Inform : Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi
Vol.11 No.1, January 2026, P-ISSN : 2502-3470, E-ISSN : 2581-0367

Hybrid Face Recognition System Using Haar Cascade and Local Binary Pattern Histogram for Automatic Smart Door Access

Zahra Humaira Kudadiri[1], Muhammad Ikhsan[2]

[1,2]*Computer Science Department, Universitas Islam Negeri Sumatera Utara Medan, Indonesia*

[1]humairazahra623@gmail.com(*)

[2]mhd.ikhsan@uinsu.ac.id

Received: 2025-12-29; Accepted: 2026-01-17; Published: 2026-01-29

Abstract— Conventional key-based door access systems remain vulnerable to loss, duplication, and misuse, motivating biometric access mechanisms that can operate reliably under constrained resources. This paper proposes a hybrid face recognition system for automatic smart door access that integrates Haar Cascade for real-time face detection and Local Binary Pattern Histogram (LBPH) for lightweight recognition. The system adopts an IoT-assisted architecture in which an ESP32-CAM captures facial frames and transmits them via Wi-Fi to a processing unit that performs detection, recognition, and access-decision logic, subsequently activating a solenoid lock and generating Telegram-based event logs to support traceability. Haar Cascade efficiently localizes facial regions via multi-scale scanning and cascade-based rejection, while LBPH encodes local texture patterns into histograms for identity matching with low computational overhead. The proposed system was evaluated with three enrolled participants across seven trials, covering illumination variation, multiple faces, and a controlled failure case designed to simulate an unauthorized or non-verifiable attempt. Experimental results show a successful unlocking rate of 85.71% (6/7 trials) with an average end-to-end response time of approximately 2.20 s, demonstrating that the system can operate within practical latency constraints for real-time access control. In addition, the controlled failure case was correctly rejected, indicating a conservative security posture that prevents unsafe unlocking when facial evidence is insufficient. Overall, the findings suggest that the proposed classical-method hybrid design provides an effective balance between recognition reliability, latency, and deployment feasibility for IoT-enabled smart door security applications, particularly in cost- and power-constrained environments.

Keywords— Face Recognition; Haar Cascade; Local Binary Pattern Histogram; Automatic Smart Door Access; Internet of Things.

I. INTRODUCTION

Smart access control has become a critical layer in contemporary physical security because conventional key-based mechanisms remain prone to loss, duplication, and unauthorized transfer, thereby weakening accountability and making post-incident tracing difficult in real deployments [1], [2]. In parallel, the rapid diffusion of Internet of Things (IoT) infrastructure in homes, laboratories, and office environments has accelerated demand for access systems that are both automated and auditable, enabling sensing, decision-making, and actuation to be integrated into a coherent security workflow [2][3]. Within this landscape, biometrics has been increasingly positioned as a practical alternative to token-based authentication, particularly in IoT-driven security ecosystems that emphasize continuous operation and minimal user friction [1][2]

Among biometric modalities, face recognition is attractive for door access because it is contactless, scalable, and well-suited to camera-based security systems [4][5]. Recent literature synthesizes substantial progress in face recognition algorithms and operational deployments, ranging from feature-based classical pipelines to deep learning systems optimized for high-accuracy identification under diverse conditions [6][7]. In applied security contexts, face recognition has been adopted not only for identification but also for enforcing access policies in controlled spaces, supporting higher-level security automation and reducing reliance on shared credentials [5][8]. Nevertheless, many high-performing solutions reported in the literature depend on computationally intensive models that can be challenging to sustain on low-cost devices without sacrificing latency or stability [4][6]

A persistent engineering challenge, therefore, lies in maintaining dependable recognition performance while ensuring predictable response time and robust, long-running operation under constrained compute and power budgets [4][9]. Studies on edge-to-cloud inference emphasize that resource-aware partitioning separating acquisition and heavy computation across heterogeneous components can reduce end-to-end delay and improve system maintainability compared to fully embedded designs [5][7] At the same time, smart-home security research continues to highlight operational constraints such as illumination variation, partial occlusion, and user behavior diversity, which collectively affect real-world reliability if not explicitly accounted for in system design [10], [4].

Beyond performance, privacy and security risks surrounding biometric data have become central concerns in face recognition deployments, particularly when images or templates traverse networks or are stored in less-trusted environments [10][11]. Recent proposals in edge-based IoT scenarios introduce privacy protection frameworks and learning-based scrambling strategies to reduce leakage risk while preserving recognition utility, indicating that practical access systems increasingly require privacy-aware design choices rather than purely accuracy-driven optimization [11], [12]. Additionally, presentation attacks and spoofing attempts remain a relevant threat class for face-based authentication, and

DOI : https://doi.org/10.25139/inform.v11i1.11442

surveys in high-impact venues have emphasized that securing face recognition systems requires anticipating both benign failures (e.g., occlusion) and adversarial behaviour (e.g., spoof media) [13][14]. Although face recognition has been increasingly adopted for access-control applications, real-world deployment remains challenging. System performance may degrade due to illumination fluctuation, pose variation, motion blur, and partial occlusion caused by accessories (e.g., glasses, hats) or face coverings. Moreover, many reported implementations focus primarily on recognition accuracy while providing limited validation of end-to-end access decisions, actuator reliability, and auditable event logging, all of which are critical for security-sensitive door access systems. These limitations motivate the need for an approach that is computationally efficient, reproducible, and robust enough for practical indoor use.

Motivated by these gaps, this work proposes a Hybrid Face Recognition System for automatic smart door access that combines Haar Cascade for efficient face detection and Local Binary Pattern Histogram (LBPH) for lightweight identity recognition, deployed in a hybrid processing architecture to improve stability and response predictability. While deep learning solutions frequently dominate accuracy benchmarks, recent investigations on binary-pattern descriptors and embedded face pipelines indicate that texture-based representations remain valuable when computational simplicity, training-data efficiency, and operational predictability are primary constraints [8][11]. The novelty of this study lies in (i) operationalizing a hybrid architecture that separates acquisition and recognition workloads for sustained door-access operation, and (ii) integrating a lightweight detection–recognition pipeline appropriate for constrained deployments while maintaining clear evaluation procedures for access outcomes and response time characteristics [5][7][11]. The objective is to design and validate an automatic door-access workflow that reliably distinguishes authorized from unauthorized attempts with stable latency, while remaining implementable on practical hardware configurations commonly used in low-cost security prototypes [9][10][11].

A. Face Recognition-Based Access Control System

Face recognition has become one of the most prominent biometric modalities for physical access control systems due to its non-intrusive operation and high user acceptance. Unlike key-based or card-based mechanisms, facial authentication does not rely on transferable credentials, thereby reducing risks associated with loss, theft, or duplication. Recent security studies emphasize that contactless biometrics are increasingly favoured in smart infrastructure, particularly for access control systems that operate frequently and autonomously [1]. In smart door applications, face recognition is typically embedded within a broader access-control pipeline consisting of image acquisition, face detection, identity recognition, and actuation.

