the interior to release the gate for exit, so that leaving the premises requires no biometric interaction. This division of labour, fingerprints for the intimate space of the room and faces for the shared threshold of the gate, matches each modality to the social character of the boundary it guards.

5.3 Operational Logic of Dual-Layer Access

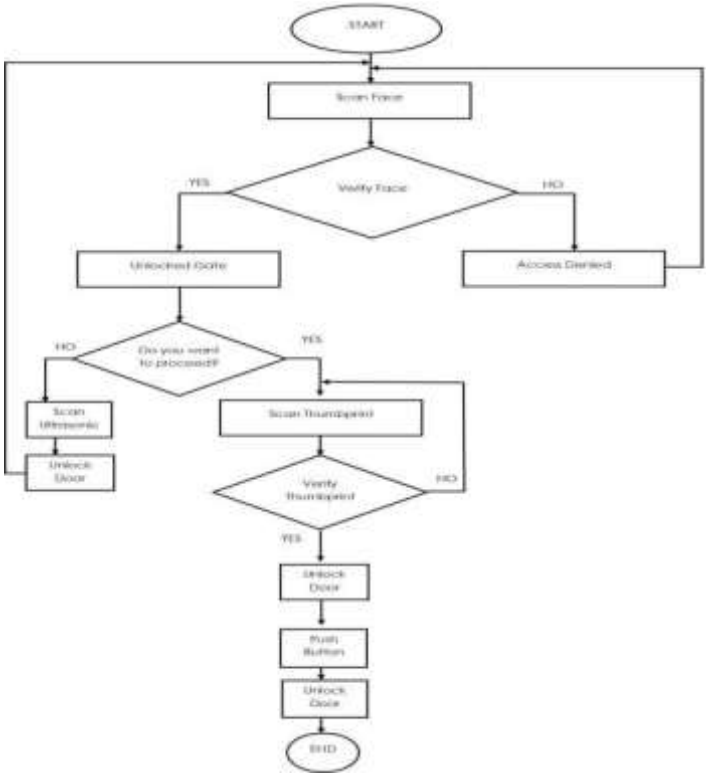

Figure 3. Face- and thumbprint-based access control flowchart.

Figure 3 traces the operational logic that binds the two subsystems. The process begins by capturing a user's biometric data and proceeds to a verification step that checks whether the face or thumbprint is registered. A successful match unlocks the relevant barrier and grants access; an unmatched attempt is denied, and the barrier remains secured. The flowchart also accommodates egress: a user leaving through the gate or door may trigger release by the ultrasonic sensor or the manual button, so that exit is never impeded by a failed scan. This design enforces secure and intentional entry while preserving freedom of movement outward, and it supports continuous operation for multiple users in sequence, an essential property in a multi-tenant building where several residents may arrive within minutes of one another.

