

A Secure Face–Fingerprint Dual-Biometric Staff Attendance System for Confluence University of Science and Technology, Osara

*¹Abraham Ayegba Alfa, ²Emmanuel Eturpa Salami, ¹Kharimah Bimbola Ahmed and ³Precious Bamiyo Metiboba

¹Department of Computer Science, Confluence University of Science and Technology, Osara, Kogi State, Nigeria.

²Department of Software Engineering, Confluence University of Science and Technology, Osara, Kogi State, Nigeria.

³Department of Cyber Security, Confluence University of Science and Technology, Osara, Kogi State, Nigeria.

*Corresponding authors' email: alfaaa@custech.edu.ng

ORCID ID: <https://orcid.org/0000-0001-5926-9520>

ABSTRACT

The paper presents the design, implementation, and evaluation of a secure dual-biometric staff attendance system for Confluence University of Science and Technology (CUSTECH), Osara. The methodology combined biometric acquisition and preprocessing, pretrained MobileNetV2, ResNet-50, and ViT-B/16 feature extractors, L_2 normalization, cosine-similarity matching, multimodal feature/score fusion, AES-256-GCM template cryptography, SHA-256 integrity safeguard, and SQLite-logging of grounded attendance data. Ten-subjects produced 10-genuine and 90-imposter verification pairs for the backbones. ResNet-50 showed the biggest general verification capability at accuracy of 0.77, EER of 0.2167, FAR of 0.2333, FRR of 0.20, decidability index of 1.565, and mean latency of 335.75 ms. MobileNetV2 produced the least latency of 207.93 ms, while ViT-B/16 attained accuracy of 0.72 and latency of 694.55 ms. ViT-B/16 revealed the greatest comparative performance against the backbone models. AES-256-GCM enlarged template storage from 10,368 to 10,396 bytes, with encryption times of 0.058 and decryption time of 0.098 ms; SHA-256 hashing time of 0.043 ms, and template recovery of 100%. Initial usability evaluation using 10 volunteers across 60 task observations gave task success of 98.30%, mean task time of 24.30 s, ease rating of 4.20/5, mean SUS score of 80.50/100, and no unrecoverable crashes. This research interconnects verification decisions to secure official records, which runs role-based access and exportable reports, and a reproducible basis for future edge deployment and larger-scale validation studies. The results demonstrate proof-of-concept feasibility while supporting larger-scale validation before deployment.

Received: 21 Sep. 2026

Accepted: 05 Oct. 2026

Published: 07 Oct. 2026

Keywords: Fingerprint, Face, Attendance, Dual-Biometric Recognition, Deep Learning, Security

INTRODUCTION

Biometric attendance systems leverage on physiological attributes of persons for its authentication operation by matching captured information against pre-existing templates. The drive towards automated attendance systems is partly caused by the ineffectiveness of the traditional modes like time-consumption, large secondary data capturing, and highly prone to manipulation and proxy attendance. The incorporation of biometric verification in verifying identity and approving access to restricted places is already common for digital systems (Aldabagh, 2024; Sodiq et al., 2025).

The foundational biometric theory and historical developments in fingerprint technology, system design methodologies as solutions to limitations of traditional attendance mechanisms including magnetic cards, manual registers, and password-based systems. These have demonstrated vulnerability to manipulation, inefficiency, and administrative burden. Biometric systems made it possible for organizational timekeeping management, better accuracy, efficiency and accountability (Calderón & Laurent, 2025).

The quest to develop accurate and robust attendance solutions heralded biometric systems during the 1990s, starting with fingerprint- and iris-based recognition approaches. Later in 2000s, facial recognition technology begun as a practicable substitute owing to the availability of high-resolution cameras, and growth of image processing algorithms (Vardhan et al., 2025)

Feature-level fusion correlates or concatenates feature vectors realised from autonomously from diverse biometric characters into a single, high-dimensional depiction preparatory to pattern matching processes. Tarafder et al. (2025) and Garg et al. (2025) alluded that feature fusion retains cross-modal correlations and rich discriminative details, producing higher recognition accurateness. Present-day biometric schemes have evolved from initially handmade minutiae/ texture descriptors (such as HOG, LBP, Gabor filters and SIFT) to deep neural networks. In effect, deep learning methods can autonomously extract translation-invariant and hierarchical illustrations inside raw images, exposing high robustness to and sensor noise, illumination shifts, and pose variations.

Pretrained CNN models like VGGFace2, ResNet-50, MobileNet, and EfficientNet are commonly deployed for fingerprint and facial feature extraction by leveraging on transfer learning approaches. Jena et al. (2021) assessed pretrained CNN frameworks with augmented and real-time fingerprint/face datasets. FaceNet variant attained greater facial feature extraction at training accuracy of 95.28%, and test accuracy of 92.05% against Xception and InceptionResNetV2 counterparts. Also, InceptionResNetV2 fused with the feature level and fingerprint embeddings attained training accuracy of 98.14%, testing accuracy of 96.26%, FAR of 0.0019% and EER of 1.87%.

Gimba et al. (2025) built a dual-branch CNN model for fingerprint (FVC2000/SOCOFing datasets) and face (Essex/Georgia Tech datasets) detection, which produced unimodal face accuracy of 99.66%, fingerprint accuracy of 100%, multimodal accuracy of 98.35%, and relatively smaller FAR at 0.001%. Tarafder et al. (2025) performed face embeddings with ResNet50/VGGFace2, and fingerprint embeddings with EfficientNet/ResNet, thereafter integrating L-2 normalization to project vectors/unit hypersphere to produce accuracy of 98.2% and outpaced single CNN architectures.

Sliding-window Swin Transformers and Vision Transformers (ViTs) takes advantage of self-attention mechanisms to extract extended-range contextual associations throughout biometric frames. Paul et al. (2025) conducted comparative performance analysis of ViT and ResNet-50 architectures in the case a dual-modal detection task of face and emotion. ResNet-50 underperformed ViT by an accuracy of 0.86 and AUC-ROC of 0.89 for face detection and an accuracy of 0.90 and AUC-ROC of 0.96 for emotion recognition.

Garg et al. (2025) utilized Swin Transformers/attention-augmented CNNs to capture local minutiae and texture features throughout fused fingerprint (SOCOFing), ECG (HEARTPRINT), and iris (IITD) datasets. It obtained detection accuracy of 99% for 199 subjects investigated.