The literature stresses that system effectiveness cannot be evaluated solely by recognition accuracy; operational reliability, response time, and stability during continuous use are equally critical [8]. As a result, access-control research increasingly adopts a system-oriented evaluation perspective. From a usability standpoint, facial biometrics offer a seamless authentication experience. Users are not required to remember passwords, carry physical tokens, or perform any explicit actions beyond simply being in front of a camera. This advantage has been widely cited as a key motivation for deploying face recognition in residential and institutional smart door systems [8].

Despite these advantages, face recognition-based access control systems face notable challenges. Environmental variations such as illumination changes, camera angle deviations, and partial occlusions can significantly degrade recognition performance. Several studies report that systems performing well in laboratory conditions may experience reduced reliability in real-world deployments if these factors are not adequately addressed [15]. Deep learning-based face recognition models often achieve superior accuracy in unconstrained environments; however, they typically require large-scale training data and significant computational resources to provide low-latency inference. Such requirements can be impractical for IoT-oriented deployments, where power consumption, cost, and maintainability are critical.

In contrast, Haar Cascade and LBPH offer a lightweight, interpretable alternative: Haar Cascade enables rapid face localization through early rejection. At the same time, LBPH performs identity matching with low computational overhead and modest training requirements. Therefore, this study adopts Haar Cascade and LBPH to ensure efficient processing, acceptable latency, and feasibility for edge-device-assisted smart door access systems. Security concerns also shape contemporary research directions. Presentation attacks, including the use of printed photographs or digital displays, have been identified as significant threats in unattended access scenarios. Consequently, recent literature emphasizes the importance of robust system design and complementary safeguards rather than relying solely on recognition accuracy metrics [16].

B. Face Detection in Smart Door Systems

Face detection is a fundamental pre-processing stage in face recognition–based access control systems, as it defines the region of interest for subsequent recognition processes. Errors at this stage propagate directly to recognition, increasing false rejection rates and undermining system reliability. Consequently, detection performance is a decisive factor in the operational success of smart door systems [17]. Among classical face detection techniques, Haar Cascade classifiers remain widely employed due to their computational efficiency and suitability for real-time applications. The method relies on Haar-like features evaluated using integral images, enabling rapid computation even on resource-constrained platforms [18]. Haar Cascade detection is structured as a cascade of weak classifiers trained using the AdaBoost algorithm. Early stages of the cascade quickly reject non-face regions, while later stages perform more detailed analysis of candidate regions. This hierarchical design significantly reduces average

DOI : https://doi.org/10.25139/inform.v11i1.11442

processing time, which is critical for access control systems requiring immediate response [18].

The decision function of a Haar Cascade classifier can be expressed in Equation (1), $f(x)$ denotes the classifier score obtained by combining multiple weak classifiers, where $w_i$represents the weight of the i-th classifier and $h_i(x)$is its corresponding response.

$$S(x) = \sum_{i=1}^{N} \alpha_i h_{i(x)} \quad (1)$$

This formulation reflects how multiple simple features are combined into a strong classifier capable of distinguishing facial patterns from background regions. Haar Cascade performs reliably in controlled environments, particularly under frontal face orientation and moderate illumination. While deep learning–based detectors outperform Haar methods in unconstrained settings, their computational demands often limit practical deployment in embedded or hybrid smart door systems [6]. As a result, Haar Cascade continues to be adopted in smart door applications where system simplicity, predictable latency, and ease of implementation are prioritized over maximal robustness in unconstrained scenarios [8].

C. Face Recognition Using Local Binary Pattern Histogram

Local Binary Pattern Histogram (LBPH) is a feature-based face recognition method widely adopted in access control systems due to its simplicity and robustness under controlled conditions [17]. Unlike holistic approaches, LBPH focuses on local texture variations, making it less sensitive to global illumination changes commonly encountered in indoor access scenarios [7]. The fundamental concept of LBPH is to compare the intensity of a central pixel with that of its neighbouring pixels within a predefined radius. This comparison generates a binary pattern that captures micro-texture information such as edges and corners, which are critical for discriminating facial identities [7]. The LBPH operator is mathematically defined in Equation (2), $LBP(x_c, y_c)$ denotes the local binary pattern code computed at the center pixel located at coordinates (x_c, y_c). The parameter Prepresents the number of neighboring pixels considered in the local neighborhood, where $i_c$is the intensity value of the centre pixel and $i_n$is the intensity of the n-th neighboring pixel. The function $s(\cdot)$is a thresholding function that converts the intensity difference $(i_n - i_c)$into a binary value, and the resulting binary pattern is weighted by $2^n$and summed over all neighbors to produce the final LBP code.

$$LBP(x_c, y_c) = \sum_{n=0}^{P-1} s(i_n - i_c) \times 2^n \quad (2)$$

In practice, LBP codes computed over the facial region are accumulated into histograms that represent individual identities. Recognition is performed by comparing histogram distances using similarity metrics such as Euclidean or Chi-square distance, enabling efficient identity matching [7]. LBPH offers a favourable trade-off between recognition accuracy and computational complexity. While deep learning–based approaches often achieve higher accuracy in unconstrained datasets, LBPH requires significantly fewer training samples and lower computational resources, which is advantageous for real-time access control systems [7].

D. Hybrid Architecture in Face Recognition–Based Smart Door Systems

Hybrid architecture has been increasingly adopted in face recognition–based smart door systems to address the limitations of fully embedded implementations [4]. In hybrid systems, image acquisition and recognition processing are decoupled, allowing each subsystem to operate according to its computational characteristics. This architectural separation enables continuous image acquisition without interruption from recognition processing tasks. Studies report that such decoupling significantly improves system responsiveness and stability, particularly in access-control applications that require real-time operation [19]. Hybrid architectures also facilitate better resource management. Computationally intensive recognition tasks can be executed on more capable processing units, while lightweight acquisition modules focus on consistent data capture, reducing overall system latency [20]. From a design perspective, modular hybrid architectures support scalability and maintainability. Algorithm updates or hardware upgrades can be implemented independently, minimizing system downtime and redevelopment effort [21]. Reliability is another critical advantage of a hybrid design. By isolating system components, faults or delays in recognition processing do not necessarily disrupt image acquisition or access monitoring, enhancing fault tolerance [22].

E. Automatic Access Control Systems Based on Face Recognition

Automatic access control systems based on face recognition have been widely investigated as a secure alternative to conventional authentication mechanisms. Unlike card-based or password-based systems, facial authentication enables seamless verification without requiring physical contact or user interaction [23]. Recent studies emphasize that face recognition–based access control is particularly suitable for environments where security and convenience must be achieved simultaneously. In automatic smart door applications, access decisions are generated by integrating facial recognition outputs with control logic that governs door locking mechanisms. This integration allows doors to be unlocked only when an authorized face is detected, thereby preventing unauthorized entry [7]. Access control systems employing classical computer vision techniques remain relevant due to their interpretability and ease of deployment. Unlike deep learning approaches that require extensive datasets and high computational resources, classical methods such as Haar Cascade and LBPH offer practical advantages in constrained environments [19]. A hybrid smart door architecture that separates image acquisition from recognition processing to enhance efficiency and system stability, to implement a complete face detection and recognition pipeline using Haar Cascade and LBPH including access-decision logic, solenoid

DOI : https://doi.org/10.25139/inform.v11i1.11442

actuation, and Telegram-based event logging and to evaluate the system under practical scenarios (illumination variation, multi-face presence, and controlled failure conditions) by reporting the success rate and end-to-end response time as key performance indicators.