5.4 Management Interface

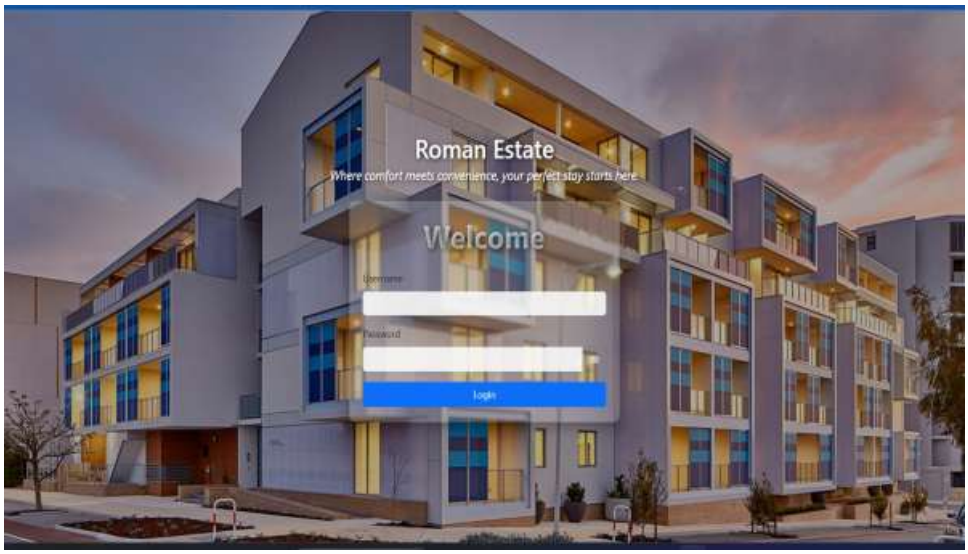

Figure 4. Login page of the biometric access control system for residential apartments.

Figure 4 presents the login page of the management application, branded for the apartment complex as "Roman Estate." Both renters and administrators authenticate here, with the interface distinguishing the privileges available to each role. The page exemplifies the study's commitment to a user-friendly front end, a feature whose absence earlier scholarship identified as a recurrent weakness of residential biometric systems.

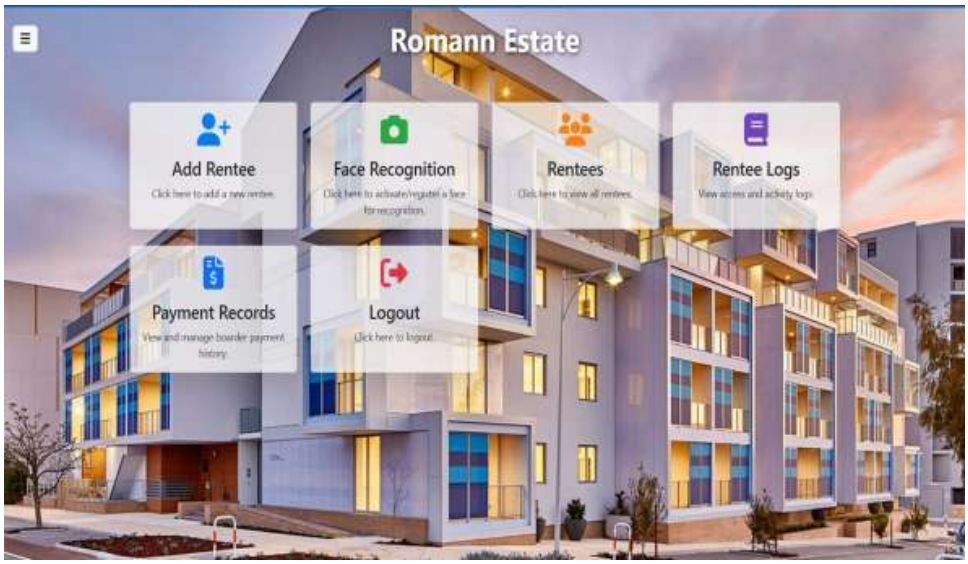

Figure 5. Administrator dashboard page.

Figure 5 shows the administrator dashboard of the "Romann Estate" management system, designed for efficient oversight of renters. From this console, an administrator can register fingerprint and facial recognition data, add new renters, monitor payment records, and track entry and exit logs in real time, consolidating the functions that prior systems left dispersed into a single pane. Renters, by contrast, are granted a constrained view limited to their own payment history and access logs. This asymmetry of capability operationalizes the principle that monitoring power should be proportionate to responsibility, granting landlords the visibility they require while preserving a measure of informational dignity for tenants.

6. Results and Discussion

The qualitative evidence was organized using the ISO/IEC 25010 framework, whose six characteristics served as deductive anchors for coding, while inductive themes were admitted wherever participants insisted on them. Table 1 sets out the framework as it was applied, pairing each characteristic with the guiding concern that directed attention during interviews and observation. The themes that follow are reported against this scaffold, and a thematic synthesis is consolidated in Table 2.

Table 1. ISO/IEC 25010 characteristics as the deductive coding framework.

