



Research Article

Enhanced Access Control Management System in an Edge Computing Environment Using Bimodal Biometrics Technique

Paul Ndudiri Ohia^{1,*} , Friday Eleonu Onuodu¹ , Ugochi Adaku Okengwu² 

¹Department of Information Technology, University of Port Harcourt, Port Harcourt, Nigeria

²Department of Computer Science, University of Port Harcourt, Port Harcourt, Nigeria

Abstract

This study presents an enhanced access control management system for edge computing environments using bimodal biometrics, contextual risk analysis, and Chinese Wall policy enforcement. The work addresses a limitation in context-only access control frameworks, namely their inability to confirm that the person requesting access is the genuine enrolled user. To close this identity-verification gap, the proposed system integrates face recognition, fingerprint recognition, and contextual decision support into a unified edge-aware authentication workflow. The implementation was developed in Python using Flask, with MySQL for transactional data storage and IPFS for content-addressed storage of biometric-related artifacts. A hybrid dataset strategy was adopted. Public datasets such as VGGFace2 and SOCOFing supported preliminary experimentation, while locally captured biometric samples were emphasized for operational training and evaluation in order to reduce domain mismatch. A one-dimensional convolutional neural network was used for contextual access analysis, while transfer-learning-based convolutional neural networks were used for face and fingerprint recognition. The datasets were split into 70% training and 30% testing. Experimental results showed strong performance for the biometric and contextual modules. The face model achieved about 0.96 accuracy, the fingerprint model achieved about 93.36% classification accuracy with 95.83% precision, recall, and F1-score for the enrolled-user fingerprint class, and the contextual Conv1D model achieved 84.08% test accuracy. System-level testing further showed that integrating biometric evidence with contextual intelligence and policy enforcement improved access-decision reliability over the earlier context-only model. The study concludes that combining bimodal biometrics with edge-based contextual reasoning can provide stronger identity assurance, better real-time responsiveness, and more dependable access control for distributed computing environments.

Keywords

Edge Computing, Bimodal Biometrics, Access Control, Fingerprint Recognition, Face Recognition, Contextual Risk Analysis, Chinese Wall Policy, Ipfs

*Correspondence: Paul Ndudiri Ohia (Paul.ohia@uniport.com.ng)

Received: 15 September 2026; **Accepted:** 24 September 2026; **Published:** 14 October 2026



Copyright: © The Author(s), 2026. Published by Science Publishing Group. This is an **Open Access** article, distributed under the terms of the Creative Commons Attribution 4.0 License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

1. Introduction

Access control remains a fundamental security requirement in distributed systems because it determines who can access protected resources, under which conditions, and at what privilege level. In edge and IoT environments, this requirement becomes more demanding because users, devices, and services operate across heterogeneous and latency-sensitive infrastructures [1-3]. Modern Zero Trust thinking further emphasizes that access should not be granted merely because a requester appears to be in a familiar location or on a trusted network; identity, device posture, and request context should all be evaluated explicitly before access is approved [4].

Although context-aware access control improves risk sensitivity, context alone does not always prove that the requester is the legitimate enrolled user. A trusted device, expected login time, or familiar location may still be exploited by an impostor. This study therefore extends a context-driven framework by adding bimodal biometric verification through face and fingerprint recognition, while retaining contextual reasoning and policy enforcement. The proposed system is intended to support low-latency decision making at the edge while improving resistance to impersonation, credential misuse, and unauthorized access [5-7].

2. Related Works

Related works on access control have proposed policy-based and attribute-based methods for controlling access in distributed systems. Attribute-Based Access Control (ABAC) improves flexibility by evaluating user, resource, action, and environmental attributes before granting access [8]. More recently, adaptive and risk-aware models have been introduced for access control at the network edge. Muhammad et al. proposed an adaptive risk-based access control system for edge environments, using contextual factors such as resource sensitivity, action severity, and risk history to determine whether access should be granted or denied [9]. However, such context-based systems may still be limited because they do not always verify whether the requester is the real authorized user. This creates a gap for biometric-enhanced access control, where face and fingerprint verification can strengthen identity assurance before edge-based access decisions are finalized [6]. Within this setting, the key research gap is not the absence of contextual risk analysis, but the absence of strong identity assurance inside context-aware access workflows. The proposed

study addresses this gap by combining biometric identity evidence with contextual and policy-based reasoning in a unified edge architecture.

