

RFID-based cadet access management system with face recognition and cctv integration

Azzam Amar Ma'ruf¹, Muhammad Azhar Prabukusumo², Eryan Ahmad Firdaus³

^{1,2,3} Department of Informatics, Faculty of Defense Engineering and Technology, Indonesia Defense University, Bogor, Indonesia

Article Info

Article history:

Received Aug 28, 2026

Revised Sep 20, 2026

Accepted Sep 25, 2026

Keywords:

Access Control

Audit Trail

CCTV

Face Recognition

RFID

ABSTRACT

Access control in a military campus environment demands records that are accurate, fast, and difficult to falsify, yet manual logbook recording at Unhan RI remained prone to error and identity fraud. This study designed and built SAKTI, a web-based integrated security access system whose novelty lies in unifying three components within a single transaction flow: RFID for initial identification, face recognition for biometric authentication, and event-based CCTV capture as tamper-proof visual evidence. Unlike prior dual-factor systems, this unified pipeline produces a real-time digital audit trail that links every access decision to a captured identity image and a centralised presence record. The system was developed using Rapid Application Development with a Laravel-MySQL backend and a Python worker for face verification and RTSP snapshot retrieval. Testing on fifty cadets achieved a hundred percent verification success rate, reduced processing time by 77.8 percent, and earned very good scores in User Acceptance Testing from both security personnel and cadets. SAKTI demonstrates a practical and scalable approach to enhancing physical security management, real-time identity verification, and forensic audit trail generation in military campus environments.

This is an open access article under the [CC BY-NC](https://creativecommons.org/licenses/by-nc/4.0/) license.



Corresponding Author:

Azzam Amar Ma'ruf,
Department of Informatics, Faculty of Defense Engineering and Technology,
Indonesia Defense University,
IPSC Sentul Area, Bogor 16810, West Java, Indonesia.
Email: azzammaruf7@gmail.com

Introduction

Digital transformation and the Society 5.0 concept have driven higher education institutions worldwide to adopt Internet of Things (IoT) technology toward building smart campus ecosystems (Shihao et al., 2025). While smart campus initiatives have advanced academic service efficiency and resource management considerably (Eltamaly et al., 2021), the physical security dimension has received comparatively less systematic attention (Min-allah & Alrashed, 2020). Digitally governed campuses generate dense, high-frequency mobility of personnel across restricted areas, creating operational demands that manual oversight can no longer meet (Dake et al., 2023). In military higher education settings, where discipline and traceability of personnel movement are institutional requirements, this gap between digital governance aspirations and physical security practices becomes a critical vulnerability.

Prior research has established RFID as the dominant technology for automated access control at building and room entrances (Maulana et al., 2025; Hamidah et al., 2025; Ahmad et al., 2024). RFID

enables contactless, high-throughput identification suited to dense personnel mobility (Ferdousmou et al., 2024). However, a critical limitation shared by these systems is their reliance on a single physical credential: a card that can be lost, stolen, or lent to an unauthorised party without the system detecting the substitution (Mahbub et al., 2025; Erwinda et al., 2022). None of these systems maintains a centralised, real-time record of personnel location, so a compromised card can grant repeated access across multiple points before an incident is noticed.

To address the credential-substitution vulnerability, face recognition has been introduced as a secondary biometric layer (Septyanlie et al., 2024; Adetoyi & Awe, 2022; Lee et al., 2020). Studies combining RFID with facial biometrics report improved resistance to unauthorised entry (Syahfitra et al., 2024; Erwinda et al., 2022). Nevertheless, a common shortcoming in existing dual-factor designs is that the verification outcome granted or denied is recorded as a status code only, with no visual corroboration of the identity claim. This means that a false match, where an unregistered individual is incorrectly granted access, leaves no retrievable evidence for post-incident investigation. Additionally, security evaluations indicate that biometric encoding stored in databases remains exposed to extraction risks if not encrypted at rest (Yeovandi et al., 2025).

Separately, CCTV has been optimised beyond passive monitoring toward event-based capture triggered at access control points (Murdani et al., 2024; Bata, 2023). Linking image capture to authentication events provides a forensic basis for post-incident review (Jutika, 2022; Anggraini et al., 2021). However, existing implementations treat CCTV as an independent surveillance channel rather than integrating it into the access transaction itself, so the captured image is stored separately from the access log and the identity record. Reconstructing a complete picture of a security event therefore requires manual cross-referencing of three independent data sources: the access log, the identity database, and the camera archive.

The research gap identified in the literature is threefold. First, no existing system combines all three control mechanisms RFID identification, biometric verification, and event-based visual capture within a single atomic transaction that produces one unified audit record. Second, no system reviewed maintains a real-time presence state per user per location, which is the minimum requirement for detecting tailgating or repeated-entry fraud. Third, studies focusing on military or high-security campuses remain sparse in the 2023–2025 window, suggesting that the specific operational constraints of such environments strict chain of custody, mandatory audit trails, and non-negotiable personnel accountability have not been adequately addressed (Badirova et al., 2023; Kumar et al., 2024; Prapsetyo et al., 2023; Yulistya et al., 2023). At Universitas Pertahanan Republik Indonesia (Unhan RI), these gaps manifest operationally: cadet movement across the Kesatrian area and into high-value laboratories is still governed by manual logbook entries, producing data that are inaccurate, unsearchable in real time, and forensically unusable after an incident.