Quality characteristic	Guiding analytic concern
Functional suitability	Whether the system delivered the entry, notification and monitoring functions stakeholders expected.
Interaction capability	How intuitive and learnable the enrolment, scanning and dashboard interactions felt in practice.
Performance efficiency	How quickly and smoothly the system responded during entry, peaks and notification delivery.
Usability	How much effort daily use demanded and whether the system reduced or added burden.
Reliability	How dependable operation proved across repeated use, and how failures were experienced and recovered.
Security	How protected participants believed their premises and personal data to be against unauthorized access.

6.1 Confidence in Dual-Factor Authentication

Security was the dimension participants spoke of with the greatest conviction, and it anchored the most prominent theme. Stakeholders consistently described a heightened sense of protection arising from the pairing of two independent modalities at two distinct boundaries, a face at the gate and a fingerprint at the door, so that an intruder would need to defeat not one safeguard but two of different kinds. Owners and landlords valued the accountability this produced: because each admission was attributable to a registered identity and timestamped in the log, the question of who had entered, and when, ceased to be a matter of conjecture. Renters, for their part, expressed relief that entry no longer depended on a key that could be copied or a card that could be lent. This confidence in robust, tamper-resistant protection is consistent with

the security and privacy assurances biometric systems are designed to provide [22] and with the reduction in unauthorized access reported across the deployment literature [8]. It also fulfills the functional expectation that the system would reliably deliver its core feature, dual-layer authentication, a finding that echoes earlier intelligent access work [11].

6.2 The Relief of Keyless Living

If security was the dimension of greatest conviction, usability was the dimension of greatest warmth. A clear theme of relief ran through accounts of keyless living. Participants described the elimination of physical keys as an unburdening: no more fumbling at a dark door, no more anxiety over a lost or stolen key, no more cost of rekeying when a tenant departed. The interaction was experienced as intuitive: after orientation, residents reported that presenting a finger or facing a camera required little learning and quickly became habitual. The ease of monitoring entry through the web dashboard and mobile access logs was singled out as a particular convenience, allowing residents to confirm activity at a glance. These accounts align with established usability principles, which hold that a system's value is realized only when its operation is learnable and low in cognitive load [21], and they answer directly the criticism that residential biometric systems too often neglect the intuitive interface on which acceptance depends [6].

6.3 Timely Notifications and Financial Transparency

A third theme centred on the SMS notification channel, which participants treated not as a technical flourish but as a meaningful improvement in the social conduct of tenancy. Renters welcomed timely reminders of payment due dates, describing them as a courtesy that helped them plan and spared them the embarrassment of a missed deadline; landlords valued the same prompts for the financial transparency and reduced friction they brought to rent collection, which had previously depended on awkward in-person reminders. Beyond rent, the prospect of real-time alerts for access events was read through the lens of family care, with parents associating notification with the assurance that a child had safely reached home. This convergence of financial and affective value reflects the literature's insistence that notification is constitutive of, rather than incidental to, residential security and management [7], and that monitoring integrated with safety assurance speaks to the concerns of guardians [13]. In participants' accounts, the message that arrives is what makes the silent lock trustworthy.

6.4 Performance and Reliability in Everyday Use

Performance efficiency drew broadly favorable accounts: participants characterized the system as responsive during entry and stable during periods of concentrated use, when several residents arrived in close succession, a smoothness consistent with assessments of well-implemented biometric systems' responsiveness [23]. Reliability, however, was the dimension where appreciation was most qualified, and here an inductive theme surfaced that the framework had not anticipated in full. While participants judged the system dependable in normal operation, they reported occasional inconsistencies, most concretely a delay during fingerprint registration and a dependence on the network for remote features. These frictions did not negate confidence, but they tempered it, and they map onto long-standing observations about the reliability and availability of biometric authentication under real-world conditions [24]. That the principal reliability concerns clustered around enrolment latency and connectivity, rather than around false acceptance, is itself instructive: for these users, dependability was less a question of whether the system would admit the wrong person than of whether it would admit the right one promptly and without recourse to the manual override.

