3DiVi Building the Intelligent World

WHITE PAPER

Facial Recognition for Access Control and Attendance Tracking:

Technology, Architectures, Case Studies and Implementation Practices

Table of contents

Facial Recognition in Workplace Security: From Trend to Standard

The shift toward smarter, more secure workplaces is well underway. According to HID Global's 2024 State of Physical Access Trend Report, the use of biometric technologies in physical access control (ACS) systems has grown from 30% in 2022 to 39% in 2024, based on a survey of over 1,200 security professionals worldwide.

Notably, 23% of respondents identified biometrics as one of the top three technology trends shaping the future of access control.

Yet, outdated technologies remain common: one in three companies still rely on proximity cards, and 28% continue using systems compatible with magnetic stripe cards.

These traditional methods are increasingly seen as vulnerable, with well-known risks like lost cards, "buddy punching," and limited real-time tracking.

With the global facial recognition market projected to grow from US$5.73bn in 2025 to US$14.55bn by 2031, facial recognition is quickly rising as a practical alternative.

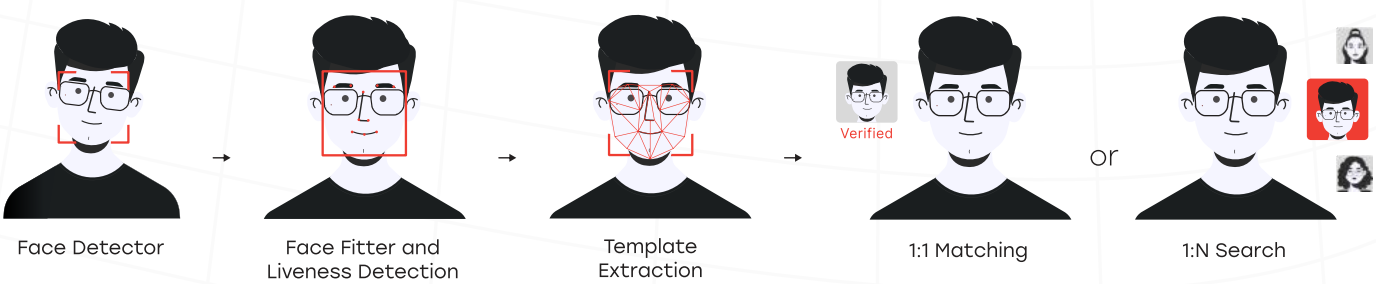
Unlike PINs, badges, or manual attendance logs, it offers contactless, real-time identity verification that is both secure and user-friendly. This makes it particularly effective for managing access, tracking work hours, and automating employee attendance—without the friction of physical tokens or manual input.

As face recognition technology becomes more accurate, cost-effective, and privacy-conscious, its role in everyday workforce management is no longer a future trend—it's becoming a new standard for secure and efficient workforce operations.

> This white paper explores how facial recognition can be effectively implemented for access control, time tracking, and attendance management in 2025—highlighting real-world use cases, technology requirements, privacy considerations, and practical steps for adoption.

Facial Recognition vs Physical ID Methods

Facial recognition offers seamless and secure identity verification that is difficult to forge or manipulate. Unlike physical tokens or passwords, a person's face cannot be lost, forgotten, or shared. At its core, the technology follows a four-step process that enables real-time contactless identification.



Face Detection: Finding the Face

The first step is to detect whether a human face is present in a photo or video frame. Modern face recognition systems use AI models—especially deep learning networks like Convolutional Neural Networks (CNNs)—to scan for facial patterns and draw bounding boxes around detected faces. These models are trained to recognize faces even in difficult conditions, such as poor lighting, side angles, or partial occlusions.

Face Alignment: Standardizing the View

Once a face is detected, it needs to be adjusted into a consistent, frontal view. This is done using facial landmarks—such as the eyes, nose, and mouth—to correct for head tilt, rotation, and scale. The result: every face looks similar in orientation and proportion, which improves recognition accuracy in the next steps.