Since biometric traits are permanently linked to identity of persons and cannot be reset upon compromise, protecting their raw template is critical. Hence, Jagadiswary & Saraswady (2016) proposed an RSA crypto-biometric framework by fusing retina, fingerprint, and finger vein characteristics at the feature level. The framework encrypted the fused feature vector to produced FAR of 0.01% and genuine acceptance rate (GAR) of 95.3%.

Chitrapu et al. (2026) combined Channel Attention (MN+CA), MobileNetV2, Trust-Adaptive Fusion and CKKS homomorphic cryptography for multimodal identity recognisance system. Fused embeddings (256-dimensional fingerprint and face) were scrambled and matched completely within the encrypted frame deprived of decryption. The encrypted similarity computation grabbed 110 ms (a rational 59.4 ms overhead against plaintext) to attain accuracy of 99.61%, EER of 0.0038%, and entire end-to-end authentication of 558.25 ms.

Recently, BioHashing, cancellable transformation functions (like Adaptive Vector Transformation), and cryptographic commitments (template hashed with SHA-256 and signed with private keys infrastructure) were applied identity management systems to guarantee biometric template unlinkability and revocability across databases. In terms of application of biometric for institutional campus attendance management, Mohammed et al. (2018) designed an educational business intelligence student recognition system combining video face recognition (HaarCascade+PCA and MS-SSIM motion detection) and active RFID tags to achieve attendance accuracy of 99.00% within 2.88 seconds, resolving RFID tag collision and removing proxy roll calls. Indhumathi et al. (2025) developed a two-step university attendance framework pairing edge-based facial recognition with contactless RFID scanning. Immutable decentralized blockchain ledger served protection against log attendance transactions database to obtain RFID accuracy of 99.8%, face detection accuracy of 98.5%, false positives of zero, and database tampering.

Bisht et al. (2025) developed a scalable client-server advanced access control system (AACS) fusing a MySQL database, JavaFX frontend, Eigenface/LBPH feature extraction for facial and fingerprint access. The system enabled real-time organisational lockdown and monitoring.

Deepthi et al. (2025) constructed a cardless locker access system by integrating Librosa MFCC voice vectors and OpenCV facial embeddings (128-D vectors). It was implemented using React, Flask, Firebase, ESP32 microcontroller to actuate physical solenoids in 2 – 3 seconds for triggering successful dual authentication. Sodiq et al. (2025) advanced biometric-based students attendance monitoring system at average recognition accuracy of 0.957 using Face API.JS deep learning facial recognition, and live video streams with Socket.IO for exchanges between Raspberry Pi module or mobile device. The privacy of stored records of students could be compromised by relying solely on face api.js. Again, student positioning affected the system accuracy. Facial recognition algorithms of SVM and Insightface models were integrated with IP Webcam from Python OpenCV to monitor attendance by (Osazuwa-Ojo & Eliagwu, 2024). It achieved 0.9878 accuracy, but ethical and security concerns persist.

Computerised attendance systems based on facial recognition and detection technology have been adopted and implemented in different scenarios like educational institutions, event venues, and workplaces (Shrivastava et al., 2025). These systems utilize biometric information, specifically facial features, to recognise persons and monitor their attendance events, which offer superior accuracy and efficiency when likened to manual methods like roll calls/sign-in sheets deployed in most educational institutions (Mishra, et al., 2022; Jha et al., 2023; Sodiq et al., 2025; Usiobaifo & Osaseri, 2025).

The aim of the paper is to propose a secure dual-biometric staff attendance system for CUSTECH, Osara, to addresses the weaknesses of the traditional attendance tracking process presently undertaken by the university by raising the accurate, efficiency, and security. The key contributions of the paper include:

- i. To design framework for capturing face and fingerprint details of the staff for CUSTECH, Osara.
- ii. To develop secure dual-modal biometric staff attendance system for the university.
- iii. To measure system performance, security effectiveness, and its usability in a pilot study.

MATERIALS AND METHODS

The framework for the proposed dual-biometric staff attendance system comprises biometric acquisition, preprocessing, deep-feature extraction, multimodal matching, template protection, and performance assessment into a unified authentication architecture.

Fingerprint and Face data are autonomously improved prior to being transformed into condensed discriminative embeddings using Transformer/convolutional neural network-grounded models. Afterward, early or late fusion is introduced to reveal matching information throughout the modalities.

Cryptographic safeguards and presentation-attack detection offer security reinforcements, whereas system performance is assessed using standard authentication parameters, latency profiling, and statistical separation measures.

Research Design

The paper adopted an applied experimental design strategy involving system development, biometric assessment, security testing, and usability evaluation. The system prototype combined fingerprint and face detection with pretrained ResNet-50, MobileNetV2, and ViT-B/16 frameworks, AES-256-GCM cryptography, SHA-256 hashing, and attendance administration. The system

performance was determined through recognition measures, template recovery, processing latency, security overhead, and user usability metrics.

System Architectural Design

The proposed system uses a multi-tier architecture based on client-server structure. The dual-biometric staff

recognition-based attendance monitoring system for the university staff is made up of the image acquisition module, biometric preprocessing module, security module (encryption/decryption), biometric feature template storage, deep learning processing module (features extraction and matching), and final decision model as shown in Figure 1.

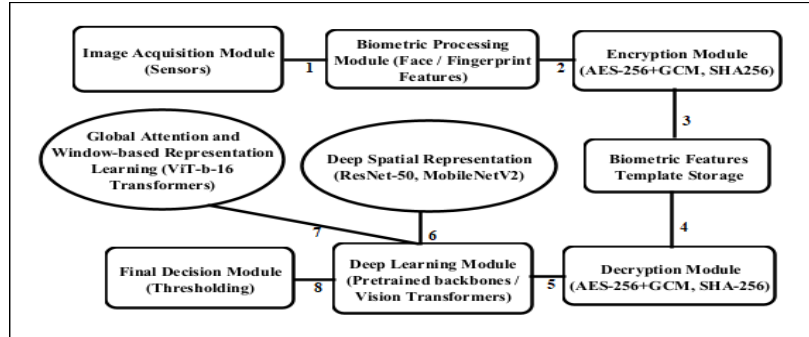


Figure 1: Layout design of the proposed attendance management system

Mathematical Formulation of Biometric and Security Methods

Given biometric sample serving as input (x_0) the pretrained deep-learning backbone, $d_\phi(\cdot)$ creates a feature embedding as indicated by Eq. 1:

$$v = d_\phi(x_0), \hat{v} = \frac{v}{\|v\|_2}, \quad (1)$$

Where, $\hat{v} = L_2$ -normalized embedding. The relative similarity index (C) within an enrolled template ($\hat{v}_e$) and a query template ($\hat{v}_q$) was calculated with the cosine similarity as given by Eq. 2:

$$C = \frac{\hat{v}_e^T \hat{v}_q}{\|\hat{v}_e\|_2 \|\hat{v}_q\|_2}. \quad (2)$$

And fingerprint (C_{fi}) and face (C_{fa}) scores were combined into the decision score (C_{fb}) using the expression provided by Eq. 3:

$$C_{fb} = (1 - \tau)C_{fi} + \tau C_{fa}, \quad 0 \leq \tau \leq 1. \quad (3)$$

The authentication is accepted if and only if $C_{fb} \geq \alpha$; where, α = the decision threshold.

In the case of biometric-template safeguard, AES-256-GCM with a 256-bit key (R), nonce (O), plaintext template (W), and discretionary accompanying data (a) to generate ciphertext (S) and authentication tag (t) as given by Eq. 4:

$$(S, t) = \text{AES.GCM}_R(O, W, a). \quad (4)$$

While authenticated reconstructed was expressed by Eq. 5:

$$W = \text{AES.GCM}_R^{-1}(O, S, a, t). \quad (5)$$

The GCM authentication tag offers authenticity and integrity, with necessary verification prior to accepting the reconstructed template. Additionally, SHA-256 was utilised to generate a fixed 256-bit integrity digest (j) as expressed by Eq. 6:

$$j = \text{SHA 256}(W), \quad j \in \{0, 1\}^{256}. \quad (6)$$

And template integrity was confirmed using the Eq. 7:

$$\text{SHA 256}(P') = J. \quad (7)$$

Where, W' = the reconstructed template.

Hence, the methodology fuses normalized deep-feature matching with authenticated encryption and cryptographic hashing to guarantee recognition, confidentiality, and integrity within the proposed attendance system.

System Use Case Diagram

The proposed system output offers the system user, and administrator the following functionalities: login (add users), start/end system (capture enrolment/attendance), record view/search/export (CSV, PDF, Excel formats), system backup as shown in Figure 2.

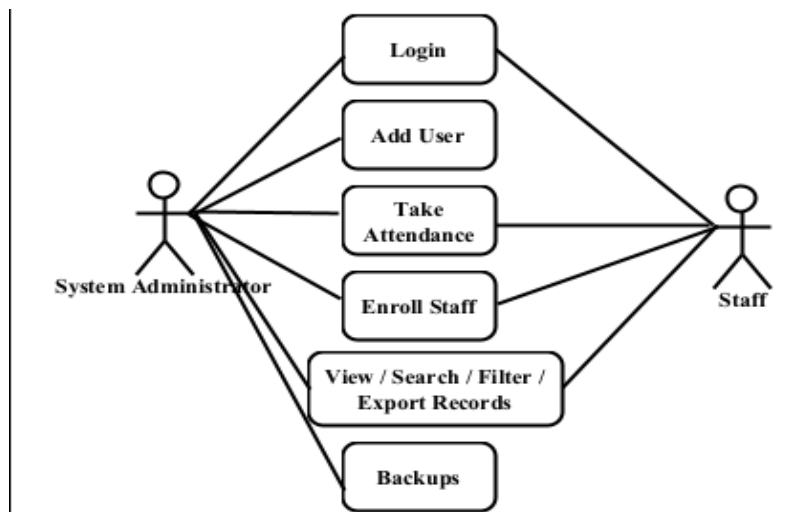


Figure 2: The proposed system use case diagram

Biometric Acquisition, Enrolment and Authentication Protocol

Fingerprint and Face data were acquired from 10 voluntary participants, containing 2 fingerprint and 4 facial images samples for each participant. Fingerprint samples were subgrouped 1/1 for enrolment and testing, whereas facial samples were separated into 2/1/1 for enrolment/validation/test sets.

Fingerprints were collected with ZKTeco ZK4500/ZKFingerprint scanner, while face images were acquired using USB 30 FPS Logitech C270 HD Webcam model. MobileNetV2, ResNet-50 and ViT-B/16 were used as pretrained feature extractors, and cosine similarity was applied to compare enrolled and query embeddings. Face and fingerprint matching scores were fused at weights and verification threshold of 0.50 in each case. The authentication was accepted when the fused score is greater than 0.75.

Biometric templates were protected using AES-256-GCM encryption and SHA-256 integrity hashing before storage in SQLite, with cryptographic keys managed programmatically at runtime and never embedded in biometric template dataset nor use of persistent production-grade key management for key storage/management service. Liveness/spoof detection was not evaluated in the present study and is kept during future implementation.

Fingerprint and face samples were converted into deep feature embeddings, which were stored after AES-256-GCM based encryption. SHA-256 digests were created to assist verification of integrity. In effect, the proposed system stored protected biometric representations as against unencrypted feature templates.

System Implementation Environment

The paper conducts a proof-of-concept of the proposed secure dual-biometric staff attendance system. The prototype was realised in Python through a desktop-based client architecture with OpenCV, PyTorch/TorchVision, SQLite, and a graphical user interface for enrolment, attendance capture, record management, and administration. ResNet-50, MobileNetV2, and ViT-B/16 were assessed as pretrained feature extractors for matching of biometric information. Fingerprint and face samples were captured from ZKTeco ZK4500/ZKFingerprint scanner, and USB 30 FPS Logitech C270 HD Webcam, and then processed through the system prototype, whereas Jetson Nano, R305, and UBio-X Pro signify the envisioned configuration of hardware for next embedded deployment rather than the framework utilised for all described experiments.

The system design describes both the physical and logical arrangements, in which the interactions between the users and the system are explained. The system designed is to adopt to the client architecture.