2.1. Access Control at the Network Edge

Access control at the network edge has become important because edge computing moves computation, storage, and security decisions closer to users, devices, and data sources. In this architecture, the Device Layer generates access requests through sensors, smartphones, biometric scanners, and IoT devices; the Edge Layer performs local authentication, risk evaluation, and policy enforcement; while the Cloud Layer supports long-term storage, model updates, and centralized management [10]. Prior studies show that edge computing reduces latency and supports real-time decision-making, but its distributed structure also increases exposure to threats such as unauthorized access, compromised nodes, spoofing, and data leakage [2, 3]. Recent work on edge computing highlights the need to move security decisions closer to users and devices in order to reduce latency and support real-time services [2, 3]. At the same time, the distribution of computation across exposed edge nodes introduces new concerns for authentication, privacy, and policy enforcement. These concerns make adaptive and identity-sensitive access control more important than purely static credential checks [1, 4].

2.2. Edge Computing Architecture

Edge computing brings computation and data storage closer to end-user devices and data sources instead of relying only on distant cloud servers [11, 12]. In an access-control environment, data from cameras, sensors, smartphones, and biometric scanners can be processed near the source, reducing latency, bandwidth use, and response time [11]. The architecture can be viewed in three layers: Device Layer, where biometric scanners, cameras, sensors, and user devices generate access data; Edge Layer, where gateways or edge servers process biometric and contextual information for real-time access decisions; and Cloud Layer, where large-scale storage, model updates, backup records, and long-term analytics are maintained. This layered approach supports fast, secure, and responsive biometric access control in edge environments [10].

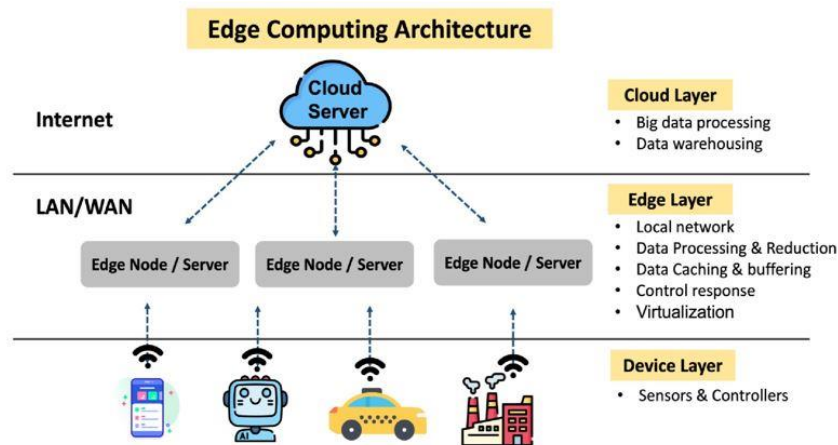


Figure 1. Edge computing architecture adapted from XenonStack [13].

2.3. Biometric System Theory

Biometric systems theory is based on the idea that individuals can be identified through measurable physiological or behavioral traits such as fingerprints, facial features, iris patterns, voice, and other unique human characteristics [14]. Unlike passwords, cards, or tokens, biometric traits are directly linked to the individual and are more difficult to forget, share, steal, or duplicate. This makes biometrics useful for secure identity verification in access-control systems [15]. The theory also emphasizes that effective biometric traits should possess qualities such as uniqueness, permanence, collectability, and reliability [16].

2.3.1. Biometric Technology

Biometric technology refers to the use of unique physiological or behavioural characteristics to identify or verify an individual. It converts human traits into digital templates that can be stored, matched, and used for authentication or registration [14]. Unlike passwords or access cards, biometric features are directly linked to the person, making them useful in security, law enforcement, banking, healthcare, border control, and access-management systems [15]. Commonly used biometric technologies include fingerprint recognition, face recognition [18], iris recognition, voice recognition, palmprint recognition, hand geometry, signature recognition, and behavioural biometrics such as keystroke dynamics and gait. Among these, fingerprint and face recognition are widely adopted because they are relatively easy to capture, cost-effective, and suitable for real-time authentication [16].