II. Research Methodology

A. Use Case Diagram

The Use Case Diagram is employed to describe the functional interaction between the user and the smart door access system at a high level of abstraction [24]. This diagram focuses on the system's behaviour from the user's perspective rather than its internal implementation, making it an essential tool for capturing functional requirements [25]. In the proposed system, the primary actor is the user attempting to access the door, while the system itself represents the boundary enclosing all recognition and control functionalities [26]. The main use case involves facial authentication, which includes image capture, identity verification, and access decision. Secondary use cases, such as access denial and system standby, are implicitly triggered based on recognition outcomes [27]. The Use Case Diagram clarifies that the authentication process is fully automated and requires no explicit user interaction beyond being in front of the camera. This design reflects the non-intrusive nature of biometric face recognition systems and aligns with usability principles emphasized in access control research [28]. From a methodological standpoint, the Use Case Diagram serves as a foundation for subsequent modelling stages. By defining system boundaries and user-system interactions early, the diagram helps prevent functional ambiguity. It ensures that all later architectural and behavioural models remain consistent with the intended system purpose [29].

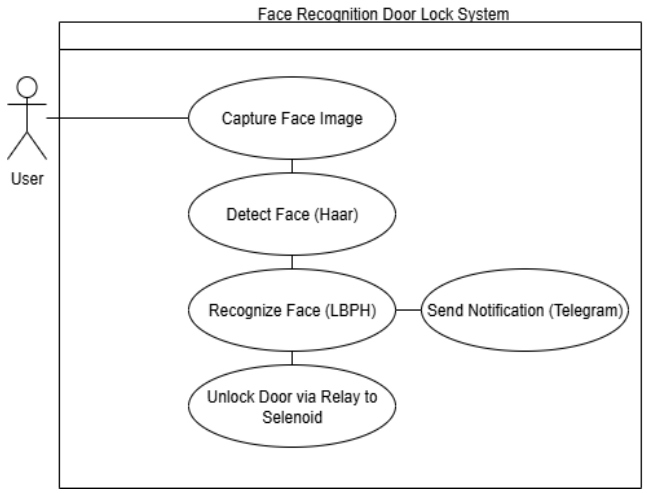

Fig.1. Use Case Diagram of the Smart Door Access System

Fig.1 summarises the system's functional requirements by mapping the main authentication use case and its outcomes. It clarifies the boundary of interaction between the user and the smart door system during access attempts.

B. Overall System Architecture

The System Architecture Diagram provides a structural representation of the proposed hybrid smart door access system, illustrating the relationship between hardware and software components [30]. This diagram is critical for understanding how system modules are organized and how responsibilities are distributed across components [31]. The architecture comprises three principal subsystems: the image acquisition unit, the processing unit, and the access control actuator. The image acquisition unit consists of a camera module that captures facial images. These images are transmitted to the processing unit, which performs face detection, feature extraction, and recognition [32].

The processing unit hosts the core algorithms, including Haar Cascade for face detection and Local Binary Pattern Histogram for recognition. Haar Cascade detects faces by evaluating Haar-like rectangular features computed efficiently using integral images. A cascade of weak classifiers is applied in a multi-scale, sliding-window manner, rejecting non-face regions early to enable fast detection. The output is a bounding box ROI used for recognition. LBPH performs recognition by encoding local texture patterns. For each pixel, the neighborhood intensity is thresholded to form a binary pattern; these patterns are accumulated into histograms across spatial grids, producing a robust representation under moderate illumination changes. During inference, the histogram of an input face is compared with enrolled templates using a distance metric. The system assigns the identity with the minimum distance and grants access only when this distance is below a predefined threshold; otherwise, access is denied. Separating these functions from the acquisition unit reduces computational burden at the sensing level and improves overall system stability [28]. The access control actuator receives recognition results and executes physical actions, such as unlocking or maintaining the door in the locked state [32]. This architectural separation embodies the hybrid design principle, which has been shown to enhance scalability, maintainability, and fault tolerance in biometric access control systems [31]. The System Architecture Diagram, therefore, provides a clear blueprint that supports both implementation and future system extensions.

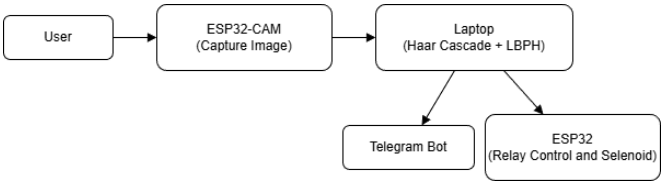

Fig.2. System Architecture Diagram of the Hybrid Smart Door Access System

Fig.2 shows how captured facial images are processed for detection and recognition before triggering the door actuator. It also highlights the separation between acquisition, processing, and actuation modules to support stable operation.

C. Flowchart of System Operation

The flowchart describes the sequential operational logic of the smart door access system from start to finish [15]. Unlike

DOI : https://doi.org/10.25139/inform.v11i1.11442

the Use Case Diagram, which captures functional intent, the flowchart focuses on procedural execution and decision-making paths [16]. The operational flow begins with continuous monitoring of the access area through the camera module. When a face is detected, the system captures an image frame and forwards it to the processing unit. Face detection is performed first to ensure that only valid facial regions proceed to recognition [28]. After detection, the recognition process compares the extracted facial features with registered templates stored in the database. A decision node evaluates whether the similarity score exceeds a predefined threshold. If the threshold is met, access is granted; otherwise, access is denied, and the system returns to the monitoring state [29]. The flowchart explicitly represents all decision points and termination conditions, ensuring that no undefined operational states exist. Such explicit workflow modelling is crucial for avoiding logical errors and improving system reliability in real-world deployments [32].