Biometric Template Extraction: Creating the Digital Faceprint

After alignment, the system extracts a unique biometric "template" from the face. Think of it as a mathematical snapshot—a numerical vector that captures distinctive facial features like shapes, contours, and texture patterns. This compact representation makes it easy to compare one face to another in milliseconds.

Face Matching: Verifying or Identifying the Person

Now comes the matching phase:

- 1:1 Matching (Verification): Compares a person's face to a single stored template (e.g., unlocking a smartphone or verifying a logged-in user).
- 1:N Matching (Identification): Compares a face against a database of templates to identify who it is—used in access control or video surveillance systems.

Face recognition addresses the following shortcomings of traditional physical ID systems.

Feature	Facial Recognition	Physical Methods (Cards, Badges, PINs, Paper Logs)
Security	Biometric data is resistant to forgery and misuse (especially when combined with liveness checks)	Cards and PINs can be stolen, copied, or shared
User Experience	Hands-free and frictionless	Requires manual interaction (swiping, typing, scanning)
Speed	Instant authentication	Slow check-ins and bottlenecks during peak hours
Accuracy	High accuracy, minimal error rate	Prone to manual input errors and "buddy punching"
Maintenance	No physical devices or replacements needed	Cards can be lost, worn out, or deactivated
Hygiene	Fully contactless	Requires physical contact (badges, keypads, turnstiles)

To sum up, with contactless operation, automation capabilities, and strong integration potential with HR, payroll, and facility management systems, face recognition goes beyond replacing traditional physical IDs—it outperforms them.

Access Control

Facial recognition is transforming how organizations manage facility entry by enabling instant identity verification, dynamic role-based access permissions, and real-time detection of unauthorized individuals through watchlists.

This not only strengthens security but also eliminates entry bottlenecks — minimizing wait times during peak hours without compromising protection.

Key Functionality:

- **Real-Time Identity Verification:** Instant matching of live faces against authorized biometric templates enables quick and secure access decisions.
- **Multi-Level Access Permissions:** Role-based access control allows restricting entry to sensitive areas based on employee roles or clearance levels.
- **Watchlists and Alerts:** Systems maintain customizable watchlists (e.g., VIPs, blacklisted individuals, contractors), triggering real-time alerts when matches occur.
- **Visitor Management:** Temporary enrollment and controlled access for non-employee personnel streamline site security without manual oversight.
- **Audit Trails and Reporting:** Automated logging of access events, including identities, timestamps, and image snapshots, supporting security audits and incident investigations.
- **Liveness Detection:** Identifies and blocks spoofing attempts using photos, videos, or masks—ensuring only real, live individuals gain access.
- **Multi-Factor Authentication:** Facial recognition can be combined with additional credentials such as access cards to strengthen security layers when needed.

Integration Options:

- **Scalability and Integration:** Designed to integrate with existing physical security systems (e.g., turnstiles, alarm systems, CCTV) and built on a scalable architecture that accommodates deployments from small offices to large campuses and multi-site enterprises.
- **Emergency Response Support:** Integration with emergency management systems can facilitate rapid lockdowns or targeted alerts if unauthorized or flagged individuals are detected during critical incidents.
- **Customizable Access Policies:** Access permissions can be tailored dynamically based on time of day, location, or situational context (e.g., temporary lockdowns or elevated security alerts).

Attendance Tracking

Attendance tracking is the process of monitoring when employees start, take breaks, and end their work shifts to ensure accurate timekeeping and payroll management.

Facial recognition technology reshapes this process by providing a fast, touch-free way to log attendance — eliminating the need for badges or fingerprint scanners. Employees simply walk past or glance at a camera, and their presence is recorded instantly.