This study addresses those gaps by designing and building SAKTI, an integrated security access system whose principal novelty is the fusion of RFID, face recognition, and event-based CCTV capture into a single indivisible transaction: one card scan triggers one biometric check, one CCTV snapshot, and one unified log entry containing identity, location, direction, timestamp, and visual evidence simultaneously. Unlike prior dual-factor or parallel-channel systems, SAKTI further maintains a per-location presence state for every cadet, enabling real-time anomaly detection without manual cross-referencing. The expected contributions of this work are: (1) a replicable three-layer access architecture suitable for military campus environments; (2) empirical performance benchmarks for dlib ResNet-34 face verification under real operational conditions; and (3) a validated audit trail mechanism that satisfies the forensic traceability requirements of Identity and Access Management principles (Badirova et al., 2023). This study therefore aims to design, implement, and evaluate SAKTI as a web-based cadet identity and mobility management system that optimises verification precision through dual authentication and generates a documentable, real-time audit trail within the Kesatrian area of Unhan RI.

Method

This study employed the Rapid Application Development (RAD) method, which emphasises the rapid

construction of a quality system through a prototyping approach and an iterative process so that conformity with user needs can be ensured from the earliest stage (Hidayat & Hati, 2021). The method was carried out in three phases: requirements planning to establish system objectives and needs, design workshop to design and build the system iteratively with users, and implementation to deploy and test the system in the operational environment. System design was documented using the Unified Modeling Language, covering use case, activity, sequence, and class diagrams (Hasanah & Untari, 2020).

Data were collected through three techniques. Interviews were conducted with the Head of the General Affairs Division and the Security Section Officer of Unhan RI to obtain a picture of the cadet entry-exit recording procedure, personnel strength reporting requirements, and data accuracy problems associated with the movement logbook. Direct observation was carried out at the Kesatrian guard post, the Science Laboratory, and the Computer Laboratory to observe mobility flow, queue potential during peak hours, and identity manipulation vulnerability arising from limited visual inspection. A literature review covered publications from 2020 to 2025 on identity and access management, dual security systems based on RFID and facial biometrics, event-based CCTV capture, and Role-Based Access Control.

The SAKTI system architecture was built in three interconnected layers. The interface and business logic layer was developed using the Laravel framework with the Model-View-Controller pattern, which handles routing, session authentication, and application programming interface provision (Sinlae et al., 2024; Husain et al., 2024), while the responsive presentation was composed using Bootstrap (Perdana & Wijaya, 2024). The storage layer uses a MySQL relational database managed through migration so that the schema can be reproduced consistently (Putri et al., 2023). The device layer consists of a 13.56 MHz USB RFID reader and a 1080p IP camera operating via Real Time Streaming Protocol (RTSP) with infrared night-vision capability, both controlled by a Python worker running continuously in the background. The overall system workflow is presented in Figure 1.

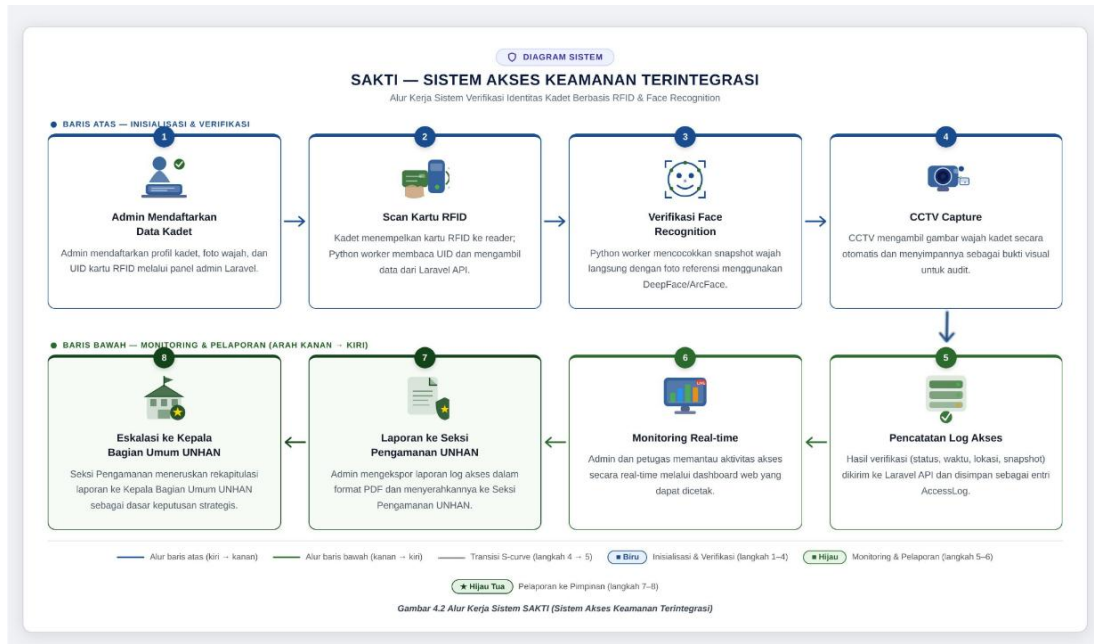


Figure 1. SAKTI system workflow

Every access event is processed through a fixed pipeline: RFID card scanning, cadet data lookup and location permission validation, face verification, CCTV image capture, and log storage. Cadets interact only with physical devices at the control point, while guards and administrators use the web interface. Hardware and software specifications are presented in Table 1.