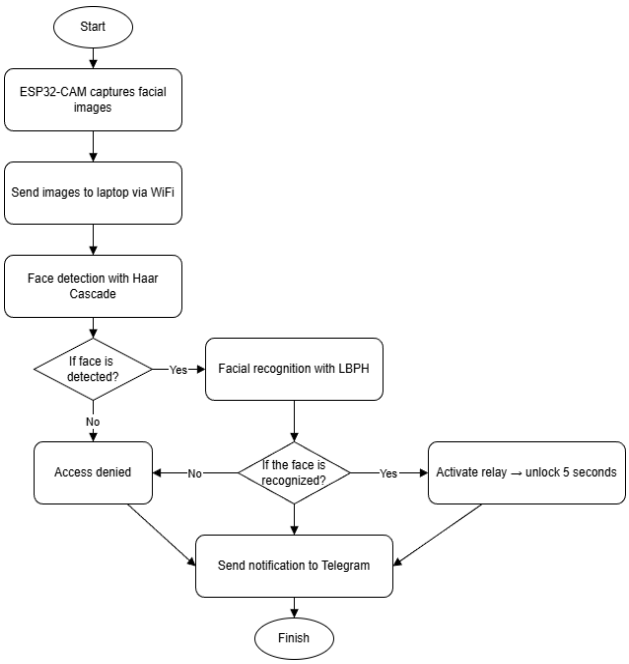

Fig.3. Flowchart of the Smart Door Access Workflow

Fig.3 presents the end-to-end workflow from monitoring, face detection, and recognition to the final access decision. It ensures that each decision branch (grant/deny) and the system loop-back are clearly defined.

D. Sequence Diagram

The Sequence Diagram illustrates the temporal order of interactions among system components during an access attempt [30]. This diagram emphasizes *when* and *in what order* messages are exchanged, making it particularly useful for analyzing communication latency and synchronization [29]. In the proposed system, the sequence begins when the camera module captures a facial image and sends it to the processing unit. The processing unit sequentially invokes face detection and recognition functions before transmitting the authentication result to the access control module [31]. The access control module then issues a command to either unlock the door or maintain its locked state. Once the action is completed, a feedback signal confirms execution, and the system returns to the idle monitoring state. This sequence ensures a closed-loop operation with clear initiation and termination points [32]. By explicitly modelling message exchanges, the Sequence Diagram helps identify potential communication delays and supports optimizing response time, a critical performance metric in smart door access systems [28]. Security in smart access control systems depends on reliable authentication, since weak verification may enable unauthorized access [33]. To implement automated verification efficiently, computer vision–based recognition is widely adopted, as it can accurately identify visual information in real time [34].

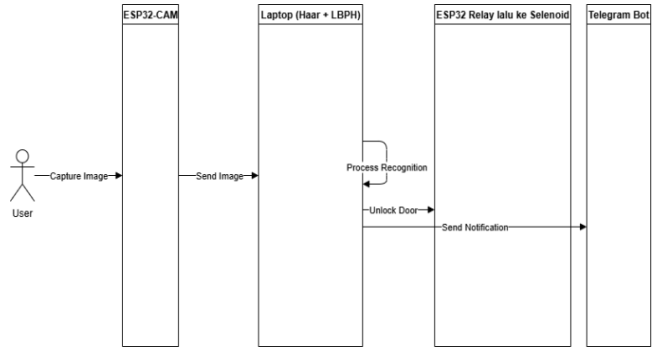

Fig.4. Sequence Diagram of Communication Between System Components

Fig. 4 depicts the message sequence from image capture to recognition and actuator control during an access attempt. It confirms that the door unlock command is issued only after a valid recognition response is returned.

E. Experimental Protocol and Evaluation Metrics

The proposed smart-door access system was evaluated end-to-end with three enrolled participants (P1–P3). The evaluation was designed to reflect practical access scenarios: (i) illumination variation, (ii) multi-face presence in a single frame, and (iii) accessory-induced appearance variation, including a controlled failure case under full face covering. A trial is defined as a single access attempt in which an enrolled participant presents their face to the system. A trial is counted as successful only when correct recognition is immediately followed by physical solenoid unlocking, ensuring that both algorithmic decision-making and actuator execution are validated as a unified workflow. Based on the conducted experiments, Participant P1 completed two trials with two successful unlocks; Participant P2 completed one trial with one successful unlock; and Participant P3 completed four trials, comprising three successful unlocks and one failed attempt under a full face covering, yielding a total of seven trials.

To support auditability, each access attempt is documented using aligned evidence: (1) the recognition output (bounding

DOI : https://doi.org/10.25139/inform.v11i1.11442

box and identity label), (2) the system notification log reporting confidence and detection duration, and (3) the physical lock state (locked vs unlocked). In terms of classification outcomes, the evaluation yielded 6 true positives, 1 false negative, and 0 false positives, resulting in a recall and precision of 100% for unlocking events. Response-time measurements were recorded for successful unlocking events. Specifically, the logged detection durations. These measurements were used to compute descriptive statistics for system responsiveness, including mean response time.

III. Result and Discussion

This section reports the experimental outcomes of the proposed hybrid face-recognition door-access system using three enrolled participants (P1–P3) selected to represent (i) illumination variation, (ii) multi-face presence in a single frame, and (iii) accessory-induced appearance change, including a controlled failure case. The evaluation is conducted end-to-end. A trial is considered successful only when the system (a) produces a correct recognition decision and (b) executes a physical unlocking action through the solenoid mechanism. To ensure reproducibility and auditability, each subject's result is presented using three aligned pieces of evidence: (1) the visual recognition output (bounding box and label), (2) the system log showing confidence and detection duration, and (3) the final physical state of the lock (locked vs unlocked).

A. Illumination Variation (Dim vs Normal)

Fig.5 to Fig.7 present the recognition performance of Participant P1 under different lighting conditions. Under normal illumination (Fig.5), recognition remains correct, with improved confidence of 36%. Under dim illumination (Fig.6), the system correctly recognizes P1 with a confidence score of 45%. The notification logs shown in Fig. 7 report detection durations of 2.09 s and 2.30 s, confirming successful solenoid actuation. These results indicate that although illumination affects the confidence value produced by the LBPH classifier, the system maintains stable identity decisions and reliable end-to-end unlocking behaviour.

Fig. 5. Participant P1 Recognition Output Under Normal Illumination (Confidence: 36%).

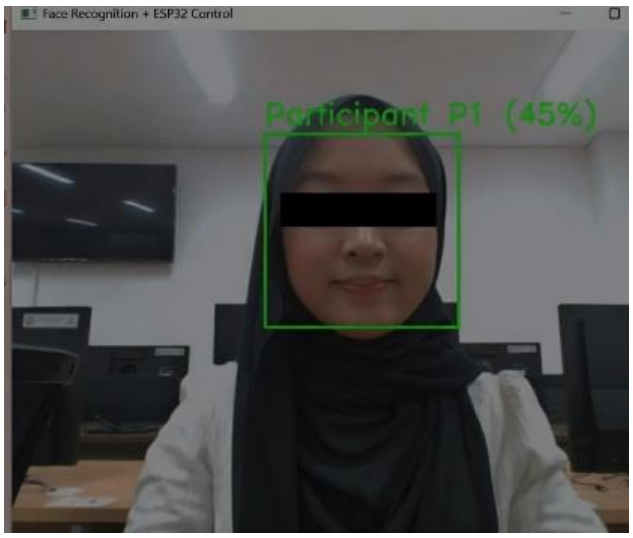

Fig.6. Participant P1 Recognition Output Under Dim Illumination (Confidence: 45%).

