CENTRE FOR PROFESSIONAL AND ADVANCED STUDIES
GANDHINAGAR P.O, KOTTAYAM-Phone 0481 2595478

No.2152/2023/CPASHO 17.05.2025

QUOTATION NOTICE

Sealed competitive quotations are invited from registered/approved firms for the supply and installation of PUNCHING MACHINES to various institutions under CPAS.

SlNo	specification	quantity
	Required System Features 1. **Face Recognition with Gesture Detection** 1. **Automatic Detection**: Captures the employee's face upon approach to the device. 2. **Palm Gesture Validation**: Attendance is marked upon detecting a palm gesture, with the image securely stored locally. 3. **Liveness Detection**: Prevents spoofing by ensuring only real faces are detected. 4. **Fallback on Validation**: Ask for RF Tag and check the template exist locally. If not, fetch from the cloud server and validate again. If exist, check again with lower accuracy. If success, log the event as suspicious. If failed, generate warning and notify the administrator. 5. **Fallback Without Gesture:** **Known Face**: The user's event is logged with the stored image. **Unknown Face**: The system captures and stores the face image and keep the details including date and time for manual review. 6. **Features storage** The device should support local storage of features of face (for detection) if it detect once and also can send and revive the same from the central server. Also should able to search in the remote server for the face details and fetch from the server and match the face if required 7. **Face Entry Support**: The administrator should be able to remotely enroll new users and upload their facial templates to the central server. 2. **Units** 1. **Cloud Server** **Server provided by the institution with Linux** as operating system. Suggest the recommended configuration of the server.the functions are as follows.	

Centralised Data Management

Attendance Data Storage: Stores all attendance records from multiple devices,including user IDs,timestamps,encrypted data and gesture validation . **Synchronization**: Ensures seamless synchronization of offline attendance data once client devices reconnect to the server.

User Profiles: Maintains a centralized database of user information, including facial recognition templates, RFID data, and user credentials.

Data Storage (Shareable Database from institution)

Database Integration: Utilizes robust database systems such as MySQL or PostgreSQL for manaing attendance data, userprofiles, and systemlogs.

Access to Video Recording and Storage

Play back Support: Allows authorized personnel to access and review recorded videosand images stored in the local storage of units for security investigations for the central control and also from each unit.

Centralized Login and User Verification

Provides a centralized login portal for all users (administrators, employees, and operators) using secure credentials.

Enables authentication across all connected devices and platforms through a unified system.

Login Event Logs :

Maintains logs of all login attempts, including successful logins, failures, and lockouts for security auditing.

Custom Configuration and Management

Access Control: Manages user roles and permissions for accessing system data, ensuring only authorized personnel can view or edit sensitive information.

Client Configuration Updates: Sends configuration changes to client devices, such as enabling or disabling features like palm gestures or fallback modes.

Cloud Dashboard: Provides an intuitive web-based interface for administrators to monitor and manage the entire system.

Remote Data Control and Management

Centralized Data Access: Allows administrators to access and control attendance records, device logs, and system configurations from any location via a secure cloud dashboard. Enables real-time monitoring and reporting of attendance data. Remote Data Updates

Updates user profiles, device configurations, and encryption keys remotely from the server.

Pushes firmware updates to client devices to maintain system compatibility and introduce new features.

Manual Data Adjustments:

Allows administrators to manually add, update, or delete attendance records or user profiles in case of anomalies or corrections.

Data Export:

Provides options to export attendance data and logs in various formats (e.g., CSV, Excel, or PDF) for integration with payroll or other systems.

Data Security & Compliance

Data protection mechanisms (e.g., AES-256, TLS for transmission).

Role-based access to personal data.

Retention policies and legal compliance

2 .Processing Unit:

The central unit managing all operations, device communication, and attendance logs in the cloud.

Handles facial recognition, gesture detection, encryption, timestamps validation, and offline synchronization.

Units: Raspberry Pi, Jetson Nano Local Storage: 1TB SSD for offline data storage, Capable of handling encrypted attendance logs and additional video recording data.

3 .Camera Unit:

Captures facial images and detects palm gestures.

Includes RFID reader for dual-mode authentication and audio and visual feedback for user interaction.