Key Functionality:

- **Contactless Time Logging:** Automatically records employee check-ins and check-outs with timestamps through facial recognition, eliminating the need for cards or fingerprint scanners.
- **Shift and Schedule Validation:** Cross-references attendance data against predefined schedules, flagging early arrivals, late check-ins, or unauthorized presence.
- **Buddy Punching Prevention:** Unique biometric identifiers ensure that only the authorized employee can log attendance, preventing proxy clock-ins.
- **Event Logging:** Detailed logs with timestamps and facial snapshots support audits, incident investigations, and compliance with labor regulations.

Integration Options:

- **System Compatibility:** Facial recognition can be integrated with HR, payroll, and workforce management systems for smooth data flow and unified operations like wage calculations.
- **Real-Time Alerts:** Configurable notifications for attendance anomalies help managers respond promptly to scheduling issues.

Hardware Considerations

The choice and configuration of devices directly influence face identification speed, accuracy, and user experience. The most widely used hardware options include:

- **Built-in Cameras in Smartphones and Tablets**

  Smartphones and tablets equipped with face recognition software to clock in and out offer convenience and mobility, allowing access and attendance to be tracked even in remote or outdoor environments without additional hardware installations. Beyond mobility, built-in cameras continually benefit from hardware advancements such as higher-resolution sensors or improved low-light performance.

- **Biometric Terminals**

  These all-in-one devices combine a camera, processing unit, and interface (e.g., touchscreen or badge scanner). Commonly deployed at turnstiles, gates, or secure doors, biometric terminals handle face capturing, liveness detection, and face matching. They are typically configured to capture a high-quality facial image as a person approaches—positioned to look down at the user for an optimal angle. The terminal detects the face, matches it against the database, and unlocks the turnstile—all in under 2 seconds.

- **Standalone Cameras for Flow-Based Identification**

  Standalone cameras should be positioned to face the flow of people directly, capturing frontal or near-frontal images. Ideally, the camera detects a face a few seconds before a person reaches the access point, allowing the system more time to select the best frame to improve identification accuracy.

  When using standalone cameras, a dedicated device with a screen is required near the gate or turnstile so that users can clearly see their entry status (e.g., door opened or access denied).

  Proper camera setup is essential, especially in areas with challenging lighting or high foot traffic. Effective placement ensures reliable identification results without requiring users to stop or interact with the system.

For 14+ years in real-world face recognition deployments, we identified internal and external critical factors that affect face recognition performance: lighting, camera angles and resolution, the quality of your reference photos and more.

Even seasoned integrators overlook these variables — which is why we built **3DiVi Cam QA** — a camera quality assessment tool. It scans 19+ key camera factors from live or recorded footage and gives you clear, expert recommendations to fix camera setups and boost face identification accuracy.

📎 Learn more or request an assessment here

System Architectures

Implementing facial recognition for access control and attendance tracking requires carefully designed system architectures that balance performance, security, scalability, and privacy. Understanding these architectures and their common bottlenecks is crucial to ensure reliable, efficient operation in real-world conditions.

Key Business Factors

Constant connectivity (device ↔ server)

The ability of a device to operate even when the connection to the server is lost. For example, one of our clients, a large macadamia plantation operator, used face recognition to track employee attendance on remote sites, allowing devices to collect and match facial data locally and sync with the server once connectivity was restored.

Data synchronization criticality (revoking/adding access rights)

- How fast an access removal must reach the gate: seconds, minutes, or “next visit.”
- The reverse is also critical: knowing who is currently on-site or on shift is essential, for example, in hazardous facilities or high-security areas.

Recognition errors criticality (FAR/FRR)

Business cost of letting outsiders in (FAR) vs. inconveniencing staff (FRR).