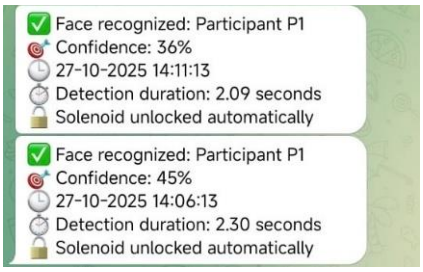

Fig.7. Participant P1 Notification Logs Showing Confidence (36%, 45%) and Detection Duration (2.09 S, 2.30 S) with Solenoid Actuation Confirmation.

B. Multi-Face Presence in a Single Frame

The system's robustness in a multi-person scenario is evaluated using Participant P2, as illustrated in Fig. 8 and Fig. 9. In Fig. 8, two faces appear simultaneously in the camera frame. The system correctly recognizes the enrolled face (P2) with 46% confidence, while rejecting the additional face as Unknown. This behaviour is critical for access control, as it prevents unauthorized unlocking by non-enrolled individuals. Fig.9 further confirms correct operation by reporting a detection duration of 2.01 s and successful solenoid actuation following valid recognition.

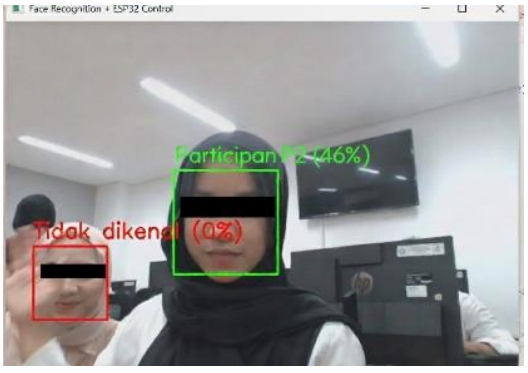

Fig. 8. Participant P2 Multi-Face Frame: The Enrolled Face Is Recognized (Confidence: 46%) While the Additional Face Is Rejected as Unknown (0%).

DOI : https://doi.org/10.25139/inform.v11i1.11442

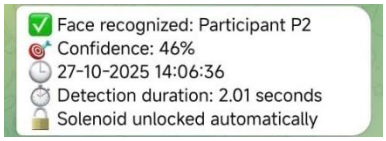

Fig. 9. Participant P2 Notification Log Confirming Recognition (Confidence: 46%), Detection Duration (2.01 S), and Solenoid Actuation.

C. Accessories and Controlled Failure (Full Face Covering)

The recognition robustness of Participant P3 under appearance variations caused by accessories and occlusion is illustrated in Fig.10 to Fig.14. In the baseline condition (Fig.10), the system recognizes P3 with a confidence of 23%. When glasses are introduced (Fig. 11), confidence increases to 41%, and with a hat (Fig. 12) to 44%. Despite these variations, the system consistently performs correct recognition and executes unlocking, as confirmed by the notification logs in Fig.14 with detection durations of 2.02 s, 2.23 s, and 2.54 s. A controlled failure scenario is presented in Fig. 13, where a full-face covering prevents successful recognition, and no unlock command is issued. This conservative response demonstrates that the system prioritizes security by denying access based on insufficient facial evidence.

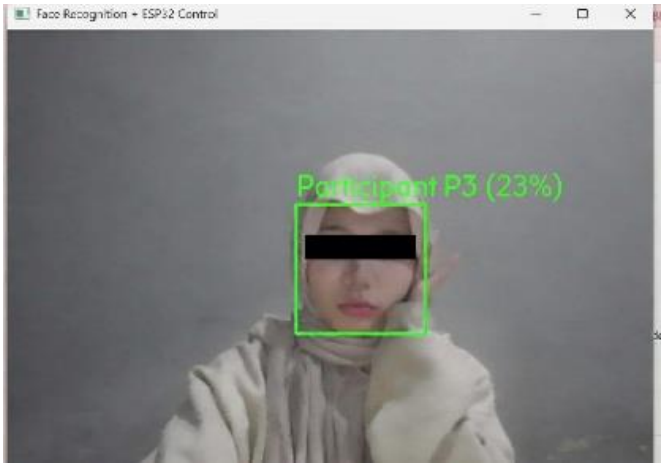

Fig.10. Participant P3 Baseline Recognition (Confidence: 23%)

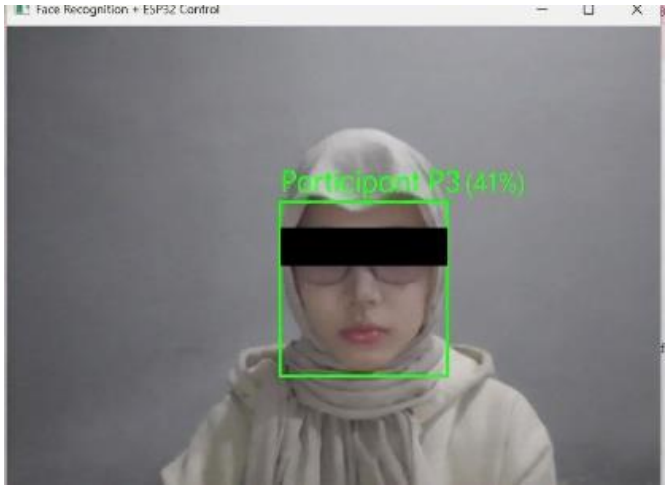

Fig.11. Participant P3 Recognition with Glasses (Confidence: 41%)

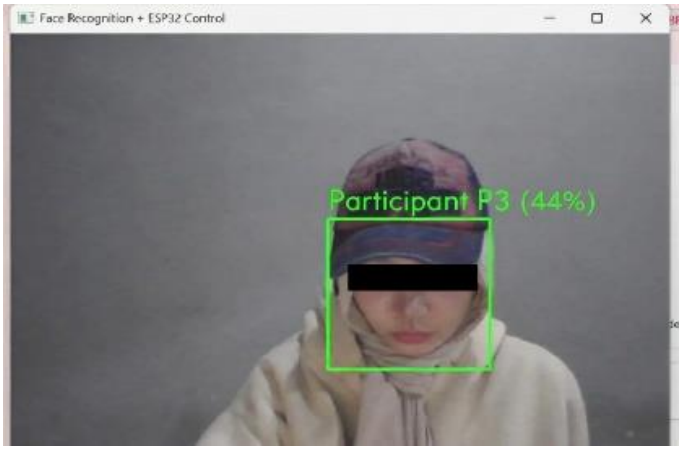

Fig.12. Participant P3 Recognition with A Hat (Confidence: 44%).