6.5 System Behaviour under Varied Real-World Conditions

Observation of the facial-recognition subsystem during field testing furnished a documentary complement

to participants' accounts, recording how the system behaved as capture conditions varied. Table 2 summarises these observations. With a consistent capture delay of about two seconds, the system authorized registered users across a range of conditions, performing best when the subject was centred under good lighting and degrading gracefully, though not collapsing, under shadow, dim light and partial occlusion by a face mask, where recognition succeeded once full facial features became visible. Critically, the system correctly rejected an unregistered individual, returning no match and denying access, which participants read as direct evidence that the safeguard functioned as promised. The observation that recognition quality tracked lighting and facial visibility corroborated the most frequently voiced reservation in the interviews and foreshadowed the final theme. A hardware ceiling was also noted: image storage was bounded by the device's memory capacity, a reminder that the artifact's robustness is conditioned by its physical substrate.

Table 2. Observed behaviour of the facial-recognition subsystem under varied conditions.

Observed condition	Subject status	Authorization	Field note
Subject centred under good lighting across repeated attempts	Known	Authorized	Ideal capture conditions; no issues observed
Shadow present on one side of the face	Known	Authorized	Matched correctly despite uneven illumination
Dim ambient light; subject used a phone flashlight	Known	Authorized	Recognition passed after improvised illumination
Face partially occluded by a mask	Known	Authorized	Failed initially; succeeded once full features were visible
Unregistered individual attempted recognition	Unknown	Unauthorized	Correctly rejected; no match returned
Image storage bounded by device memory capacity	—	—	Volume of stored captures limited by hardware

6.6 Environmental and Power Dependencies

The most insistent inductive theme, voiced by participants and confirmed by observation, concerned the system's dependence on favourable environmental and electrical conditions. Two vulnerabilities dominated. The first was lighting: facial recognition, however graceful its degradation, performed less confidently in dim or shadowed conditions, prompting the improvised use of a phone flashlight that participants tolerated but did not welcome. The second, and more consequential, was power: in a setting where brownouts are a fact of life, participants worried that a loss of electricity would disable the very threshold meant to protect them. These concerns are not incidental to the system but structural, arising from the same hardware that makes affordable biometric protection possible. They cohere with the foundational caution that biometric performance is bounded by capture conditions [2] and with the

recognized limitation that such systems depend on stable power and are sensitive to environmental factors. Significantly, participants did not treat these frictions as grounds for rejection; they treated them as problems to be engineered around, and their suggestions, solar integration and extended battery backup to preserve function during outages, were offered in the spirit of co-design rather than complaint.

6.7 Thematic Synthesis

Table 2 above and Table 3 below together consolidate the analysis. Read across the framework, the findings describe a system that is socially acceptable and contextually apposite, earning genuine confidence in its security and warmth toward its convenience, yet conditioned by reliability and environmental dependencies that residents are willing to live with only insofar as they can be mitigated. The overall pattern affirms the system's viability as a practical and user-accepted solution for residential access control while locating the frontier of its improvement precisely where participants placed it: at the meeting point of power and light.

Table 3. Thematic synthesis across the ISO/IEC 25010 framework.

Quality dimension	Core theme	Representative stakeholder concern
Security; functional suitability	Confidence in dual-factor authentication	Two safeguards at two boundaries; accountable, attributable entry
Usability; interaction capability	The relief of keyless living	No lost keys, no rekeying; intuitive scanning and at-a-glance logs
Functional suitability	Timely notifications and financial transparency	Rent reminders ease collection; alerts assure parental peace of mind
Performance efficiency; reliability	Performance and reliability in everyday use	Responsive in peaks, but enrolment delay and network dependence
Reliability (cross-cutting)	Environmental and power dependencies	Dim-light recognition and brownouts; calls for solar and backup