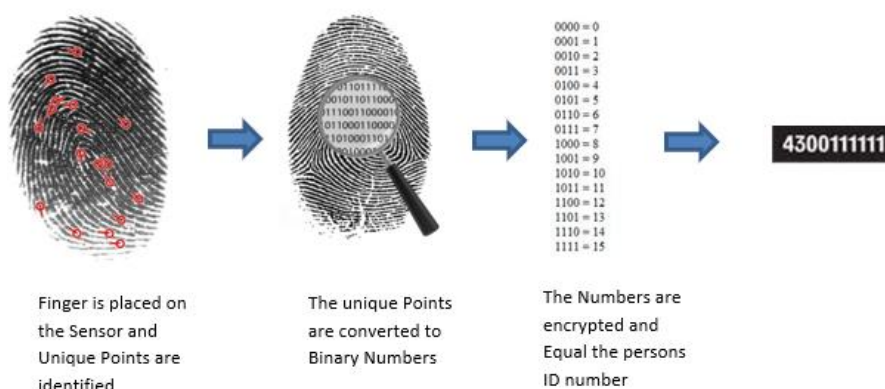


Figure 2. Fingerprint recognition process adapted from Maltoni et al. [17].

Bimodal biometric authentication combines complementary physiological evidence in order to reduce the weaknesses of unimodal verification. In this study, face recognition supported convenient and contact-light identity capture, while fingerprint recognition supplied a more stable and distinctive

physiological factor. This design aligns with biometric theory and with recent multimodal authentication studies that seek stronger resilience against spoofing and identity misuse [6, 7, 15, 16].

2.3.2. Edge Computing and Biometric Authentication Systems

Edge computing has become important in biometric authentication systems because identity verification often requires fast, secure, and reliable processing. Traditional cloud-based biometric systems may experience high latency, network dependence, and privacy concerns when raw biometric data must be transmitted to remote servers. By processing biometric data closer to the user, edge computing reduces response time, limits unnecessary data transmission, and supports real-time access-control decisions [11, 12].

In bimodal biometric systems, edge devices can process facial and fingerprint data locally using deep learning models. Convolutional Neural Networks (CNNs) are useful for this purpose because they can extract discriminative features from biometric images. Lightweight CNN architectures such as MobileNetV2 and EfficientNetB0 are suitable for edge environments because they are computationally efficient and can support faster recognition on resource-constrained devices [19, 20].

2.4. Machine Learning Models

Machine learning models improve access-control systems by enabling them to learn from historical data, detect patterns, assess contextual risk, and support adaptive decision-making. Instead of relying only on static rules, ML-based access control can evaluate factors such as user behavior, device trust, access history, and abnormal activity before granting or denying access [21, 22]. In this study, CNN-based models were applied to biometric recognition, while a 1D CNN/Conv1D model was used for contextual access-risk analysis.

2.4.1. Convolutional Neural Network

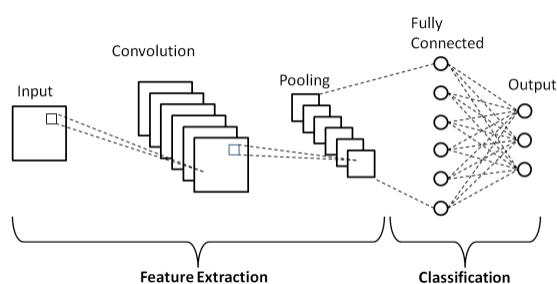


Figure 3. Structure of convolutional neural network (CNN).

A Convolutional Neural Network (CNN) is a deep learning model widely used for image processing, feature extraction, and pattern recognition. In the proposed enhanced access-control system, CNN models served as the core biometric recognition engines for processing face and fingerprint images. The CNN extracts discriminative features from biometric samples and converts them into numerical representations for identity verification

[23]. Its main components include the input layer, convolutional layer, ReLU activation layer, pooling layer, fully connected layer, and softmax/output layer. In this study, MobileNetV2 was used for facial recognition, while EfficientNetB0 was used for fingerprint recognition because both architectures support efficient image-based feature learning [19, 20].

2.4.2. Transfer Learning Models

Transfer learning models were used to adapt pretrained convolutional networks to the biometric recognition tasks. In this study, MobileNetV2 supported face recognition because of its lightweight inverted residual structure, while EfficientNetB0 supported fingerprint recognition through balanced depth, width, and resolution scaling. These models reduced training cost and improved feature extraction for the locally captured biometric samples.