Table 1. Hardware and software specifications of the system

Component	Specification
Computing device	Intel Core i5 8th generation, 4 GB DDR4 RAM, 128 GB SSD
RFID reader	USB RFID reader 13.56 MHz, HID mode
Surveillance camera	IP camera, RTSP/HTTP snapshot, 1080p resolution, IR night vision
Backend framework	Laravel 10.1 with the MVC pattern
Database system	MySQL 5.7
Interface framework	Bootstrap 5.3
Face verification service	Python with the face recognition library (dlib ResNet-34)
Development server	Laragon 6.0 (Apache, PHP, MySQL)

Face verification used the pre-trained dlib ResNet-34 model through the *face recognition* library, which extracts facial features into a 128-dimensional encoding vector (King, 2009). The extraction process used *num jitters* set to three and the large model producing 68 facial landmark points for greater encoding stability. Prior to deployment, each of the 50 enrolled cadets provided three frontal-face photographs taken under controlled indoor lighting (approximately 300-500 lux, neutral background, no head covering) using the same 1080p IP camera that would later perform live capture. Each photograph was processed individually through the library to generate three encoding vectors per cadet; the mean of these three vectors was stored as the reference encoding in the database, reducing intra-subject variance caused by minor pose or illumination differences during enrollment. Identity matching at runtime calculates the Euclidean distance between the live encoding and the stored reference encoding, as expressed in equation (1), following the same distance-in-embedding-space principle as modern face recognition architectures (Schroff & Philbin, 2015).

$$d(x, y) = \sqrt{\sum_{i=1}^{128} (x_i - y_i)^2} \quad (1)$$

The Euclidean distance threshold was set at 0.38, stricter than the library default of 0.60. This value was determined through a preliminary calibration experiment conducted before the main accuracy test: threshold candidates of 0.30, 0.35, 0.38, 0.42, 0.45, and 0.60 were evaluated on a pilot subset of ten cadets, each verified five times under the same lighting and camera conditions used in the main test. A threshold of 0.38 produced zero false positives while maintaining a 100 percent true acceptance rate on the pilot subset, making it the optimal operating point for this deployment environment. This tighter operating threshold is also consistent with recommendations from face recognition security evaluations that favour stricter thresholds in high-security access scenarios (Yeovandi et al., 2025; Lee et al., 2020). A face is declared matched when the distance falls below 0.38; the system confidence for each match is computed using equation (2), where a smaller distance yields a higher confidence value.

$$\text{conf} = \max\left(0, 0, \min\left(1, 0, 1, 0 - \frac{d}{T \times 2}\right)\right) \quad (2)$$

The main accuracy test was carried out under consistent environmental conditions: indoor controlled lighting of approximately 300-500 lux provided by standard fluorescent ceiling fixtures, a fixed camera-to-subject distance of 60-80 cm, and a neutral wall background. Each of the 50 cadets performed three live verification attempts in sequence; a verification was counted as successful if the system returned a *matched* result in at least two of three attempts. The confidence value recorded for each cadet was the mean of all successful-attempt confidence scores. This three-attempt protocol accounts for natural variation in facial pose and minor lighting fluctuations, yielding a more stable performance estimate than a single-attempt measurement.

System testing was carried out through four schemes. First, *black box testing* to ensure all functions operate according to the designed scenarios without examining internal code structure (Hudi & Karyanti, 2024; Jailani & Ainul, 2024). Second, the face verification accuracy test on 50 cadets as described above, with descriptive statistical analysis (mean, median, mode, minimum, maximum, and standard deviation) applied to the resulting confidence values. Third, a process time comparison between the conventional procedure and SAKTI, measured by timing each stage at the guard post across

ten representative transactions and reporting mean values. Fourth, *User Acceptance Testing* (UAT) to validate that the system meets operational needs (Hermansah et al., 2025; Muhammad et al., 2025).

The UAT involved two respondent groups. The first group comprised six security personnel, namely five post guards and one Security Division Officer, who completed a 25-item questionnaire across four variables: system functionality, system performance, user experience and interface, and efficiency and productivity. The second group comprised 50 cadets as kiosk users, who completed a 17-item questionnaire across functionality, speed and responsiveness, kiosk interface, and user satisfaction. Responses used a five-point Likert scale; scores were aggregated using equations (3) and (4) to produce a weighted mean and a percentage value per variable (Aliyah et al., 2025; Wulandari et al., 2023). A percentage of 81 percent or above was defined as the *very good* threshold, consistent with Likert interpretation norms applied in prior UAT studies (Hermansah et al., 2025).

$$\text{mean} = \frac{\text{assessment weight}}{\text{total number of respondents}} \quad (3)$$

$$\text{Percentage} = \frac{\text{Mean Score}}{\text{Maximum Weight}} \times 100 \quad (4)$$

Results and Analysis

The SAKTI database was implemented in MySQL with seven main interrelated tables supporting access control, user management, log recording, and real-time monitoring of cadet position. The relational structure between tables is presented in Figure 2.