Units: Arduino, ESP or any other with PoE Support for RF, Monitor, Touch Screen, feedback and other support.

4 .Camera Specifications and Recommendations:

Resolution: Full HD (1080p) or higher for precise face and gesture detection.

Frame Rate: Minimum 30 fps for smooth motion capture.

Infrared (IR) Support: Ensures accurate detection in low-light or nighttime conditions.

Wide Dynamic Range (WDR): Handles varying lighting conditions effectively.

Field of View (FOV):

Horizontal: 70-90 degrees for multi-user capture.

Vertical: 50-70 degrees for proper face alignment.

Recommended Models:

◦ Hikvision DS-2CD2387G2 or better

CP Plus CP-UNC-TB41PL3-VMS or better

any other higher resolution camera that support this function, should approved by the instituion on demand.

Camera Placement :

1	Height: 4.5 - 5.5 feet for optimal face alignment. Distance: 2-6 feet from the user. **Weatherproofing**: Necessary for outdoor installations. **3. Offline Key Management and Encryption** 1. **Random Key Reception**: Client devices fetch AES-256 keys and sequence numbers from the server at random intervals, storing them encrypted locally during offline periods. (Optional) 2. **Key Expiry and Updates:** The server updates keys 1-2 times daily at random intervals. (optional) 3. Offline Mode Functionality: Attendance data is encrypted locally and synced upon reconnection with sequence validation to prevent replay attacks . **4. Lighting Installation for Low-Light Conditions** 1**. Lighting Recommendations**: **LED Lights with Motion Sensors:** Activates upon detecting movement. **IR Lighting:** Enhances facial recognition in complete darkness. **Adjustable Brightness**: Ensures optimal lighting without glare. 2. **Placement**: Above or near the camera for even illumina tion of faces. Weather proof casings for out door installa tions. **5 .Client-Server Status Checks** 1. **Boot Success Notification**: Client sends a "Boot Suc cess " message after every restart, including device ID, boot timestamps, and local time. 2. **Periodic Health Checks**: Server pings clients periodically to monitor uptime and connectivity. Alerts are generated if devices fail to respond after multiple retries. 6 **.System Communication and Data Flow** 1. **Client - to - Server Communication** : Normal Data Transmission: Includes user ID, encrypted a ttendance data, status code , and local timestamp. Boot Notification: Includes device ID, boot timestamp, and local time. **7. Server-to-Client Communication:** 1. **Key Updates**: New encryption keys and sequence numbers sent periodically. 2. **Health Checks**: Periodic server pings to confirm device status. **8 .System Resilience and Tamper Detection** **1. Offline Mode Functionality:** Attendance data is captured and encrypted locally during connectivity issues.	40

Data is queued for synchronization upon reconnection.

2. **Reconnection Logic** :

Unsent logs are synced with sequence validation, ensuring no duplication.

3. **Tamper Detection:** The server flags time discrepancies or unresponsive devices for manual investigation.

9 .**Video Recording for Security Purposes**

1. **Low - Rate Recording:** Continuous or event - triggered video recording is stored locally at low bit - rates to reduce storage consumption.

2. **Retention Period:** Configurable retention (e.g., 30 days) with automatic over writing of old footage.

10 . Database Requirements

1. **Database System:**

Primary: MySQL or PostgreSQL for structured attendance data storage.

Secondary: SQLite for lightweight local storage in offline scenarios.

2. **Cloud Server Integration**: The institution's server running Ubuntu Linux, with the following specifications: **CPU**: 8+ cores.

RAM: 16GB+.

Storage: Minimum 4TB SSD for encrypted back ups and real-time log uploads.

Network: Gigabit Ethernet for seamless communication.

Software: Docker for containerized services and database management.

11 .System Communication and Data Flow

1. Client-to-Server Communication:

Attendance logs, encrypted data, status codes, and timestamps are transmitted.

2. **Server-to-Client Communication:**

Encryption keys, sequence numbers, and health checks are pushed to devices.

12 .System Resilience and Tamper Detection

1. **Offline Mode Functionality**: Attendance data is captured and encrypted locally during connectivity issues. Data is queued for synchronization upon reconnection. 2. **Tamper Detection**: Time discrepancies or unresponsive devices are flagged for manual investigation.