2.5. Edge Computing Deployment Models

Edge computing can be deployed in different ways depending on where computation and storage resources are placed. In a device-edge model, processing is performed directly on smart devices, sensors, cameras, or biometric scanners with limited dependence on external servers. In an edge-server model, nearby gateways, routers, or local edge servers handle real-time processing, authentication, and access-control decisions close to users. In a cloud-edge collaborative model, urgent tasks are processed at the edge, while the cloud supports large-scale storage, model training, backup, and long-term analytics [11, 24]. This layered deployment approach is suitable for biometric access control because identity verification and risk analysis can be performed quickly at the edge, while records and system updates can still be managed through the cloud.

2.5.1. Benefits of Edge Computing

Edge computing provides several benefits for real-time access-control systems. It reduces latency by processing data close to the source instead of sending every request to a distant cloud server. It reduces bandwidth consumption because only selected or processed data is transmitted to the cloud. Edge computing improves privacy by allowing sensitive biometric and contextual data to be processed locally. It supports faster decision-making, which is important for security systems that require immediate grant, step-up, or deny responses [11, 12]. In the proposed system, these benefits allow biometric verification, contextual risk analysis, and policy enforcement to occur close to the access point.

2.5.2. Edge Deployment Considerations

Edge deployment also requires attention to hardware capacity, model size, latency, network availability, storage protection, and privacy. For biometric access control, these considerations are important because face and fingerprint evidence

must be processed quickly while preventing unnecessary exposure of sensitive biometric data.

3. Materials and Methods

The study adopted an object-oriented analysis and design methodology for developing the proposed access-control system. This methodology was suitable because the system consists of interacting entities such as users, biometric inputs, access requests, edge nodes, risk-analysis modules, policy enforcement components, and administrative records. The approach supported clear modelling of system actors, workflows, data objects, and decision processes before implementation. The proposed prototype was implemented as a web-based access-control platform using Python and Flask, with MySQL for structured records and IPFS for content-addressed storage of biometric-related artifacts [25].

3.1. Proposed System Architecture

The proposed system architecture was implemented as an

edge-aware web application using Python and Flask. MySQL stored structured entities such as users, biometric labels, access logs, contextual records, and historical access decisions, while IPFS stored biometric-related artifacts using content-addressed identifiers. The intelligence layer of the system integrated MobileNetV2 CNN for facial recognition, EfficientNetB0 CNN for fingerprint recognition, and a 1D CNN/Conv1D model for contextual risk analysis. These models worked together to verify user identity, analyze access conditions, and support real-time decision-making at the edge. During an access request, the face and fingerprint models generated biometric confidence scores, while the contextual model evaluated attributes such as device trust, login time, known location, resource sensitivity, and access history. The system then combined biometric evidence, contextual risk output, and policy restrictions to produce a grant, step-up, or deny decision. This combination allowed the system to provide transactional control, biometric identity assurance, contextual risk evaluation, policy-aware authorization, and verifiable storage of sensitive supporting files [25]. Figure 2 shows the main architecture of the proposed system.