Biometric Dataset and Experimental Protocol

The study maintained the same numbers of participants for dual-biometric enrolment and testing for uniformity and consistency. Consequently, the experiment involved 10 subjects, with two fingerprint and four facial images samples acquired per subject, giving 20 fingerprint and 40 face images as detailed in Table 1.

Table 1: Experimental Partition and Biometric Dataset Composition

Parameter	Value
Number of subjects	10
Face samples per subject	4
Total face images	40
Fingerprint samples per subject	2
Total fingerprint images	20
Face enrolment/validation/test	2/1/1 per subject
Fingerprint enrolment/test	1/1 per subject
Face/fingerprint input size (pixel)	224 × 224
Backbones assessed	ResNet-50, MobileNetV2, ViT-B/16
Similarity quantity	Cosine similarity
Random seed	42
Training images	2 facial, 1 fingerprint (30 images)
Testing images	2 facial, 1 fingerprint (30 images)
Threshold score of face	≥ 0.70
Threshold score of fingerprint	≥ 0.70
Threshold fused score	≥ 0.75

From Table 1, the fingerprint samples were separated into enrolment and test sets, whereas facial samples were partitioned into enrolment (30 images), validation, and test sets (30 images). Images were handled by ResNet-50, MobileNetV2, then ViT-B/16 extracts pretrained feature, and L_2 -normalized embeddings were matched based on cosine similarity index. A static random seed of 42 was utilised to support reproducibility.

Verification leverages on cosine similarity between enrolled and query templates. Different-subject comparisons were taken as impostor pairs, while same-subject comparisons

were treated as genuine pairs. Fingerprint and face scores were fused prior to threshold-based authentication. The three backbones were evaluated using similar parameters like accuracy, FRR, FAR, EER, mean latency and decidability index.

System Testing Procedure

The practical allocation of the 10 test users for the proposed dual biometric staff attendance system is presented in Table 2.

Table 2: Real-Time Usability Testing User Allocation

Role	Staff	Operators	Administrators	Total
Count	8	2	2	10

As shown in Table 2, the tasks are premeditated to align with the role of users on the proposed system. *Operators* test login, enrolment, attendance, record search/filtering, and exports. *Staff users* test fingerprint/face check-in and check-out. *Administrators* test creation of user and backup. For each task, the tester documents the following: failure/partial/success; task time of completion; number of assistance events; number of errors; ease rating (1–5); tester comments. Every participant fills the standard 10-item SUS questionnaire after performing the allotted tasks, and the evaluation software automatically computes a usability score in the range of 0–100.

Ethical Approval and Informed Consent

The usability evaluation of the biometric-based attendance system recruited university staff voluntarily to participate. Partakers were told the research purpose of the survey, the forms of biometric data gathered, and the data usage intentions prior to their involvement. Documented informed permission was gotten from all partakers, and personal identifiable information was substituted with special IDs throughout the analysis phase. Ethical approval was sought from the Directorate of Research, Innovation, and Development (DRID), Confluence University of Science and Technology, Osara, Kogi State. Fingerprint and face templates were warehoused in encrypted manner and utilised entirely for the purposes of the proposed system's assessment and research.

RESULTS AND DISCUSSION

This section presents and discourses the performance of the proposed dual-biometric attendance system in terms of recognition accuracy, processing latency, template security, and usability. The interpretation of the results is accompanied with similar multimodal biometric research for the purpose determining the practical implications and weaknesses of the proposed system.

System Implementation Outputs

The dual-modal biometric attendance system was implemented as a Python-based desktop application integrating fingerprint and face recognition, attendance management, and administrative control. Biometric features were extracted using pretrained deep-learning models, normalized, and fused to support authentication decisions. Attendance records were stored in an SQLite database with date, time, biometric scores, and user details. The system also provided live face/fingerprint capture, face/fingerprint input, secure login, dashboard monitoring, backup, and CSV, Excel, and PDF export functions. The main system components are discussed as follows:

Secure user login interface: It provides controlled access to the attendance system by verifying and authenticating users' username and password previously registered during enrolment as illustrated in Figure 3. Thereafter, only valid users are granted access to the main functions of the system functions, thereby removing unapproved users or imposters to the university community. Moreover, the login mechanism offers user accountability by keep track of associated activities of active users' sessions across the diverse system components.

The image shows a web-based login interface. At the top center is a circular logo with a gear-like border and a blue and orange design. Below the logo, the text "Secure User Login" is displayed in a bold, blue font. Underneath this, a smaller line of text reads "Every application session requires an authenticated user." The form consists of two input fields: "Username" and "Password", each with a small icon of a person and a key respectively. Below these fields is a wide, light gray button with the word "LOGIN" in black capital letters.

Figure 3: Secure user login interface

User (administrator) system dashboard. It delivers summary of registered staff, daily check-ins, check-outs, staff attendance, and total records as illustrated in Figure 4. Also, it shows recent attendance events according to staff details,

event type, date, time, and fused biometric scores. The navigation panel empowers the administrator to access enrolment, attendance capture, view attendance records, and manage system functions.

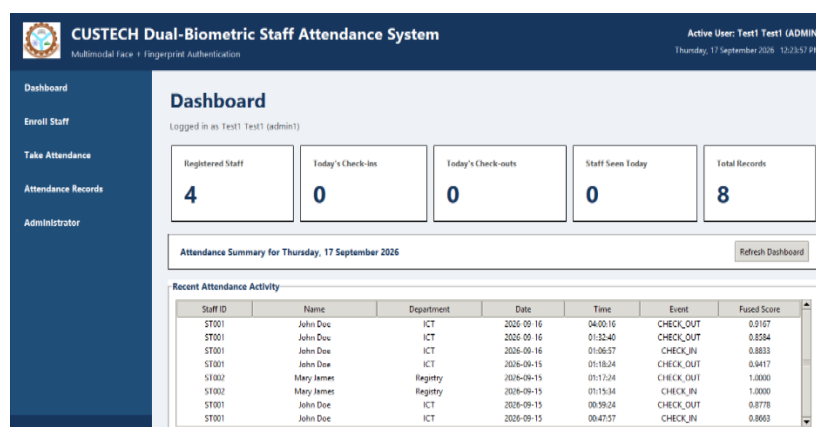


Figure 4: User (admin) system dashboard interface

Staff attendance enrolment subsystem: It captures staff identity particulars like staff ID, full name, and department as illustrated in Figure 5. Once more, it permits the system operator to capture/upload the corresponding fingerprint and face photograph images for biometric template generation as

system tolerance approach in case of equipment failure. The commit enrolment button saves the supplied staff information and biometric data to storage on the server for subsequent attendance verification and authentication operations.