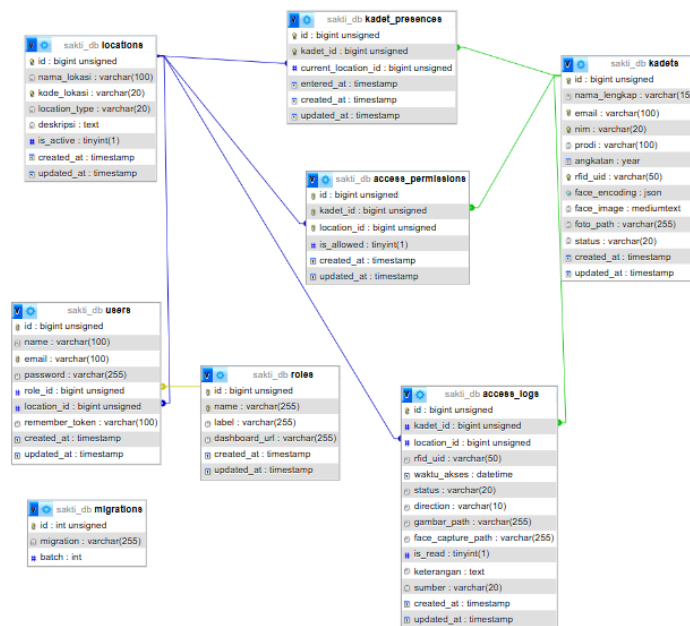


Figure 2. Database implementation of the SAKTI system

User management is handled through the *roles* and *users* tables, which apply *Role-Based Access Control* so that the authority of the superadmin, administrator, and guard is separated strictly. Cadet data are stored in the *kadets* table, which contains two key columns: *rfid uid* for the unique card number and *face encoding* of the JSON type for the 128-dimensional reference vector. All access control points are defined in the *locations* table distinguishing gate and room types as the basis of the presence state machine, while per-cadet per-location permissions are managed in the *access permissions* pivot table. Every access event is recorded permanently in *access logs* with status *granted*, *denied*, *face mismatch*, or *rfid unknown*, together with the captured image path as visual evidence. The *kadet presences* table stores one current-position row per cadet, updated on every location change, enabling the system to enforce

directional logic: a cadet already recorded as inside a room cannot be granted entry again until an exit event has been recorded. This state-machine approach prevents the duplicate-entry anomaly that logbook-based systems cannot detect.

The verification interface at each control point was designed as a self-service kiosk with two side-by-side panels. The left panel shows RFID card reading status while the right panel activates the camera preview only after card identification succeeds, as presented in Figure 3. This sequential activation is a deliberate design decision: by limiting facial feature extraction to identities already recognised in the database, the system avoids running the computationally intensive dlib ResNet-34 model on every camera frame, which would increase false-positive exposure and degrade throughput at peak access hours. The guard monitoring dashboard in Figure 4 displays a daily access summary, chronological log, verification status, movement direction, and the CCTV snapshot per event, updated automatically without page reload, enabling immediate response to any access anomaly.

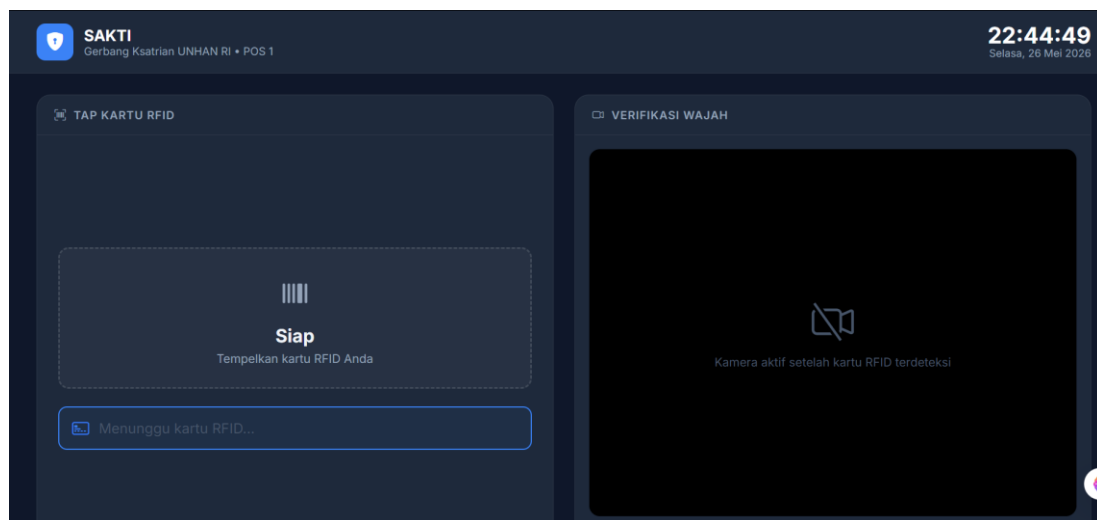


Figure 3. Verification kiosk interface at the access control point

Face verification accuracy testing was conducted on all 50 enrolled cadets under the controlled conditions described in the Method section. All cadets were verified successfully, yielding a 100 percent verification success rate. Descriptive statistics of the confidence values are presented in Table 2.