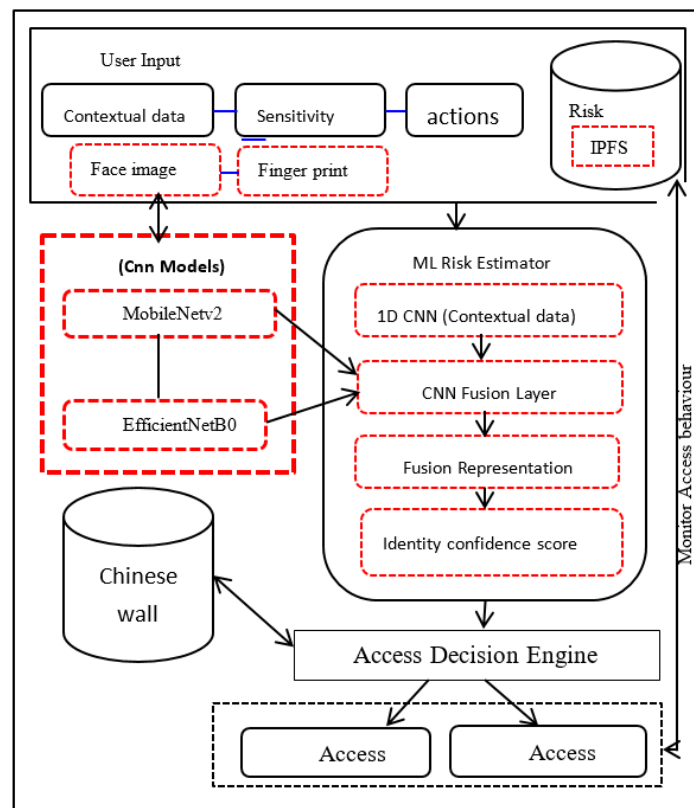


Figure 4. Proposed system architecture for the edge-based bimodal biometric access-control framework.

3.2. Dataset Analysis

The study used both public and locally captured datasets to

develop the proposed bimodal biometric access-control system. VGGFace2 and SOCOFing supported early experimentation with face and fingerprint recognition, while locally captured enrolled-user samples were used for the final operational training to reflect the real deployment environment [26, 27].

Face and fingerprint data were organized into identity-based folders for supervised learning, while contextual access records were prepared as tabular feature vectors for risk analysis. Preprocessing involved image resizing, normalization, labeling, contextual data cleaning, encoding, scaling, and class balancing. The datasets were split into 70% training and 30%

testing. Evaluation was based on accuracy, precision, recall, F1-score, confusion matrices, and functional system testing to confirm support for identity verification, risk evaluation, and real-time edge-based access decisions.

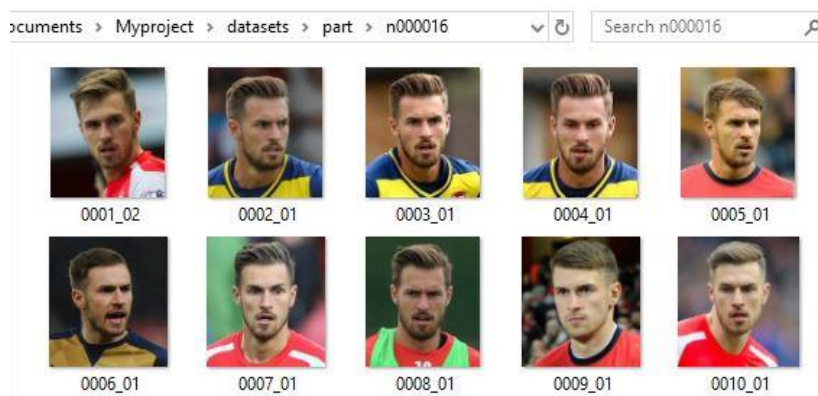


Figure 5. Public face image dataset (VGGFace2 from Kaggle).

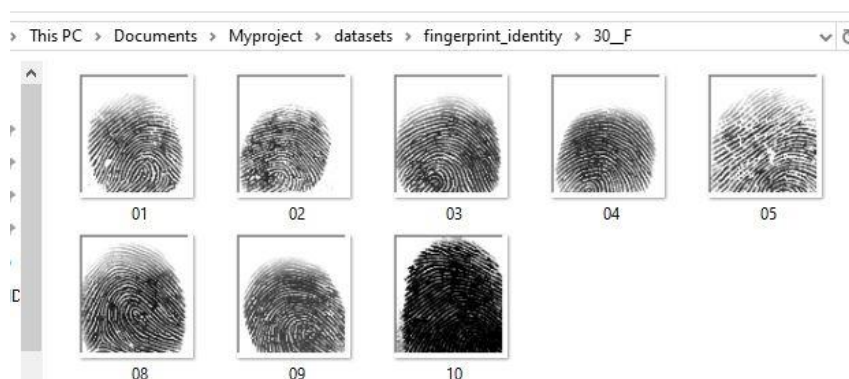


Figure 6. Public fingerprint dataset (SOCOFing from Kaggle).