CUSTECH Dual-Biometric Staff Attendance System
Multimodal Face + Fingerprint Authentication

Active User: Test1 Test1 (ADMIN)
Thursday, 17 September 2026 12:26:12 PM

Enroll Staff

Your existing enroll staff.py is retained. Use the form below to call it.

Staff ID

Full Name

Department

Face Photograph

Fingerprint Image

Browse

Browse

COMMIT ENROLLMENT

Operation Output

Figure 5: Staff attendance operation enrolment form

Staff attendance capturing subsystem: It integrates live facial and fingerprint captures to provide dual-biometric staff attendance authentication as indicated in Figure 6. It has buttons for starting, capturing, and stopping the camera, while displaying fingerprint scanner readiness for the selected

attendance event. After successful matching/attaining threshold set for the similarity index, the system inserts the attendance information and displays the confirmation window like staff identity, biometric scores, event type, and active operator details.

CUSTECH Dual-Biometric Staff Attendance System
Multimodal Face + Fingerprint Authentication

Active User: Test1 Test1 (ADMIN)
Wednesday, 16 September 2026 04:01:00 AM

Staff Attendance - Face + Fingerprint Verification

1. Live Face Capture

START CAMERA CAPTURE FACE STOP CAMERA

Camera status: stopped

Camera stopped

Click START CAMERA to resume.

2. Fingerprint & Attendance

Captured Face Preview

Fingerprint Sample

C:\Biometric_Project\data\enrollment\ST001_fp.png

BROWSE

Fingerprint scanner: SAMPLE READY

Attendance Event: CHECK_OUT

ATTENDANCE RECORDED

Staff ID: ST001
Name: John Doe
Department: ICT
Event: CHECK_OUT
Operator: Test1 Test1 (admin1)

Face Score: 0.8334
Fingerprint Score: 1.0000
Fused Score: 0.9167

START CAMERA CAPTURE FACE STOP CAMERA User: admin1 | Face + Fingerprint required

Biometric engine ready

COMMIT ATTENDANCE

Figure 6: Staff attendance capturing subsystem

Staff attendance records view/search/export subsystem: This interface displays recorded staff attendance according to staff identity, department, date, time, event type, and biometric matching scores as shown in Figure 7. Users can filter records by date, search terms, and view attendance event, with

options to clear or refresh the current view. Again, the subsystem offers option to export the displayed attendance records to several formats like PDF, Excel, and CSV for administrative and reporting uses.

CUSTECH Dual-Biometric Staff Attendance System
Multimodal Face + Fingerprint Authentication

Active User: Test1 (ADMIN)
Wednesday, 16 September 2026 16:11:22 AM

Attendance Records
Filter, review, refresh, and export attendance records directly from the institutional dashboard.

Date: Search: Event: ALL Apply Today Clear

Export Current View: EXPORT EXCEL EXPORT PDF EXPORT CSV 8 records REFRESH

Staff ID	Name	Department	Date	Time	Event	Face Score	Fingerprint Score	Fused Score	Oper
ST001	John Doe	ICT	2026-09-16	04:00:16	CHECK_OUT	0.8334	1.0000	0.9167	adm
ST001	John Doe	ICT	2026-09-16	01:32:40	CHECK_OUT	0.7109	1.0000	0.8284	N/A
ST001	John Doe	ICT	2026-09-16	01:06:57	CHECK_IN	0.7666	1.0000	0.8833	N/A
ST001	John Doe	ICT	2026-09-15	01:18:11	CHECK_OUT	0.8814	1.0000	0.9417	N/A
ST002	Mary James	Registry	2026-09-15	01:17:34	CHECK_OUT	1.0000	1.0000	1.0000	N/A
ST002	Mary James	Registry	2026-09-15	01:15:34	CHECK_IN	1.0000	1.0000	1.0000	N/A
ST001	John Doe	ICT	2026-09-15	00:59:54	CHECK_OUT	0.7507	1.0000	0.8778	N/A
ST001	John Doe	ICT	2026-09-15	00:47:57	CHECK_IN	0.7326	1.0000	0.8663	N/A

LOGOUT

Figure 7: Staff attendance records view/search/export subsystem.

Administrator controls interface: This delivers secured tools for handling system users, system institutional setups, and system backup as depicted in Figure 8. It enables designated administrators to enrol new system users by supplying their usernames, names, passwords, and designated

access roles. Also, this interface assists administrator in the branding of institutions and its operational backup, as well as controlling access, configuring system, and protecting data assets.

CUSTECH Dual-Biometric Staff Attendance System
Multimodal Face + Fingerprint Authentication

Active User: Test1 (ADMIN)
Thursday, 17 September 2026 12:21:50 PM

Administrator Controls
Manage user accounts, institutional branding, and system backups.

Users Institution / Logs Backup

Username:

Full Name:

Password:

Role: OPERATOR

CREATE USER

LOGOUT

Figure 8: Administrator controls interface

System Security-Engineering Performance

The security evaluation focused on safeguarding warehoused biometric templates and verifying the delicate attendance information's integrity. AES-256-GCM encrypted the biometric features vectors, and SHA-256 signed them by

generating fixed size cryptographic commitments for integrity checks. The evaluation measures include encryption and decryption time, successful template recovery, storage overhead, and hashing latency who's computed values are obtainable in Table 3.

Table 3: Security Performance of Biometric-Template Protection

Security Parameters	Value
Size of plain template (bytes)	10,368
Size of encrypted template (bytes)	10,396
Encryption time of AES-256-GCM (ms)	0.058477
Decryption time of AES-256-GCM (ms)	0.097743
hashing time SHA-256 (ms)	0.043437
Recovery success rate of encrypted template (%)	100.00

In Table 3, the security mechanisms of the biometric-template produced slight computational and storage costs. AES-256-GCM raised the size of template only marginally, from 10,368 - 10,396 bytes, whereas encryption procedure needed 0.058 ms and decryption required 0.098 ms. For SHA-256 hashing, 0.043 ms time was expended, and the template recovery rate of 100% established that the encrypted biometric information was properly recovered upon decryption procedure. The AES-256-GCM and SHA-256 outcomes indicated that biometric-template safekeeping could be realised with slight computational cost to support the practicality of secure multimodal verification and improving the secure fusion method in (Chitrapu et al., 2026).