Architecture	Edge-centric	Server-centric
Decision point	On device (smartphone / tablet / biometric terminal)	Frames/videostream → server decides
Server connectivity	Not required (periodic sync)	Constant, reliable
Access rights sync	Risk of outdated rights → fast push needed for revocations	Single source of truth
Recognition quality	Limited by device power	Maximum accuracy (ensembles, heavy models)
Best fit	Remote / offline locations	Secure sites with strong connectivity

Edge-Centric Architecture

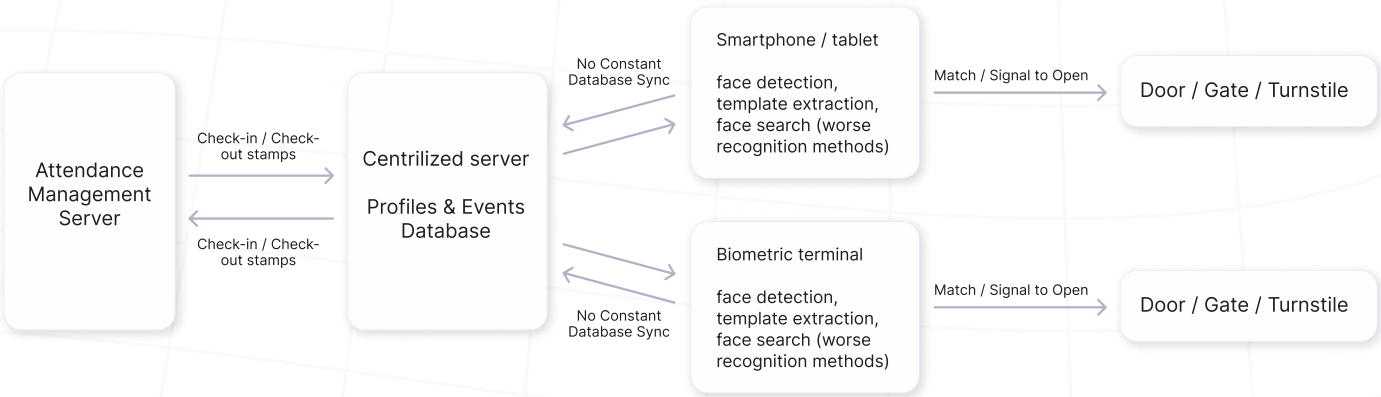
In an edge-centric setup, all facial recognition tasks—face detection, liveness detection, template extraction, and matching—are performed directly on the device (camera, tablet, or biometric terminal). The system functions independently of a server or constant network connection, making it suitable for remote or offline sites.

Advantages:

- **Works offline:** No constant connectivity required, resilient to network outages.
- **Ultra-low latency:** Fast authentication at the door, even in high-traffic areas.

Challenges:

- **Data synchronization risks:** Revoking or updating access rights may take time.
- **Limited scalability:** Device compute power restricts accuracy and large-scale deployments.