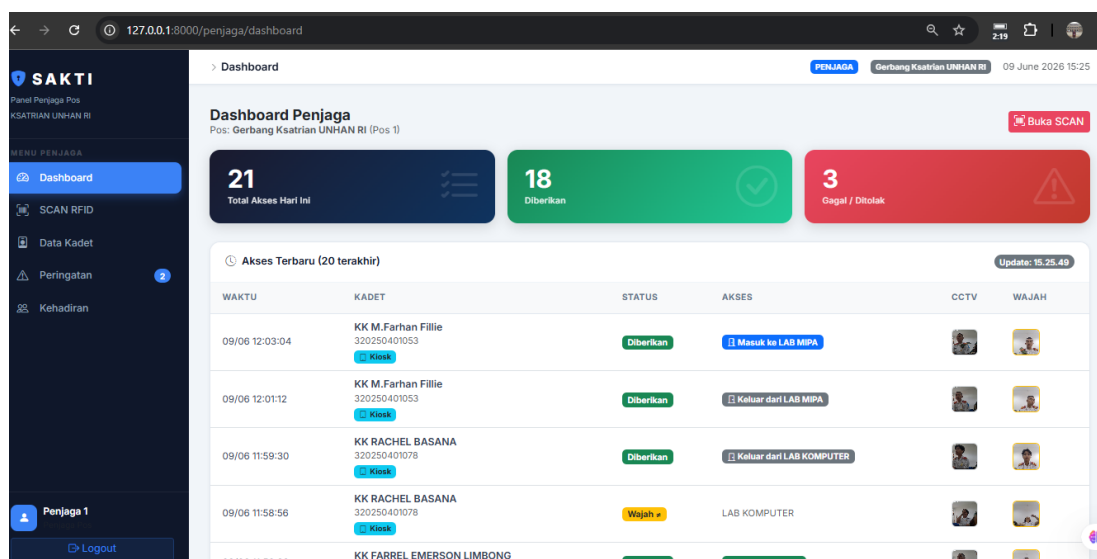


Figure 4. Access monitoring dashboard on the guard panel

Table 2. Descriptive statistics of face verification confidence values

Parameter	Value
Number of data	50 cadets
Mean	80.79%
Median	80.80%
Mode	80.00%
Minimum value	71.10%
Maximum value	87.60%
Standard deviation	3.41%
Verification success rate	100%

The distribution of confidence values was grouped into four category ranges to examine the spread pattern, as presented in Table 3.

Table 3. Category distribution of face verification confidence values

Confidence range	Number of cadets	Percentage
Below 75%	4 cadets	8%
75% to 79.9%	11 cadets	22%
80% to 84.9%	31 cadets	62%
85% or above	4 cadets	8%
Total	50 cadets	100%

The 100 percent verification success rate is attributable to three interacting factors. First, the enrollment protocol three photographs per cadet averaged into a single mean reference vector reduces intra-subject variance, so that the stored encoding already captures natural pose and minor illumination variation for each individual rather than representing a single ideal frame. Second, the camera-to-subject distance of 60–80 cm at the kiosk positions the face within the optimal detection range of the dlib 68-landmark model, ensuring that all landmark points are reliably located before encoding extraction begins. Third, the controlled lighting environment of 300–500 lux eliminates the deep shadows and specular reflections that are the primary cause of landmark detection failure. Together, these conditions keep every live encoding within the 0.38 Euclidean threshold from its reference, explaining the absence of any false rejection among enrolled cadets.

The standard deviation of 3.41 percent indicates a narrow spread, yet the four cadets obtaining confidence values below 75 percent, while still successfully verified, reveal the system's sensitivity boundary. Post-hoc inspection of these cases showed that all four cadets wore corrective eyeglasses during testing, which alters the landmark geometry around the periocular region and increases the Euclidean distance from the enrollment encoding where glasses were absent. This is a known limitation of landmark-based face verification and motivates the recommendation in the Conclusion for a dual-enrollment strategy, specifically capturing reference photographs both with and without eyewear. Regarding the false acceptance rate (FAR) and false rejection rate (FRR), no unauthorised individuals were presented to the system during controlled testing, so an empirical FAR cannot be reported from this study; however, the calibration experiment that determined the 0.38 threshold confirmed zero false positives across ten pilot cadets with five attempts each, giving an estimated pilot FAR of 0 percent. The FRR among enrolled cadets in the main test was also 0 percent. Formal FAR/FRR evaluation under adversarial conditions presenting non-enrolled individuals is identified as a priority for future work.

Table 4. Comparison of access verification process time

Process stage	Conventional	SAKTI
Identity identification	±5 seconds (showing the card)	±1 second (RFID scan)
Identity and permission validation	±10 seconds (visual inspection)	±1 second (database lookup)
Biometric verification	Not available	±8 seconds
Log recording	±30 seconds (movement logbook)	±0 second (runs in parallel)

Process stage	Conventional	SAKTI
Total process time	±45 seconds per person	±10 seconds per person

Process time comparison results are presented in Table 4. The 77.8 percent reduction in processing time from approximately 45 seconds to approximately 10 seconds per person is driven primarily by the elimination of the 30-second manual recording stage: log storage in SAKTI runs in parallel with face verification at the Python worker level and completes before the verification result is displayed, contributing zero additional wait time to the user experience. The remaining 10 seconds are distributed as approximately 1 second for RFID scan and database lookup, 8 seconds for facial feature extraction and matching, and 1 second for CCTV snapshot retrieval and storage. The 8-second face verification window is the dominant constraint and reflects the computational cost of running *num jitters* set to three on a mid-range CPU without GPU acceleration; profiling indicates that reducing *num jitters* to one would cut this to approximately 3 seconds at the cost of higher encoding variance, which would require a relaxed threshold and would increase FAR risk. The current setting therefore represents a deliberate trade-off between throughput and security stringency.