The security outcomes compare constructively against previous biometric-protection studies with regards to computational cost. Jagadiswary and Saraswady (2016) utilised RSA-based safeguard to fused biometric features, while Chitrapu et al. (2026) applied CKKS homomorphic encryption and reported 110 ms encrypted similarity computation with an extra 59.4 ms overhead. Although the cryptographic objectives and experimental platforms vary, the present results demonstrate that authenticated template protection can be combined into the attendance prototype with relatively small processing and storage overhead.

Biometric-Recognition Performance

Table 4 summarizes the comparative verification performance of MobileNetV2, ResNet50, and ViT-B/16 under the same 10-subject cross-split protocol. The models are evaluated jointly using confusion-based measures, FAR,

FRR, EER, accuracy, decidability index, decision threshold, and mean latency to assess both biometric discrimination and computational efficiency. The performance metrics were taken together to assess the trade-off between recognition effectiveness and computational efficiency.

Table 4: Comparative Performance of Deep-Learning Backbones

Measure	MobileNetV2	ResNet50	ViT b/16
subjects	10	10	10
Genuine pairs	10	10	10
Impostor pairs	90	90	90
Decision threshold	0.893504	0.896324	0.853214
TP	7	8	7
TN	66	69	65
FP	24	21	25
FN	3	2	3
FAR at threshold	0.266667	0.233333	0.277778
FRR at threshold	0.3	0.2	0.3
EER	0.283333	0.216667	0.288889
Accuracy at threshold	0.73	0.77	0.72
Decidability index	1.47142	1.565068	1.502261
Mean latency (ms)	207.9265	335.7463	694.5505

Table 4 presents the joint interpretation of recognition accuracy, EER, decidability, verification errors, and computational latency for the three pretrained backbones. Firstly, ResNet50 produced the strongest general verification performance by achieving the largest accuracy of 0.77, least EER of 0.2167, lowest FAR of 0.2333, lowest FRR of 0.20, and biggest decidability index of 1.565. It correctly accepted 8/10 genuine comparisons and rejected 69/90 impostor comparisons. Secondly, MobileNetV2 attained marginally smaller discrimination, with accuracy of 0.73, EER of 0.2833, and decidability of 1.471, nonetheless delivered the smallest mean latency of 207.93 ms. Lastly, While ViT-B/16 realised considerable discrimination at decidability of 1.502; it produced the biggest EER of 0.2889, FAR of 0.2778, and significantly larger latency of 694.55 ms.

When taken together, these outcomes signify a strong compromise between recognition efficiency and computational overhead. ResNet50 ran the most stable performance, whereas MobileNetV2 is ideal for quicker processing and ViT-B/16 imposed the largest computational cost whose verification accuracy did not improve during this

pilot assessment. The values of EER remain extensive in absolute terms, which shows that the pretrained models are not yet appropriate for deployment-grade authentication. Since the evaluation utilised only 10-subjects, 10 genuine pairs, and 90 impostor pairs.

The recognition performance is lower in absolute terms than the values reported by Jena et al. (2021), Gimba et al. (2025), and Tarafder et al. (2025), who reported multimodal accuracies above 96% under larger and differently configured datasets. Unlike Paul et al. (2025), where ViT outpaced ResNet-50, ResNet50 achieved better than ViT-B/16 in the present experiment, showing that backbone performance is sensitive to dataset size, enrolment protocol, threshold calibration, and task-specific fine-tuning. The current results should therefore be interpreted as a preliminary comparative assessment rather than a deployment-scale benchmark.

In similar representations, Figures 11 and 12 depict the comparative evaluation curves of MobileNetV2, ResNet-50 and ViT-B/16 for FAR and FRR measures, which was conducted on the 10-subject biometric dataset using the same enrolment and test partitions for all models.

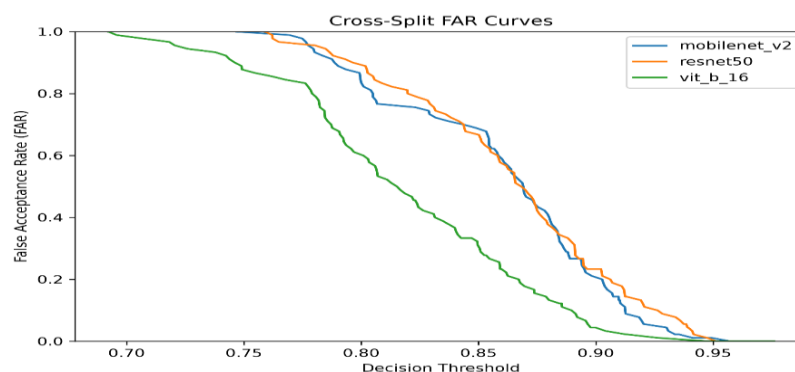


Figure 11: Cross-split FAR curves of the compared backbones

Figure 11 shows how the False Acceptance Rate (FAR) differs as the decision threshold for MobileNetV2, ResNet50, and ViT-B/16. In three models, FAR decreases as the threshold increases since stricter acceptance conditions lessen the chances of incorrectly accepting an impostor. Throughout

most of the common threshold range, ViT-B/16 displays a lesser FAR than MobileNetV2 and ResNet50, signifying stronger rejection of impostor comparisons at equal thresholds. MobileNetV2 and ResNet50 produce generally

analogous FAR movements, mostly between thresholds of 0.85 and 0.90.

This figure is noteworthy as it reveals that biometric performance relies strongly on the chosen operating threshold, as against accuracy value Soley. Though raising the threshold lessens false acceptances, it could at the same time upsurge false rejections; therefore, it should be considered together with the matching FRR curve and EER outcomes. The observable variances among the curves added to claim that each backbone needs fitting calibration of threshold to attain a suitable stability between security and genuine-user accessibility.

Figure 12 illustrates the discrepancy of the False Rejection Rate (FRR) against decision threshold for the backbone models (MobileNetV2, ResNet50, and ViT-B/16). Contrary

to FAR, FRR rises as the threshold becomes highly strict since a bigger share of genuine users fail to meet the acceptance criterion. ResNet50 mostly upholds a lesser FRR across most of the mid-threshold section, while ViT-B/16 starts rejecting genuine comparisons at reasonably lower thresholds and indicates a sharper rise in FRR.