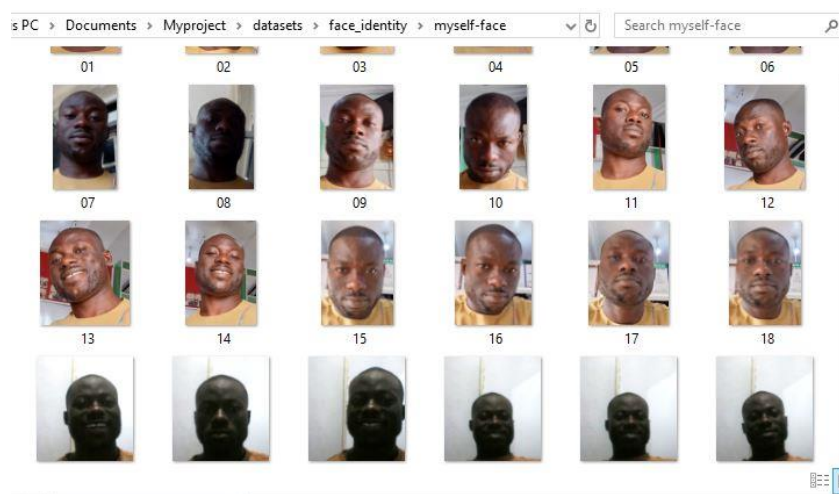


Figure 7. Locally captured face image dataset.

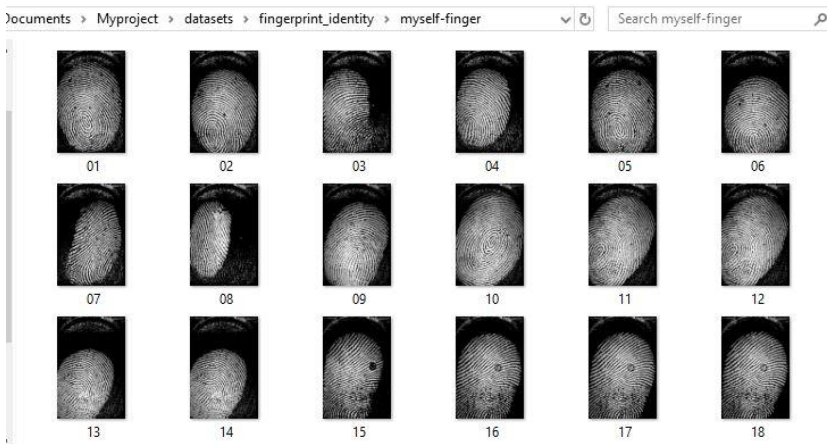


Figure 8. Locally captured fingerprint dataset.

3.3. Bias Mitigation

Bias mitigation was considered important because biometric and contextual access-control models can produce unfair or unreliable decisions when trained on imbalanced or poorly representative data. In the proposed system, bias was reduced by combining public datasets with locally captured enrolled-user samples, ensuring that the final model reflected the actual deployment environment. The face and fingerprint datasets were organized by user identity, while preprocessing steps such as resizing, normalization, labeling, and controlled class balancing were applied before training.

For contextual access analysis, records were cleaned, encoded, scaled, and balanced to reduce the effect of dominant classes on the 1D CNN/Conv1D model. Model performance was also evaluated using accuracy, precision, recall, F1-score, and confusion matrices instead of relying on accuracy alone. This helped identify whether the models performed consistently

across classes. In addition, the system combined biometric confidence scores with contextual risk analysis and Chinese Wall policy enforcement, reducing overdependence on a single model output during final access decisions.

3.3.1. Technology Stack and Data Organization

Table 1 summarizes the main technologies and analytical components integrated into the proposed prototype. The system was implemented using Python and Flask for backend logic, routing, and web-based access-control operations, while MySQL was used to store structured records such as user profiles, biometric labels, access logs, contextual attributes, and decision history. IPFS supported decentralized and content-addressed storage of biometric-related artifacts, improving traceability and reducing dependence on a single storage point.

The analytical layer combined MobileNetV2 CNN for face recognition, EfficientNetB0 CNN for fingerprint recognition, and a 1D CNN/Conv1D model for contextual risk analysis. samples captured from the biometric scanner.

Table 1. Core technologies, analytical modules, and functions in the proposed system.

Component	Technology and function
Backend service	Python for core application logic and system integration
Web framework	Flask for routing, forms, dashboards, and API handling
Relational database	MySQL for structured storage of users, logs, and decisions
Decentralized storage	IPFS for content-addressed storage of biometric-related artifacts
Face module	MobileNetV2 CNN for face feature learning and identity verification
Fingerprint module	EfficientNetB0 CNN for primary fingerprint verification
Context module	Conv1D CNN for contextual risk analysis and decision support

Note: the table summarizes the primary implementation and decision-support components used in the prototype.