13 . Integration Testing

1. Ensure seamless operation across online/offline modes and with gesture detection.

14 . User Training

1. Provide staff training for managing devices, the cloud dash board, and troubleshooting.

15 . Scalability Planning

1. Design the system to accommodate future expansions (e.g., additional units, higher user counts).

16 . **Installation and Hardware Requirements**

1. Components and Units

Cameras: Two cameras (for face and gesture detection).

Lighting: LED Lights with Motion Sensors (1-2 per entrance). IR Lights for low-light performance.

RFID Reader: For fallback attendance marking.

Audio-Visual Feedback Unit: LED indicators and audio prompts.

Touch Screen : For realtime interaction and feed back.

2. **Placement and Wiring**

Lighting Installation : Mounted at appropriate heights for uniform illumination. Weather proof casings for out door in stallations.

Network and Power: Power over Ethernet (PoE) for all devices. Wiring and mounting costs are included

3. 17 .Uninterruptible Power Supply (UPS)

UPS Selection: Based on the power requirements of the system, considering components such as the processing unit , camera units , lighting , RFID readers , and audio units . The UPS should provide over 24 hours of back up time .

4. **Estimated Power Consumption** :

Processing Unit (Raspberry Pi, Jetson Nano): 30 - 100W.

Camera Units: 5-15W per camera.

Lighting (LED & IR): 10-50W per light.tton on the router: RFID Readers and Audio Units: 5-15W each.

5. **Total Power Estimation**: A UPS capable of handling 500W+ can be selected.

6. **Quotation Requirements**

Please include the following in your quotation:

1. Hardware Unit Costs (per device/unit) -

Cameras (Face and Gesture)

- LED Lights -

Processing Units

- IR Lights

- RFID Readers

- Monitors/Touch Screens

- Audio-Visual Feedback Units

- Any other required hardware units

2. Lighting and Wiring

- LED/IR Light pricing (including mounting and wiring and other charges)

	- PoE network wiring (per-meter cost) **3. UPS Details** - Model, capacity (500W+), backup time (≥24 hrs), and pricing **4. Installation Charges** - Installation of all devices, lighting, network, and power wiring. Also include extra charges if any. **5. Cloud Integration Costs** - Setup of centralized dashboard, synchronization logic, and storage 6. Server Costs - Server setup (Ubuntu LTS, Docker, PostgreSQL/MySQL, encrypted backups) 7. **Software Costs (Responsive Design)** - Include price of software module wise. -Login & User Roles, Dashboard (for Admin/Operator/Employee), User Management, Attendance Logs, Device Management, Configuration Panel, Video Review (Security), Reports & Analytics, Mobile App **7. Annual Maintenance Contract (AMC)** - Onsite hardware support and software updates (minimum 3 years) - Minimum 3 years onsite warranty on all hardware **9. Delivery and Implementation Timeline** - Within 10 Days from the date of purchase order. 7. *All custom software developed under this project shall be the property of CPAS. Vendor shall hand over complete source code, database schema, API documentation, and admin credentials at the time of deployment. 8. Web-Based User Interface is necessarry for the processing of data and monitor and manage the units. 9. Data protection as per Indian IT Act	

Last date of receipt of quotations : Till 1.00 pm on 24.05.2025

Date of opening of quotations:2 pm on 24.05.2025

General Conditions

1. The quotations shall be submitted to DIRECTOR,CENTRE FOR PROFESSIONAL AND ADVANCED STUDIES, GANDHINAGAR P.O, KOTTAYAM 686008.
2. The price quoted should be inclusive of all taxes, loading/ unloading charges, transmission charges, installation charges etc.
3. Warranty details shall be mentioned in the quotation.
4. The equipments/ item shall be supplied within 10 days of the supply order.
5. 5 % of the total cost shall be remitted as security deposit.
6. The Director reserves the right to reject any or all quotations without specify reason.

Sd/-

DIRECTOR

CENTRE FOR PROFESSIONAL AND ADVANCED STUDIES

* This is a computer system (Digital File) generated letter. Hence there is no need for a physical signature.