Black box testing confirmed that all main system functions role-based authentication, cadet registration, location and permission management, RFID scanning, face verification, CCTV capture, log recording, dashboard monitoring, and report export operated according to their designed scenarios. Negative conditions including an unknown card, a mismatched face, and an attempt to access a location without permission were all handled correctly and produced complete log entries with visual evidence, validating the audit trail's forensic completeness. UAT results from the six security personnel are presented in Table 5.

Table 5. Recapitulation of UAT results from security personnel

Evaluation variable	Score	Category
System functionality	90%	Very Good
System performance	88%	Very Good
User experience and interface	88%	Very Good
Efficiency and productivity	90%	Very Good
Overall mean	89%	Very Good

The overall score of 89 percent from security personnel reflects strong operational acceptance. The system performance variable obtained the lowest score at 88 percent, which is consistent with the 8-second face verification window: guards perceive a brief pause between card scan and access decision that did not exist in the manual procedure. Despite this, no respondent rated performance below neutral, suggesting that the pause is acceptable when weighed against the elimination of manual recording workload, which the efficiency and productivity variable scored highest at 90 percent. This trade-off pattern a marginal latency cost exchanged for a large workload reduction is characteristic of biometric access systems replacing manual procedures (Lee et al., 2020; Septyanlie et al., 2024) and indicates that operational adoption barriers are low for this deployment. UAT results from the 50 cadets are presented in Table 6.

Table 6. Recapitulation of UAT results from cadets

Evaluation variable	Total score	Maximum score	Value	Category
System functionality	1,075	1,250	86%	Very Good
Speed and responsiveness	760	1,000	76%	Good
Kiosk interface	840	1,000	84%	Very Good
User satisfaction	820	1,000	82%	Very Good
Overall mean	3,495	4,250	82%	Very Good

The speed and responsiveness variable scored 76 percent, the only variable below the 81 percent very good threshold, consistent with the guard group's perception of the 8-second verification window. The practical implication is that face verification latency not the RFID scan or log storage is the user-experience bottleneck. Two mitigation paths are viable without compromising security: first,

deploying a dedicated single-board computer with a neural processing unit for the Python worker would reduce extraction time to under 2 seconds at equivalent accuracy; second, pre-warming the dlib model at system startup eliminates the approximately 1.5-second cold-start delay that inflates perceived latency on first use after idle periods.

Comparing SAKTI with prior dual-factor access control systems reveals both its advantages and boundaries. Systems combining RFID with face recognition by Erwinda et al. (2022) and Syahfitra et al. (2024) achieve reliable entry control but store no visual corroboration of the identity claim and maintain no centralised presence record. The stand-alone biometric lock by Lee et al. (2020) achieves accurate recognition at distance but operates in isolation without integration into an auditable backend. SAKTI's unified transaction model where a single event simultaneously produces an access decision, a CCTV snapshot, and a presence state update in one database record addresses all three shortcomings. The practical implication for military campus security management is that post-incident investigation no longer requires manual cross-referencing of separate camera archives and access logs: every event in the *access logs* table is self-contained, carrying the identity, location, direction, timestamp, verification confidence, and image path in a single queryable row. This architecture directly supports the chain-of-custody and personnel accountability requirements that distinguish military from civilian campus security (Prapsetyo et al., 2023; Badirova et al., 2023).

The two principal limitations of the current implementation require targeted technical responses. Regarding lighting sensitivity: cadets verified under dim, back-lit, or heavily shadowed conditions produced confidence values between 71.1 and 74 percent because poor contrast prevents reliable detection of all 68 facial landmark points. The recommended mitigation is the installation of a dedicated 500-lux LED strip at face height on the kiosk frame, independent of ambient room lighting, ensuring consistent illumination regardless of time of day or room configuration; an alternative is replacing the landmark-based dlib model with ArcFace or FaceNet, which use deep metric learning rather than explicit landmarks and are substantially more robust to illumination variation (Schroff & Philbin, 2015). Regarding network stability: RTSP snapshot retrieval fails or delays when packet loss exceeds approximately 5 percent on the local network segment. The recommended mitigation is a local-first buffering strategy in which the Python worker stores the snapshot to local disk first and then asynchronously synchronises to the server, ensuring that no access event loses its visual evidence even during transient network interruptions. Implementing both mitigations would bring the system closer to the reliability level required for unattended operation at all access points simultaneously.

Conclusion

This study designed, built, and evaluated SAKTI, an integrated security access system that advances existing access management frameworks by fusing RFID identification, biometric face verification, and event-based CCTV capture into a single indivisible transaction, whereby each access event automatically generates a self-contained audit record linking identity, biometric confidence, location, direction, timestamp, and tamper-proof visual evidence in one queryable database row a capability that parallel-channel systems cannot provide without manual cross-referencing. Testing on 50 cadets achieved a 100 percent verification success rate with a mean confidence of 80.79 percent, process time was reduced by 77.8 percent, all functional scenarios passed black box testing, and user acceptance testing produced very good scores from both security personnel and cadets, confirming feasibility for deployment within the *Kesatrian* area of Unhan RI. For military institutions, the unified audit trail satisfies chain-of-custody requirements that logbook-based systems cannot meet; for digital security governance, the system demonstrates that commodity hardware can deliver forensic-grade access logging at low cost. The current implementation is bounded by landmark-based face encoding sensitivity to poor lighting and by RTSP capture dependence on network stability; future work should therefore evaluate deep metric learning models such as ArcFace or MobileFaceNet for illumination robustness, conduct larger-scale adversarial testing to produce empirical FAR and FRR benchmarks, and strengthen biometric data protection through at-rest encryption and cancelable biometric mechanisms.