It demonstrates the real-world trade-off in threshold choices in which a larger threshold rallies rejection of impostor nonetheless legitimate user could be denied in the process. Consequently, the FRR curves should be considered together with the FAR curves and the matching EER values. In general, the outcomes confirm that calibration of threshold is key for harmonising security of system and accessibility of user, with ResNet50 delivering the most balanced verification behaviour in the present pilot assessment.

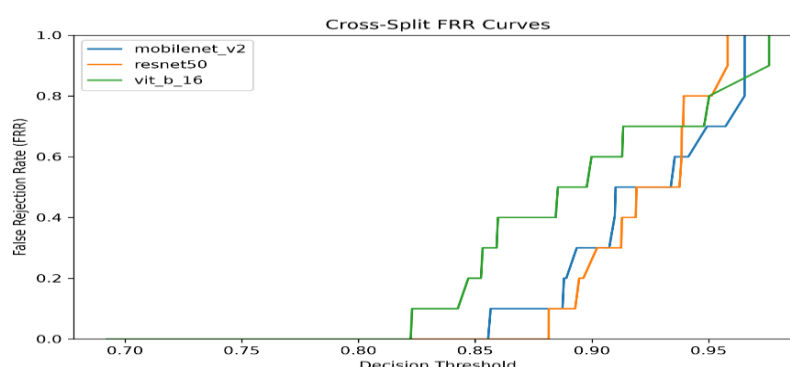


Figure 12: Cross-split FRR curves of the compared backbones

ViT-B/16 displayed the strongest relative recognition performance, while MobileNetV2 attained the least inference latency. These measures explain the computational efficiency and recognition capability of the biometric models as against the stored templates security. Therefore, these outcomes should be considered as a pilot assessment about the suitability of models, which is not a validation accuracy of

deployment-ready biometric attendance system as in the case of ViT-B/16.

System Usability Evaluation Outcomes

The outcomes of system usability assessment conducted for 10 volunteer staff-testers of the university throughout 60 task observations are summarized in Table 5.

Table 5: Summary of System Usability Evaluation Outcomes

Parameter	Outcome
Number of testers	10
Task observations	60
Total observed errors	31
Mean task time (s)	24.30
Median attendance transaction (s)	21.10
Average ease rating	4.20/5.00
Complete task success	59/60 (98.30%)
Assistance-event rate	7/60 (11.67%)
Unrecoverable crashes	NIL
Average SUS score	80.50/100
Median SUS score	82.50/100
SUS range	72.50 – 85.50

In Table 5, the initial usability confirmation further produced task success rate of 98.3%, average task time of 24.30 s, ease rating of 4.20/5, and average SUS score of 80.50/100, which reveals positive user acceptance and operational firmness. Contrasting previous attendance systems like one proposed by Mohammed et al. (2018), the proposed system syndicates dual-biometric verification, cryptographic template safekeeping, administrative reporting and control within a single institutional framework. Other existing attendance studies mostly focused on recognition accuracy and transaction effectiveness; for example, Mohammed et al.

(2018) reported 99% attendance accuracy, while Sodiq et al. (2025) reported an average recognition accuracy of 0.957. This study spreads the assessment by examining user interaction, 98.30% task completion, a mean task time of 24.30 s, an average ease rating of 4.20/5, and a mean SUS score of 80.50/100, with no unrecoverable crashes. These usability findings are preliminary because only 10 volunteers participated, but they provide initial evidence that the integrated biometric, security, and administrative functions can be operated effectively in an institutional setting. A larger

and more complex user study is essential for confirmatory usability validation.

Limitation of the Study

The biometric evaluation involved only 10 subjects, which confines the generalizability of the recognition outcomes to a greater university population. Upcoming studies must utilise greater and more varied datasets.

The paper relied on pretrained feature extractors short of task-specific optimization/fine-tuning, and liveness detection was not empirically assessed. Subsequent studies could take on presentation-attack detection, model hyperparameter optimization, and complete validation on the planned embedded hardware platform.

CONCLUSION

This paper presents a proof-of-concept of secure dual-biometric staff attendance system that incorporates fingerprint and face recognition with multimodal fusion, deep-learning models, cryptographic template security, and institutional attendance operation. The initial comparative assessment indicated that ViT-B/16 posted the biggest recognition performance, while MobileNetV2 offered the smallest processing latency, confirming the compromise between biometric discrimination and computational efficiency. The security assessment further disclosed that AES-256-GCM and SHA-256 incorporation produced nominal processing and storage overhead, which make them fit for secure real-time implementation.

These proof-of-concept results agree with former reports by Jena et al. (2021), Gimba et al. (2025), and Chitrapu et al. (2026) that that multimodal biometric fusion advance recognition robustness and security. Aside recognition effectiveness, the preliminary system usability testing revealed strong operational usability by attaining task success rate of 98.30%, median attendance transaction time of 21.10 s, average ease rating of 4.20/5, and 80.50/100 mean SUS score. There were no observable unrecoverable crashes throughout the entire 10-user evaluation records.

The contribution of research is the integration dual-biometric verification, comparative deep-learning evaluation, cryptographic template security, real-time attendance capture, record export, user management, and backup as a single institutional platform. These initial outcomes offer a stronger groundwork for improving attendance accountability, integrity, and administrative efficiency in universities and other organizations by leveraging on biometric methods. Liveness detection is retained for upcoming deployment and was excluded in the present experimental assessments.

Acknowledgement

Authors wish to appreciate the complete research funding provided by the Tertiary Education Trust Fund (TETFUND) through the Institutional Based Research (IBR) Grant, reference number: TETF/DR&R/CE/UNI/Osara/IBR/2025/VOL 1/19.