RECORD ID	USER ID	ROLE	SOURCE FILE	ACTIVITY	ACCESS TIME	HOUR	PC/EDGE NODE	DEVICE TRUST	LOCATION
CTX-001	USR-1001	Audit Officer	r1/device.csv	USB Connect	2026-05-01 09:07:11	9	PC-1117	Trusted	Known
CTX-002	USR-1002	Client Officer	r1/http.csv	HTTP Visit	2026-05-01 12:14:22	12	PC-1134	Trusted	Known
CTX-003	USR-1003	Records Staff	r1/LDAP/2010-01.csv	Database Query	2026-05-01 15:21:33	15	PC-1151	Trusted	Known
CTX-004	USR-1004	IT Admin	r1/logon.csv	Logon	2026-05-01 18:28:44	18	PC-1168	Trusted	Known
CTX-005	USR-1005	Operations User	r1/device.csv	USB Connect	2026-05-01 21:35:55	21	PC-1185	Trusted	Known
CTX-006	USR-1006	Security Analyst	r1/http.csv	HTTP Visit	2026-05-01 00:42:06	0	PC-1202	Trusted	Known
CTX-007	USR-1007	Research User	r1/LDAP/2010-01.csv	Database Query	2026-05-01 03:49:17	3	PC-1219	Trusted	Known
CTX-008	USR-1008	Finance Analyst	r1/logon.csv	Logon	2026-05-01 06:56:28	6	PC-1236	Trusted	Known
CTX-009	USR-1009	Audit Officer	r1/device.csv	USB Connect	2026-05-01 09:03:39	9	PC-1253	Trusted	Known
CTX-010	USR-1010	Client Officer	r1/http.csv	HTTP Visit	2026-05-01 12:10:50	12	PC-1270	Trusted	Known
CTX-011	USR-1011	Records Staff	r1/LDAP/2010-01.csv	Database Query	2026-05-01 15:17:01	15	PC-1287	Untrusted	Known
CTX-012	USR-1012	IT Admin	r1/logon.csv	Logon	2026-05-01 18:24:12	18	PC-1304	Trusted	Known
CTX-013	USR-1013	Operations User	r1/device.csv	USB Connect	2026-05-01 21:31:23	21	PC-1321	Trusted	Unknown
CTX-014	USR-1014	Security Analyst	r1/http.csv	HTTP Visit	2026-05-01 00:38:34	0	PC-1338	Trusted	Known
CTX-015	USR-1015	Research User	r1/LDAP/2010-01.csv	Database Query	2026-05-01 03:45:45	3	PC-1355	Trusted	Known
CTX-016	USR-1016	Finance Analyst	r1/logon.csv	Logon	2026-05-01 06:52:56	6	PC-1372	Trusted	Known
CTX-017	USR-1017	Audit Officer	r1/device.csv	USB Connect	2026-05-01 09:59:07	9	PC-1389	Untrusted	Known
CTX-018	USR-1018	Client Officer	r1/http.csv	HTTP Visit	2026-05-01 12:06:18	12	PC-1406	Trusted	Known
CTX-019	USR-1019	Records Staff	r1/LDAP/2010-01.csv	Database Query	2026-05-01 15:13:29	15	PC-1423	Trusted	Unknown

Figure 9. Contextual dataset.

The contextual dataset contains access-related attributes used to evaluate the risk level of each access request. It includes factors such as device trust, known location, login time, resource sensitivity, access history, and user behavior. Unlike biometric datasets, which are image-based, the contextual dataset is structured as tabular data and is used by the 1D CNN/Conv1D model to learn access patterns and support risk-aware decision-making. In the proposed system, this dataset helped determine whether a verified user should be granted access, required to perform step-up verification, or denied access based on the surrounding access conditions.