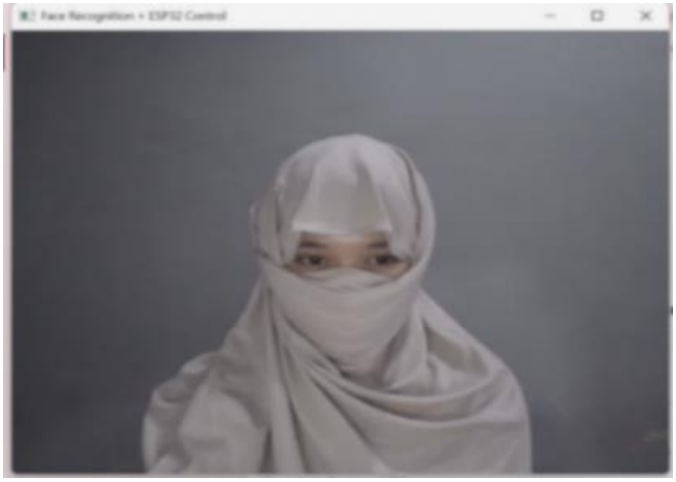

Fig. 13. Participant P3 Full Face Covering (Mask) Resulting in No Successful Recognition/Unlock Event.

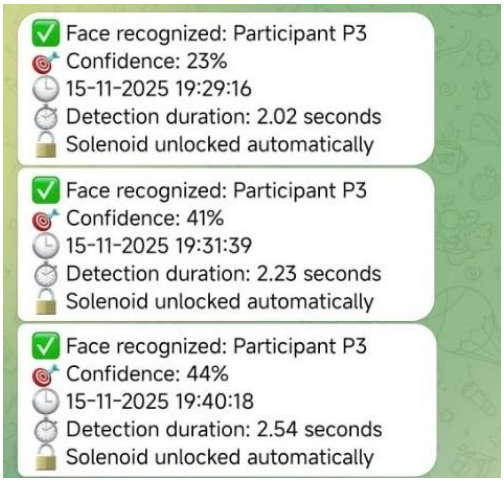

Fig. 14. Participant P3 Successful Notification Logs Reporting Confidence (23%, 41%, 44%) and Detection Duration (2.02 S, 2.23 S, 2.54 S) With Solenoid Actuation Confirmation.

D. Selenoid Door-Lock Validation (Locked vs Unlocked)

The physical validation of the access decision is shown in Figs. 15 and 16. Fig. 15 depicts the solenoid in the locked state

DOI : https://doi.org/10.25139/inform.v11i1.11442

when access is denied or no valid recognition is produced. In contrast, Fig.16 shows the unlocked state after a successful recognition event triggers the actuator. Across all valid recognition trials involving participants P1-P3, the observed physical door state consistently matches the system decision, confirming correct end-to-end integration between recognition, control logic, and mechanical actuation.

Fig.15. Door State Solenoid Remains Locked
(Access Not Granted/No Valid Unlock Command)

Fig.16. Door State Solenoid Unlocks
(Access Granted/Unlock Command Executed)

E. Trial Accounting and Definitions (End-to-End, Enrolled Attempts)

In this analysis, a "trial" denotes a single access attempt in which an enrolled subject presents their face to the system, and a trial is counted as successful only when correct recognition is immediately followed by solenoid unlocking; accordingly, Participant 1 completed two trials with two successful unlocks, Participant 2 completed one trial with one successful unlock, and Participant 3 completed four trials comprising three successful unlocks and one failed attempt under full face covering, yielding a total of seven trials.

In Equation (3), N represents the total number of evaluation trials conducted under full-face covering conditions. The total number of trials is obtained by summing three outcome categories, namely successful enrolled trials, failed enrolled trials, and unsafe unlocking events. In this experiment, the results correspond to 2 successful trials, 1 failed trial, and 4 unsafe unlocking cases, which yield a total of $N = 7$ trials.

$$N = 2 + 1 + 4 = 7 \tag{3}$$

In Equation (4), TP represents the number of enrolled trials that were successfully recognized and granted access, FN denotes enrolled trials that failed to be recognized or unlocked, and FP represents cases where a non-enrolled individual caused the system to unlock. Based on the experimental results under full-face covering conditions, six true positives were observed, along with one false negative and no false positives.

$$TP = 2 + 1 + 3 = 6, FN = 1, FP = 0 \tag{4}$$

Equation (5) defines recall (sensitivity) as the proportion of correctly recognized enrolled trials compared to all enrolled trials, combining both successful recognitions and failed recognitions.

$$Recall = \frac{TP}{TP + FN} \tag{5}$$

Equation (6) shows that recall is the ratio of correctly recognized enrolled trials to the total number of enrolled trials. The resulting recall of approximately 85.71% indicates that the system successfully granted access in 6 of 7 enrolled attempts, with only 1 missed recognition under full-face covering conditions, where conservative denial is expected.

$$Recall = \frac{6}{6 + 1} = \frac{6}{7} = 0.857142 \tag{6}$$

Equation (7) indicates that all unlocking events corresponded to enrolled users. Since no false positives were recorded, the precision value reached 100%, meaning that every observed system unlock was correct and no unsafe access occurred during the evaluation.

$$Precision = \frac{6}{6 + 0} = 1.0 = 100\% \tag{7}$$

In Equation (8), the F1-score is defined as the harmonic mean of precision and recall. Substitution ($Precision = 1.0$,

DOI : https://doi.org/10.25139/inform.v11i1.11442

$Recall = 0.857142$) is used for the evaluation. The F1-score combines precision and recall into a single balanced performance measure. By substituting, the resulting value is $F1 = 0.923076 = 92.31\%$, which indicates high overall classification performance.

$$F1 = \frac{(2 \times Precision \times Recall)}{(Precision + Recall)} = \frac{(2 \times 1.0 \times 0.857142)}{(1.0 + 0.857142)} = 92.31\% \quad (8)$$

In Equation (9), the end-to-end accuracy $Accuracy_{e2e}$ is defined as the proportion of successfully enrolled trials (TP) to the total number of trials (N). This metric summarises the system's overall success rate in granting access during the evaluation. The numerical substitution using the observed results, where $TP = 6$ and $N = 7$. The computed value indicates that the system successfully unlocked in most trials under the tested conditions.

$$Accuracy_{e2e} = \frac{TP}{N} = \frac{6}{7} = 0.857142 = 85.71\% \quad (9)$$

Detection durations were recorded only for successful access events because the full-face-covering failure case did not generate a successful log entry. Specifically, Participant P1 produced two recorded durations of 2.30s and 2.09s, Participant P2 produced one duration of 2.01s, and Participant P3 produced three durations of 2.02s, 2.23s, and 2.54s; therefore, the response-time dataset used for statistical analysis in Equation (10), the total response-time sum is computed by adding all recorded successful unlocking durations t_i for $n = 6$ trials. The resulting sum is 13.19 seconds, which serves as the basis for computing the average response time.

$$\sum_{i=1}^{n} t_i = 2.30 + 2.09 + 2.01 + 2.02 + 2.23 + 2.54 = 13.19 \quad (10)$$

Equation (11) defines the mean response $\bar{t}$ time, the total sum of response times divided by the number of observations, using the values in Equation (12), the mean response time is 2.1983 seconds, which is approximately 2.20 seconds.