Considered against the literature, the findings are broadly consistent with prior work yet contribute a distinct insight. By uniting biometric entry, parental and rent notification, and centralized monitoring in a single residential platform, and by examining that platform through the eyes of those who lived with it, the study advances the integrative agenda that earlier residential case studies and IoT monitoring research called for but seldom realized [5], [13]. The qualitative lens, moreover, recovers something the numerical literature tends to lose: that the decisive determinants of acceptance in a low- to mid-income community are not marginal gains in match accuracy but the felt experience of relief, transparency and trust, set against the lived anxiety of an outage. The system proved, in participants' own framing, technically sound, socially acceptable and adaptable to real residential conditions.

7. Conclusions

Examined qualitatively, the biometric access control system addressed the functional, usability, performance and security needs of residential apartments in a manner its stakeholders found credible and welcome. Functionally, it delivered the dual-layer authentication and SMS notification it promised, meeting user expectations in a way that resonates with prior intelligent access work [11]. Its interaction

and usability were experienced as intuitive and low in effort, consistent with established usability principles [21], while its performance was judged responsive even under concentrated use [23]. Reliability, though sound in ordinary operation, revealed the system's frontier: fingerprint enrolment delay and network dependence, in keeping with long-noted concerns about biometric availability [24]. Security drew the firmest confidence, with participants crediting the system with strong protection of premises and data and accurate exclusion of unauthorized persons, as the foundational security literature would predict [22], [1]. Above all, the study demonstrates that the meaning residents assign to such a system, the relief of keyless living, the transparency of timely reminders, the reassurance of attributable entry, and the anxiety of dependence on power and light, is itself decisive evidence of fit, and that integrated biometric security is both viable and contextually apposite for Philippine residential communities.

8. Recommendations

The findings translate into a clear agenda for refinement and further study, much of it voiced by participants themselves. First, facial-recognition performance in low-light conditions should be strengthened, whether through improved illumination at the gate, infra-red-capable capture, or algorithms tuned for adverse lighting, so that residents need not improvise with phone flashlights. Second, the system's resilience to power interruption should be hardened through solar integration and extended battery backup, directly answering the most consequential anxiety surfaced in this study and ensuring that protection persists through the brownouts that punctuate provincial life. Third, future research should examine the system across diverse and multi-site residential settings to test the transferability of these qualitative insights and to observe how meaning and acceptance shift with context. Together these directions would carry the artifact from a promising, well-received prototype toward a dependable fixture of safe, sustainable and intelligent residential infrastructure.

Acknowledgements

The authors gratefully acknowledge the apartment owners, landlords and renters of Clarin, Misamis Occidental, whose generous participation made this inquiry possible, and the institution that supported the development and field deployment of the system.

References

1. A. Yadav, S. Sharma and V. Singh, “Biometric Authentication for Residential Security: A Review of Advantages and Challenges,” International Journal of Computer Applications, vol. 182, no. 19, pp. 22–27, 2020.
2. A. K. Jain, A. Ross and S. Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004.
3. M. Hadžimehanović, D. Kečo and D. Korać, “Biometrics-Based Access Control System,” International Burch University Repository, Sarajevo, Bosnia and Herzegovina, 2020. [Online]. Available: https://omeka.ibu.edu.ba/items/show/3454.
4. M. Rahman, K. Rumman, R. Ahmmed, A. Rahman and A. Sarker, “Fingerprint-Based Biometric Attendance System,” European Chemical Bulletin, vol. 12, no. S3, pp. 184–190, 2023.
5. R. A. Baysa and J. P. Cruz, “Biometric-Based Access Control System in a Residential Apartment Complex: A Case Study,” International Journal of Engineering and Technology Innovation, vol. 11, no. 2, pp. 108–118, 2021.