Server-Centric Architecture

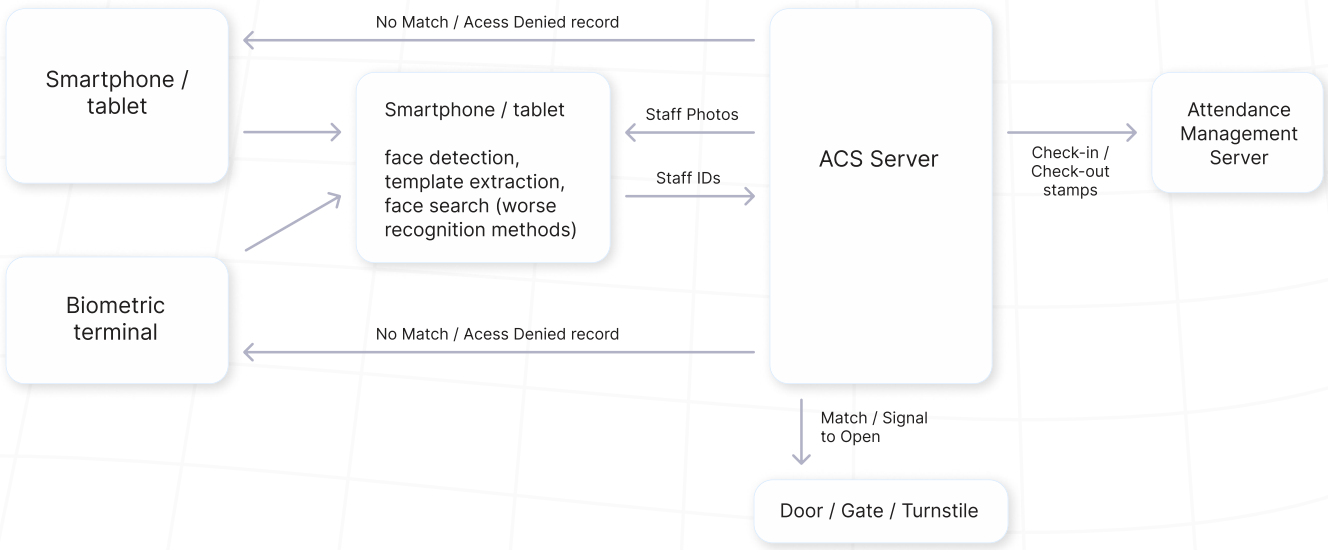
In a server-centric setup, facial images or features are securely transmitted to a centralized server for liveness detection, template extraction, and matching (where legally permitted). The server acts as the single source of truth, ensuring all access rights and biometric templates are always up to date. This model delivers maximum recognition accuracy by leveraging powerful compute resources and advanced models, making it suitable for high-security environments with reliable network connectivity.

Advantages:

- **Maximum accuracy:** Centralized use of advanced models and ensembles.
- **Always up-to-date access rights:** Revocations and updates are applied instantly.
- **High scalability:** Handles large biometric databases across multiple sites.
- **Centralized management:** Simplifies updates, monitoring, and integration with HR, payroll, and security systems.

Challenges:

- **Data synchronization risks:** Revoking or updating access rights may take time.
- **Limited scalability:** Device compute power restricts accuracy and large-scale deployments.
- **Limited scalability:** Device compute power restricts accuracy and large-scale deployments.



Case Studies

3DiVi's face recognition technology is trusted across a wide range of use cases—from large-scale outdoor attendance tracking in remote environments to high-security access control in corporate settings. Below are real-world deployments that demonstrate the versatility and reliability of our solutions in action.

Attendance Tracking in Macadamia Plantations

In large-scale agricultural plantations, traditional attendance tracking was often unreliable due to remote locations, unstable connectivity, and a transient workforce. By deploying Microsoft tablets integrated with 3DiVi Face SDK, workers can now clock in and out with a quick facial scan at the start and end of each shift.

This implementation has streamlined attendance logging, reduced disciplinary issues related to timekeeping, and improved the accuracy of work hour tracking—ideal for large outdoor workforces operating in challenging conditions.

📎 Read more here

Secure Access Control with 3D Face Terminals

A leading corporate campus upgraded its security by integrating biometric terminals featuring 3D face recognition technology from 3DiVi. These all-in-one devices provide rapid and reliable identity verification at gates and turnstiles, enabling seamless entry for authorized personnel while preventing unauthorized access.

The terminals perform liveness detection to combat spoofing attempts, delivering secure, real-time authentication in less than two seconds. This deployment strengthened site security, accelerated access flows during peak hours, and simplified visitor management through temporary access provisioning.

📎 Read more here

These are just two examples of our successful face recognition deployments. Explore more real-world projects at 3DiVi.ai.

Final Thoughts

In 2025 and beyond, facial recognition isn't just a competitive edge—it's the new standard for secure, intelligent access control and attendance tracking. From corporate offices to remote outdoor sites and high-traffic facilities, its adoption is accelerating. But success hinges on more than technology alone. Strategic alignment of system architecture, hardware configuration, and real-world testing is critical to unlock its full potential with minimal risk. The time to modernize your access and attendance is now.

Contact Information

3divi.ai info@3divi.com 440 N Barranca Ave #3430 Covina, CA 91723 United States