REFERENCES

Aldabagh, M. (2024). A review of students' attendance management systems. *Eurasian Journal of Science and Engineering*, 10(3), 136-145. <https://doi.org/10.23918/eajse.v10i3p13>

Bisht, M. S., Aman, A., Singh, S. K., Gupta, J., & Singh, S. (2025). Automated access control system using biometric authentication technologies. In *2025 8th International*

Conference on Circuit, Power & Computing Technologies (ICCPCT) (pp. 1329-1334). IEEE. <https://doi.org/10.1109/ICCPCT65132.2025.11176610>

Calderón, L. F., & Laurent, A. (2025). Fingerprint-based attendance systems in organizational governance: A comprehensive theoretical, methodological, and empirical examination. *The Parthenon Frontiers of Emerging Data Science and Machine Learning*, 2(1), 13-18. <https://www.parthenonfrontiers.org/index.php/ejedsml/article/view/402>

Chitrapu, P., Morampudi, M. K., & Kalluri, H. K. (2026). A secure and explainable multimodal biometric system using trust adaptive fusion for face and fingerprint. *Scientific Reports*, 16(1), 14244. <https://doi.org/10.1038/s41598-026-43252-x>

Deepthi, L., Shetty, A. P., Shetty, S. S., Vaishnavi, K. S., & Manvitha, M. V. (2025). A multimodal biometric approach for physical locker security: integration of face and voice. In *2025 Third International Conference on Networks, Multimedia and Information Technology (NMITCON)* (pp. 1-6). IEEE. <https://doi.org/10.1109/NMITCON65824.2025.11187497>

Garg, R., Pathak, P., & Singh, M. P. (2025). Multimodal biometric system combining Fingerprint, Iris, and ECG using convolutional attention frameworks. *Systems and Soft Computing*, 7, 200369. <https://doi.org/10.1016/j.sasc.2025.200369>

Gimba, U. A., Ariffin, N. A. B. M., Udzir, N. I., & Sani, N. F. M. (2025). Enhancing biometric authentication through multimodal approach combining face and fingerprint recognition using convolutional neural networks (CNN). *Discover Computing*, 28, 246. <https://doi.org/10.1007/s10791-025-09775-z>

Indhumathi, P., Aarthi, K., Saravanan, D., & Yogeshwaran, K. (2025). Two-step attendance system with RFID and facial recognition. In *2025 International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 109-115). IEEE. <https://doi.org/10.1109/ICICCS65191.2025.10984920>

Jagadiswary, D., & Saraswady, D. (2016). Multimodal Biometric Authentication System Using Fingerprint, Retina and Finger Vein. *Procedia Computer Science*, 85, 109-116. <https://doi.org/10.1016/j.procs.2016.05.187>

Jena, P. P., Kattigenahally, K. N., Nikitha, S., & Sarda, S. (2021). Multimodal biometric authentication: Deep learning approach. In *2021 International Conference on Circuits, Controls and Communications (CCUBE)* (pp. 1-5). IEEE. <https://doi.org/10.1109/CCUBE53681.2021.9702724>

Jha, P. B., Basnet, A., Pokhrel, B., Pokhrel, B., Thakur, G. K., & Chhetri, S. (2023). An automated attendance system using facial detection and recognition technology. *Apex Journal of Business and Management*, 1(1), 103-120. <https://doi.org/10.61274/apxc.2023.v01i01.008>

Mishra, A. K., Nepal, A., & Aithal, P. S. (2022). Industry 4.0 concept for Nepal - operating virtual farming industry. In Krishna Prasad, K., P. S. Aithal, & A. Jayanthiladevi (ed.), *Proceedings on Future Trends in ICCT and its Applications*

- in *IT, Management and Education* (pp. 31-35). IEEE. <https://doi.org/10.5281/zenodo.7215189>
- Mohammed, K., Tolba, A. S., & Elmogy, M. (2018). Educational business intelligence 3.0: multimodal student identification and attendance management system. *Ain Shams Engineering Journal*, 9(4), 2917–2929. <https://doi.org/10.1016/j.asej.2018.08.002>
- Omari, A. I., & Jaradat, A. (2020). Attendance tracking systems: A review of the literature. *International Journal of Advanced Computer Science and Application*, 11(4), pp. 194–202.
- Osazuwa-Ojo, V. O., & Elaigwu, V. O. (2024). A two-step authentication facial recognition system for automated attendance tracking. *FUDMA Journal of Sciences*, 8(6), 7–16. <https://doi.org/10.33003/fjs-2024-0806-2773>
- Paul, J., Mitra, A., Kulhadiya, D., Pawar, T., Roy, A., & Sil, J. (2025). A comprehensive approach to real-time attendance systems: Integrating face recognition and emotion detection and with web technologies. *Procedia Computer Science*, 258, 3436–3446. <https://doi.org/10.1016/j.procs.2025.04.600>
- Shrivastava, A., Suji Prasad, S. J., Yeruva, A. R., Mani, P., Nagpal, P., & Chaturvedi, A. (2025). IoT based RFID attendance monitoring system of students using Arduino ESP8266 & Adafruit.io on defined area. *Cybernetics and Systems*, 56(1), 21–32. <https://doi.org/10.1080/01969722.2023.2166243>
- Sodiq, K., Kazeem, S., Adetunji, O., Saliu, A., Oyerinde, E., Salau, S., Ojosipe, A., Pelumi, I., Nofisat, A., Wisdom, U., & Akinfe, O. (2025). Development of a scalable and real-time biometric-based attendance monitoring system. *FUDMA Journal of Sciences*, 9(12), 590–598. <https://doi.org/10.33003/fjs-2025-0912-4243>
- Tarafdar, R., Singh, H., Pahuja, V., Garg, G., Sivaraman, R., & Jegajothi, B. (2025). DL-based multi-modal biometric authentication for next-gen secure AI systems. In *2025 5th International Conference on Soft Computing for Security Applications (ICSCSA)* (pp. 12–19). IEEE. <https://doi.org/10.1109/ICSCSA66339.2025.11170949>
- Usiobaifo, A. R., & Osaseri, R. O. (2025). Design and implementation of a mobile fingerprint attendance system for student and lecturers. *FUDMA Journal of Sciences*, 9(5), 232–238. <https://doi.org/10.33003/fjs-2025-0905-3136>
- Vardhan, R., Aftab, S., Sanyal, N., Ali, K., & Kumar, A. (2025). Automated attendance system using facial recognition: a comprehensive review. In S. Mishra, A. K. Singh, & P. Prajapati (Eds.), *Challenges and Opportunities for Innovation in India* (pp. 117–122). CRC Press. <https://doi.org/10.1201/9781003606260-20>