$$\bar{t} = \left(\frac{1}{n}\right)\sum_{i=1}^{n} t_i = \frac{13.19}{6} = 2.1983 = 2.20 \quad (11)$$

In Equation (12), the median response time is obtained by averaging the two middle values after sorting the recorded durations. The computed median of 2.16 seconds indicates the system's typical central response time.

$$Median = \frac{2.09 + 2.23}{2} = 2.16 \quad (12)$$

Equation (13) calculates the response-time range as the difference between the maximum and minimum observed durations. The range of 0.53 seconds reflects the spread of response times across the successful trials.

$$Range = t_{max} - t_{min} = 2.54 - 2.01 = 0.53 \quad (13)$$

Equation (14), the sample variance s^2 measures the variability of response times around the mean $\bar{t}$. The obtained variance value indicates relatively low dispersion across the recorded trials.

$$s^2 = \frac{\sum_{i=1}^{n}(t_i - \bar{t})^2}{n-1} = 0.0414167 \quad (14)$$

Equation (15) computes the sample standard deviation $s$as the square root of the variance. The resulting standard deviation of approximately 0.20 seconds confirms that response times remain stable with only modest variation.

$$s = \sqrt{s^2} = \sqrt{0.0414167} = 0.2035 \text{ s} = 0.20 \quad (15)$$

The three-subject evaluation reveals operational characteristics relevant to the deployment of access control. Participant 1 confirms that the system maintains correct identity decisions across varying illumination, while confidence values improve in well-lit conditions. Participant 2 demonstrates that the system can recognize an enrolled user even when another face is present in the same frame and can reject the non-enrolled individual without triggering unsafe unlocking. Participant 3 shows robustness to common accessories (glasses and a hat), while the full-face covering case correctly results in denial, aligning with a conservative security posture. Finally, the solenoid-state evidence (Fig.15 and Fig.16) confirms that recognition outcomes are faithfully translated into physical lock actuation, completing the end-to-end validation loop required for smart door access applications.

The experimental results demonstrate that the proposed hybrid pipeline can support practical smart-door access under typical indoor conditions. The system achieved 6 successful unlocks out of 7 trials (85.71% success rate), with 100% precision for successful access events, indicating that it did not produce any false unlocks due to unauthorized attempts. This outcome is important from a security perspective, as false acceptance is generally more critical than false rejection in access-control applications.

However, the presence of a single failed attempt suggests that recognition reliability remains sensitive to extreme appearance changes, as evidenced by the controlled failure case involving a full-face covering. This behaviour is consistent with the underlying characteristics of LBPH, which relies on local texture patterns; when the facial region is largely occluded, the available texture information becomes insufficient, leading to rejection. From a system design standpoint, this conservative behaviour is desirable because it prevents unsafe unlocking when facial evidence is incomplete.

In terms of responsiveness, the recorded detection durations for successful unlock events ranged from 2.01 s to 2.54 s, with results of 2.30 s and 2.09 s for Participant P1, 2.01 s for Participant P2, and 2.02 s, 2.23 s, and 2.54 s for Participant P3. This response time reflects the combined latency of frame acquisition on the ESP32-CAM, wireless transmission to the processing unit, host-side detection and recognition, and

DOI : https://doi.org/10.25139/inform.v11i1.11442

solenoid actuation. Although the delay is noticeable, it remains acceptable for door access workflows, where an interaction time of approximately 2–3 seconds is practical.

Nevertheless, the current evaluation is limited by the small number of enrolled participants and the controlled indoor environment. Future work should extend the experiments to larger, more diverse datasets that include variations in pose, partial occlusion, and more challenging lighting conditions, and incorporate additional safeguards, such as illumination normalization and adaptive thresholding, to improve robustness while preserving the system's conservative security stance.

IV. Discussion

This study demonstrates that a hybrid IoT-assisted smart door access system integrating Haar Cascades for face detection and LBPH for face recognition provides a reliable, computationally efficient approach for indoor access control. The experimental evaluation confirms that the proposed architecture supports practical access decisions with conservative security behaviour, as no false unlockings occurred during the trials. Importantly, the research objectives were achieved: the system was successfully designed and implemented as an end-to-end workflow linking image acquisition, recognition, physical actuation, and event logging, and its performance was validated under representative conditions, including illumination variation, multi-face presence, and controlled failure scenarios.

Beyond the prototype, the results highlight broader implications for IoT and edge-based security deployments. Specifically, this work indicates that classical computer-vision methods, when integrated into a complete access-control pipeline, remain a viable alternative in contexts where hardware cost, power consumption, latency requirements, and long-term maintainability may constrain deep learning. In addition, integrating event logging via Telegram provides a practical pathway to traceable access control, supporting accountability and post-event verification. Future work should expand validation to larger, more diverse user populations and incorporate robustness enhancements, such as illumination normalization, adaptive thresholds, and anti-spoofing mechanisms, to improve generalizability under real-world conditions.

References

[1] A. Awad, A. Baby, E. Barka, and K. Shuaib, "AI-powered biometrics for Internet of Things security: A review and future vision," *J. Inf. Secur. Appl.*, vol. 82, p. 103748, 2024.

[2] A. Rahim, Y. Zhong, T. Ahmad, S. Ahmad, P. Pławiak, and M. Hammad, "Enhancing Smart Home Security: Anomaly Detection and Face Recognition in Smart Home IoT Devices Using Logit-Boosted CNN Models," *Sensors*, vol. 23, no. 15, 2023, doi: 10.3390/s23156979.

[3] D. Hercog, T. Lerher, M. Truntič, and O. Težak, "Design and Implementation of ESP32-Based IoT Devices," *Sensors*, vol. 23, no. 15, 2023, doi: 10.3390/s23156739.

[4] P. P. Oroceo, J. I. Kim, E. M. F. Caliwag, S. H. Kim, and W. Lim, "Optimizing Face Recognition Inference with a Collaborative Edge–Cloud Network," *Sensors*, vol. 22, no. 21, 2022, doi: 10.3390/s22218371.

[5] D. Tribuana, Hazriani, and A. L. Arda, "Face recognition for smart door security access with convolutional neural network method," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 22, no. 3, pp. 702–710, 2024, doi: 10.12928/TELKOMNIKA.v22i3.25946.

[6] Y. Xu, T. M. Khan, Y. Song, and E. Meijering, "Edge deep learning in computer vision and medical diagnostics: a comprehensive survey," *Artif. Intell. Rev.*, vol. 58, no. 3, pp. 1–78, 2025, doi: 10.1007/s10462-024-11033-5.

[7] Y. C. Chen, Y. S. Liao, H. Y. Shen, M. Syamsudin, and Y. C. Shen, "An Enhanced LBPH Approach to Ambient-Light-Affected Face Recognition Data in Sensor Network," *Electron.*, vol. 12, no. 1, 2023, doi: 10.3390/electronics12010166.

[8] S. S. F. A. Elnozahy, S. C. Pari, and L. C. Liang, "Raspberry Pi-Based Face Recognition Door Lock System," *Internet of Things*, vol. 6, no. 2, 2025, doi: 10.3390/iot6020031.