6. J. Bautista, E. Tan and R. Lim, "Access Control Systems in Residential Apartment Complexes: A Review," Smart Cities, vol. 5, no. 2, pp. 612–628, 2022.
7. S. M. Fernandez, "Dormitory Management Information System with SMS Notification and Biometric Security," Indian Journal of Science and Technology, vol. 15, no. 26, pp. 1296–1305, 2022.
8. N. Y. L. Venkata, Ch. Rupa, B. Dharmika, T. G. Nithin and N. Vineela, "Intelligent Secure Smart Locking System Using Face Biometrics," in Proc. IEEE Int. Conf. on Recent Trends in Electronics, Information and Communication Technology (RTEICT), 2021.
9. M. Alshar'e, M. Rustom, R. Kumar, M. Sharma, Dharamvir and V. Tripathi, "A Face Recognition Method in Machine Learning (ML) for Enhancing Security in Smart Home," in Proc. 2nd Int. Conf. on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022.
10. S. A. Radzi, M. K. M. F. Alif, Y. N. Athirah, A. S. Jaafar, A. H. Norihan and M. S. Saleha, "IoT-Based Facial Recognition Door Access Control Home Security System Using Raspberry Pi," International Journal of Power Electronics and Drive Systems, vol. 11, no. 1, pp. 417–424, 2020.
11. A. Mercado, J. Orial and R. Santos, "Cloud-Based Intelligent Access Control System for Apartment Complexes," International Journal of Advanced Computer Science and Applications, vol. 12, no. 5, pp. 320–326, 2021.
12. J. A. Rodrigues, "Access Control in Residential Complexes," Medium, 2 May 2024. [Online]. Available: https://medium.com/@joven.a.rodrigues/benefits-of-access-control-systems-in-residential-complexes-00930b76f5b4.
13. M. Ramachandran, S. Spoorthi and C. Raja, "A Review on Child Safety Monitoring System Based on IoT," REST Journal on Emerging Trends in Modelling and Manufacturing, vol. 4, no. 2, 2023.
14. T. Das, A. Harshey, V. Mishra and A. Srivastava, "An Introduction to Biometric Authentication Systems," in Textbook of Forensic Science, pp. 805–839, Springer, 2023.
15. H. Zhang and Q. Wang, "Implementing Biometric Access Control Systems in Residential Apartments: A Case Study," Journal of Construction Engineering and Management, vol. 146, no. 4, 04019105, 2020.
16. ISO/IEC, ISO/IEC 25010:2011 — Systems and Software Engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — System and Software Quality Models, International Organization for Standardization, 2011.
17. V. Braun and V. Clarke, "Using Thematic Analysis in Psychology," Qualitative Research in Psychology, vol. 3, no. 2, pp. 77–101, 2006.
18. H.-F. Hsieh and S. E. Shannon, "Three Approaches to Qualitative Content Analysis," Qualitative Health Research, vol. 15, no. 9, pp. 1277–1288, 2005.
19. Y. S. Lincoln and E. G. Guba, Naturalistic Inquiry. Beverly Hills, CA: Sage, 1985.
20. J. W. Creswell and C. N. Poth, Qualitative Inquiry and Research Design: Choosing Among Five Approaches, 4th ed. Thousand Oaks, CA: Sage, 2018.
21. J. Nielsen, "Heuristic Evaluation," in Usability Inspection Methods, J. Nielsen and R. L. Mack, Eds. New York: John Wiley & Sons, 1994, pp. 25–62.
22. A. K. Das and M. S. Hossain, "Security and Privacy in Biometric Authentication Systems," Journal of Cyber Security and Information Systems, vol. 3, no. 2, pp. 34–43, 2015.
23. N. Kumar, A. Saxena and V. Gupta, "Performance Evaluation of Biometric Authentication Systems," International Journal of Biometrics, vol. 2, no. 2, pp. 143–155, 2010.
24. T. Kwon, J. Lee and J. Kim, "An Analysis of Reliability and Availability of Biometric Authentication

Systems," in Proc. Int. Conf. on Information Security and Cryptology (ICISC), pp. 133–144, 2002.