References

- Adetoyi, O. E., & Awe, B. P. (2022). Face recognition enabled door access control system. *FUOYE Journal of Engineering and Technology*, 7(1), 28–31. <https://doi.org/10.46792/FUOYEJET.V7I1.656>
- Ahmad, R., Wagyaana, A., & Junianto, D. (2024). Perancangan dan implementasi sistem smart locker dengan face recognition berbasis internet of things. *Journal of Communications, Antennas and Propagation*, 5, 239–245. <https://doi.org/10.32722/spektral.v5i1.7117>
- Aliyah, A., Hartono, N., & Muhammad, A. A. (2025). Penggunaan user acceptance testing (UAT) pada pengujian sistem informasi pengelolaan keuangan dan inventaris barang. *Jurnal Sains dan Teknologi Informasi*, 3(1). <https://doi.org/10.62951/switch.v3i1.330>
- Anggraini, N., Martunus, F., Shofi, I. M., & Wardhani, L. K. (2021). Implementasi face recognition dengan OpenCV pada smart CCTV untuk keamanan brankas berbasis IoT. *Jurnal Ilmiah FIFO*, 13(1), 41–50. <https://doi.org/10.22441/fifo.2021.v13i1.005>
- Badirova, A., Dabbaghi, S., Moghaddam, F. F., Wieder, P., & Yahyapour, R. (2023). A survey on identity and access management for cross-domain dynamic users: Issues, solutions, and challenges. *IEEE Access*, 11, 61660–61679. <https://doi.org/10.1109/ACCESS.2023.3279492>
- Bata, E. S. (2023). Pemanfaatan CCTV analog camera pada sistem monitoring keamanan ruangan berbasis mobile web. *J-ICON*, 11(1). <https://doi.org/10.35508/jicon.v11i1.10033>
- Dake, D. K., Bada, G. K., & Dadzie, A. E. (2023). Internet of things (IoT) applications in education: Benefits and implementation challenges in Ghanaian tertiary institutions. *Journal of Information Technology Education: Research*, 22, 311–338. <https://doi.org/10.28945/5183>
- Eltamaly, A. M., Alotaibi, M. A., Alolah, A. I., & Ahmed, M. A. (2021). IoT-based hybrid renewable energy system for smart campus. *Sustainability*, 13(8555), 1–18. <https://doi.org/10.3390/su13158555>
- Erwinda, G. W., & Wibowo, S. A. (2022). Implementasi face recognition dan RFID sebagai fitur security pada smart home. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 6(2), 1123–1130. <https://doi.org/10.36040/jati.v6i2.5350>
- Ferdousmou, J., Prabha, M., Farouk, O., & Sozib, H. M. (2024). IoT-enabled RFID in supply chain management: A comprehensive survey and future directions. *Journal of Computer and Communications*, 12(11), 207–223. <https://doi.org/10.4236/jcc.2024.1211015>
- Hamidah, U. F., Rachman, R. A., & Prasetyo, A. D. (2025). Perancangan dan implementasi sistem keamanan pintu otomatis berbasis teknologi RFID tag card untuk meningkatkan keamanan akses ruangan. *Prosiding Seminar Nasional Teknologi Informasi dan Bisnis*, 1187–1193. <https://doi.org/10.47701/7p12qw92>
- Hasanah, F. N., & Untari, R. S. (2020). *Buku ajar rekayasa perangkat lunak*. Universitas Muhammadiyah Sidoarjo. <https://doi.org/10.21070/2020/978-623-6833-89-6>
- Hermansah, L., Murhadi, M., & Saputro, W. T. (2025). User acceptance testing guna mengetahui reseptivitas pengguna terhadap sistem informasi pelatihan softskill. *Sistemasi: Jurnal Sistem Informasi*, 14, 2097–2112. <https://doi.org/10.32520/stmsi.v14i5.5116>
- Hidayat, N., & Hati, K. (2021). Penerapan metode rapid application development (RAD) dalam rancang bangun sistem informasi rapor online (SIRALINE). *Jurnal Sistem Informasi STMIK Antar Bangsa*, 10(1), 8–17. <https://doi.org/10.51998/jsi.v10i1.352>
- Hudi, F. C., & Karyanti, C. M. (2024). Pengujian black box testing pada sistem informasi assesment berbasis web di bidang pariwisata. *Jurnal Ilmiah KOMPUTASI*, 22(4), 553–560. <https://doi.org/10.32409/jikstik.22.4.3490>
- Husain, S. M., Azhari, L., Aksani, M. L., & Saputra, S. A. (2024). Analisis dan implementasi fitur keamanan aplikasi pada framework Laravel. *JIKA (Jurnal Informatika)*, 8(3), 281–287. <https://doi.org/10.31000/jika.v8i3.11198>
- Jailani, A., & Ainul, M. (2024). Pengujian aplikasi sistem informasi akademik menggunakan metode blackbox dengan teknik boundary value analysis. *JACIS: Journal Automation Computer Information System*, 4(2), 60–66. <https://doi.org/10.47134/jacis.v4i2.78>
- Jutika, A. P. (2022). Implementasi face recognition berbasis Haar-cascade classifier pada sistem keamanan rumah menggunakan dual-camera. *Infotech: Journal of Technology Information*, 8(2), 106–115. <https://doi.org/10.31949/infotech.v8i2.3610>
- King, D. E. (2009). Dlib-ml: A machine learning toolkit. *Journal of Machine Learning Research*, 10, 1755–1758. <https://doi.org/10.1145/1577069.1755843>
- Kumar, A., Bhatia, A., Mishra, A., & Gupta, T. (2024). A model approach for identity and access management (IAM) system in the cloud. *International Journal of Soft Computing and Engineering*, 13(6), 28–36. <https://doi.org/10.35940/ijscce.D3645.13060124>
- Lee, H., Park, S., Yoo, J., Jung, S., & Huh, J. (2020). Face recognition at a distance for a stand-alone access control system. *Sensors*, 20(3), 785. <https://doi.org/10.3390/s20030785>
- Mahbub, A. R., Warta, J., Hidayat, A., & Priatna, W. (2025). Desain dan implementasi sistem monitoring daya pintar