[9] J. Zhang *et al.*, "A Real-Time and Privacy-Preserving Facial Expression," *Electronics*, vol. 13, pp. 1–25, 2024.

[10] Y. Xie, P. Li, N. Nedjah, B. B. Gupta, D. Taniar, and J. Zhang, "Privacy protection framework for face recognition in edge-based Internet of Things," *Cluster Comput.*, vol. 26, no. 5, pp. 3017–3035, 2023, doi: 10.1007/s10586-022-03808-8.

[11] S. Zhao, L. Zhang, and P. Xiong, "PriFace: a privacy-preserving face recognition framework under untrusted serve," *J. Ambient Intteligence Humaniz. Comput.*, vol. 14, pp. 2967–2979, 2023.

[12] Y. Huang, Z. Wu, J. Chen, and H. Xiang, "Privacy-Preserving Face Recognition Method Based on Randomization and Local Feature Learning," *J. Imaging*, vol. 10, no. 3, 2024, doi: 10.3390/jimaging10030059.

[13] Z. Yu, Y. Qin, X. Li, C. Zhao, Z. Lei, and G. Zhao, "Deep Learning for Face Anti-Spoofing: A Survey," *IEEE*, vol. 45, no. 5, 2023.

[14] S. M. Abdullahi, S. Sun, B. Wang, N. Wei, and H. Wang, "Biometric template attacks and recent protection mechanisms: A survey," *Inf. Fusion*, vol. 103, no. August 2023, 2024, doi: 10.1016/j.inffus.2023.102144.

[15] B. Amirgaliyev, M. Mussabek, T. Rakhimzhanova, and A. Zhumadillayeva, "A Review of Machine Learning and Deep Learning Methods for Person Detection, Tracking and Identification, and Face Recognition with Applications," *Sensors*, vol. 25, no. 5, 2025, doi: 10.3390/s25051410.

[16] A. Baran and E. Bartuzi-Trokielewicz, "Face the Challenge—Generalization of Presentation Attack Detection," *Sensors*, vol. 25, no. 18, pp. 1–18, 2025, doi: 10.3390/s25185792.

[17] A. Adouani, W. Henia, and Z. Lachiri, "A comparison of face detection methods using spontaneous videos," *Multimed. Tools Appl.*, vol. 81, pp. 23163–23191, 2022.

[18] M. R. Holla, D. Suma, and M. D. Holla, "Optimizing accuracy and efficiency in real-time people counting with cascaded object detection," *Int. J. Inf. Technol.*, 2024, doi: 10.1007/s41870-024-02153-w.

[19] W. Zhang, H. Zhou, J. Mo, C. Zhen, and M. Ji, "Accelerated Inference of Face Detection under Edge-Cloud Collaboration," *Appl. Sci.*, vol. 12, no. 17, 2022, doi: 10.3390/app12178424.

[20] P. Zhang, L. Tan, Z. Yang, F. Huang, L. Sun, and H. Peng, "Device-edge collaborative occluded face recognition method based on cross-domain feature fusion," *Digit. Commun. Networks*, vol. 11, no. 2, pp. 482–492, 2025.

[21] G. Luo, N. Chen, J. He, B. Jin, Z. Zhang, and Y. Li, "Privacy-preserving clustering federated learning for non-IID data," *Futur. Gener. Comput. Syst.*, vol. 154, pp. 384–395, 2024.

[22] Q. Yuan and Z. Li, "Distributed Inference Models and Algorithms for Heterogeneous Edge Systems Using Deep Learning," *Appl. Sci.*, vol. 15, no. 3, 2025, doi: 10.3390/app15031097.

[23] N. Fadel, "Facial Recognition Algorithms: A Systematic Literature Review," *Imaging*, vol. 99, no. 21, pp. 5217–5231, 2021.

[24] M. Arif, C. Mohammad, and M. Sadiq, "UML and NFR-framework based method for the analysis of the requirements of an information system," *Int. J. Inf. Technol.*, vol. 15, pp. 411–422, 2023.

[25] P. Boutot and S. Mustafiz, "IoTMoF: A Requirements-Driven Modelling Framework for IoT Systems," *IEEE*, vol. 3, pp. 296–305, 2023.

[26] I. Compagnucci, F. Corradini, F. Fornari, A. Polini, B. Re, and F. Tiezzi, "A systematic literature review on IoT-aware business process modeling views, requirements and notations," *Softw. Syst. Model.*, vol. 22, pp. 969–1004, 2023.

[27] Y. Kirikkayis, F. Gallik, M. Winter, and M. Reichert, "BPMNE4IoT: A Framework for Modeling, Executing and Monitoring IoT-Driven

DOI : https://doi.org/10.25139/inform.v11i1.11442

Processes †," *Futur. Internet*, vol. 15, no. 3, pp. 1–34, 2023, doi: 10.3390/fi15030090.
[28] A. Colakovic, "IoT systems modeling and performance evaluation," *Comput. Sci. Rev.*, vol. 50, p. 100598, 2023.
[29] N. Messaoudi, H. Hicham, M. T. Messaoud, and H. M. Elkamel, "Multi-Layer Consistency Validation of IoT Systems with UML Inheritance Dynamic Diagrams via SPIN Model Checking," *Ing. des Syst. d'Information*, vol. 28, no. 6, pp. 1533–1547, 2023, doi: 10.18280/isi.280610.
[30] S. Thitareedechakul and W. Catanawood, "Formal Verification of Sequence Diagram with State Invariants Using Timed Automata," in *Proceedings of the 20th International Conference on Computing and Information Technology (IC2IT 2024)*, 2024, pp. 43–54.
[31] D. Lehner, "A Model-Driven Platform for Engineering Holistic Digital Twins," *IEEE*, vol. 185, pp. 179–185, 2023.
[32] I. Hafaiedh, A. Elaoud, and A. Maddouri, "A formal model-based approach to design failure-aware Internet of Things architectures," *J. Reliab. Intell. Environ.*, vol. 10, pp. 413–430, 2024.
[33] G. F. Mumtaz, J. Zeniarja, A. Luthfiarta, and A. N. I. Muttaqin, "Optimizing Face Recognition and Emotion Detection in Student Identification Using FaceNet and YOLOv8 Models," *Inf. J. Ilm. Bid. Teknol. Inf. dan Komun.*, vol. 10, no. 1, pp. 34–44, 2025, doi: 10.25139/inform.v10i1.9304.
[34] F. A.-I. A. Putra, A. R. Jatmiko, D. M. Putri, and A. H. Al-Fath, "Vehicle Licence Number Plate Recognition Using Convolution Neural Network for Traffic Violators in Indonesia," *Inf. J. Ilm. Bid. Teknol. Inf. dan Komun.*, vol. 9, no. 2, pp. 181–186, 2024, doi: 10.25139/inform.v9i2.8449.

DOI : https://doi.org/10.25139/inform.v11i1.11442