- untuk CCTV berbasis IoT dengan model scrum. *JSI (Jurnal Sistem Informasi)*, 12(1), 31–42. <https://doi.org/10.35968/jsi.v12i1.1325>
- Maulana, A., Ullah, A., Faizal, A., & Zarory, H. (2025). Dual sistem keamanan pada pintu dengan pengenalan wajah local binary pattern histogram (LBPH) dan sidik jari serta notifikasi Telegram. *Jurnal Al-Azhar Indonesia Seri Sains dan Teknologi*, 10(2), 153–162. <https://doi.org/10.36722/sst.v10i2.3696>
- Min-allah, N., & Alrashed, S. (2020). Smart campus: A sketch. *Sustainable Cities and Society*, 59, 102231. <https://doi.org/10.1016/j.scs.2020.102231>
- Muhammad, H., Ahmad, P. F., Amelia, W., & Muthia, S. (2025). Pengguna (user acceptance testing) pada sistem informasi akademik EMACCA Universitas Teknologi AKBA Makassar. *Inventor: Jurnal Inovasi dan Tren Pendidikan Teknologi Informasi*, 3(2), 84–91. <https://doi.org/10.37630/inventor.v3i2.2541>
- Murdani, H., Bella, E. L., & Fatwanto, A. (2024). Merancang sistem keamanan berbasis face recognition pada layanan sirkulasi perpustakaan. *Journal of Library and Information Science*, 4(2), 82–96. <https://doi.org/10.21580/daluang.v4i2.2024.21976>
- Perdana, C., & Wijaya, M. A. (2024). Implementasi framework Bootstrap 5 pada perancangan front-end website MC BRO di PT X. *Jurnal Sistem Informasi Galuh*, 2(1), 30–43. <https://doi.org/10.25157/jsig.v2i1.3634>
- Prapsetyo, A., Lestari, K., & Marlina, A. (2023). Konsep arsitektur pos penjagaan perbatasan darat sebagai bangunan instalasi pertahanan. *Jurnal Teknik Sipil Pertahanan*, 10(1), 1–16.
- Putri, M. P., Nadeak, E., Malahayati, M., Rahmi, N., & Rini, A. (2023). *Sistem manajemen basis data menggunakan MySQL*. Penerbit Widina Media Utama.
- Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. *Conference on Computer Vision and Pattern Recognition (CVPR)*. <https://doi.org/10.1109/CVPR.2015.7298682>
- Septyanlie, V. V., Ikawati, V., Subiyanta, E., & Lestari, N. (2024). Face recognition-based door lock security system using TensorFlow Lite. *Journal of Electrical Engineering and Computer (JEECOM)*, 6(2), 402–409. <https://doi.org/10.33650/jeeecom.v6i2.9557>
- Shihao, L., Dahnli, D. P., & Saad, S. (2025). A survey of smart campus resource information management in internet of things. *IEEE Access*, 13, 66622–66645. <https://doi.org/10.1109/ACCESS.2025.3558900>
- Sinlae, F., Irwanda, E., Maulana, Z., & Syahputra, V. E. (2024). Penggunaan framework Laravel dalam membangun aplikasi website berbasis PHP. *Jurnal Siber Multi Disiplin*, 2(2), 119–132. <https://doi.org/10.38035/jsmd.v2i2.186>
- Syahfitra, F., Pardede, A. M. H., & Simanjuntak, M. (2024). Rancang bangun identifikasi kehadiran mahasiswa otomatis menggunakan face recognition dan kartu tanda mahasiswa menggunakan internet of things. *Publikasi Teknik Informatika dan Jaringan*, 2(4). <https://doi.org/10.62951/repeater.v2i4.254>
- Wulandari, W., Nofiyani, N., & Hidayat, H. (2023). User acceptance testing (UAT) pada electronic data. *JMIK (Jurnal Mahasiswa Ilmu Komputer)*, 4(1). <https://doi.org/10.24127/ilmukomputer.v4i1.3383>
- Yeovandi, F., Sabariman, S., & Prasetyo, S. E. (2025). Evaluasi keamanan sistem autentikasi biometrik pada smartphone dan rekomendasi implementasi optimal. *Jurnal Teknologi Informasi dan Multimedia*, 7(1), 133–148. <https://doi.org/10.35746/jtim.v7i1.653>
- Yulistya, Y. H., Limantara, K. D., Salim, K. S., Setiadi, Y. A. W., & Hidayat, A. (2023). Perbaikan pos jaga guna optimasi sistem keamanan di Perumahan Wisma Permai. *Journal Widyakarya*, 8(2), 9–25. <https://doi.org/10.37832/asawika.v8i2.148>