3.3.2. CNN Model Training Process

Figures 10 and 11 show the training process for the face and

fingerprint recognition models used in the proposed system. Figure 10 presents the MobileNetV2 face-recognition model training, where facial images were resized, normalized, labeled, and passed through the CNN model to learn identity-based facial features. The model was trained to distinguish enrolled users and generate confidence scores during authentication. Figure 11 presents the EfficientNetB0 fingerprint-recognition model training, where fingerprint samples were preprocessed and organized into identity classes before training. The model learned distinctive fingerprint patterns and produced identity confidence scores for access-control decisions. Together, the face and fingerprint models formed the bimodal biometric layer of the system, improving identity verification and reducing dependence on a single biometric trait.

```

Select Command Prompt

Training face model from C:\Users\Dpaulz\Documents\Myproject\datasets\face_identity ...
Training class distribution: {np.str_('myself-face'): 80, np.str_('user10-face'): 21, np.str_('user2-face'): 78, np.str_('user3-face'): 80, np.str_('user4-face'): 80, np.str_('user5-face'): 80, np.str_('user6-face'): 80, np.str_('user7-face'): 50, np.str_('user8-face'): 19, np.str_('user9-face'): 19}
Priority label 'myself-face' class weight: 2.0
I0000 00:00:1775291019.285542 3208 cpu_feature_guard.cc:227] This TensorFlow binary is optimized to use available CPU
instructions in performance-critical operations.
To enable the following instructions: SSE3 SSE4.1 SSE4.2 AVX, in other operations, rebuild TensorFlow with the appropriate compiler flags.
WARNING:tensorflow:TensorFlow GPU support is not available on native Windows for TensorFlow >= 2.11. Even if CUDA/cuDNN are installed, GPU will not be used. Please use WSL2 or the TensorFlow-DirectML plugin.
Epoch 1/25
--[1m30/30s-[0m +[32m--[0m+[37m-[0m +[1m0s+[0m 901ms/step - accuracy: 0.1574 - loss: 2.9153
Epoch 1: val_accuracy improved from None to 0.13559, saving model to C:\Users\Dpaulz\Documents\Myproject\app\models_dir\face_cnn.keras
--[1m30/30s-[0m +[32m--[0m+[37m-[0m +[1m38s-[0m 1s/step - accuracy: 0.1770 - loss: 2.8142 - val_accuracy: 0.1356 - val_loss: 2.2814 - learning_rate: 5.0000e-04
Epoch 2/25
--[1m30/30s-[0m +[32m--[0m+[37m-[0m +[1m0s+[0m 915ms/step - accuracy: 0.1774 - loss: 2.5386
Epoch 2: val_accuracy did not improve from 0.13559
--[1m30/30s-[0m +[32m--[0m+[37m-[0m +[1m30s-[0m 984ms/step - accuracy: 0.2068 - loss: 2.5197 - val_accuracy: 0.1356 - val_loss: 2.2964 - learning_rate: 5.0000e-04
Epoch 3/25
--[1m30/30s-[0m +[32m--[0m+[37m-[0m +[1m0s+[0m 878ms/step - accuracy: 0.2132 - loss: 2.4512
Epoch 3: ReduceLROnPlateau reducing learning rate to 0.0002500000118743628.
Epoch 3: val_accuracy did not improve from 0.13559
--[1m30/30s-[0m +[32m--[0m+[37m-[0m +[1m28s-[0m 944ms/step - accuracy: 0.2431 - loss: 2.4266 - val_accuracy: 0.1356 - val_loss: 2.2814 - learning_rate: 0.0002500000118743628

```

Figure 10. Model training process of facial biometric data.

```

Command Prompt - python retrain_biometrics.py --target fingerprint --epochs 25 --max-images-per-class 60 --fingerprint-include-labels "myself-finger...
Training class distribution: {np.str_('myself-finger'): 60, np.str_('user10-finger'): 24, np.str_('user2-finger'): 53, np.str_('user4-finger'): 50, np.str_('user5-finger'): 50, np.str_('user6-finger'): 55, np.str_('user7-finger'): 54, np.str_('user8-finger'): 20, np.str_('user9-finger'): 11}
Priority label 'myself-finger' class weight: 3.0
10000 00:00:1775290840.651986 6276 cpu_feature_guard.cc:227] This TensorFlow binary is optimized to use available CPU
Instructions in performance-critical operations.
To enable the following instructions: SSE3 SSE4.1 SSE4.2 AVX, in other operations, rebuild TensorFlow with the appropriate compiler flags.
WARNING:tensorflow:TensorFlow GPU support is not available on native Windows for TensorFlow >= 2.11. Even if CUDA/cuDNN are installed, GPU will not be used. Please use WSL2 or the TensorFlow-DirectML plugin.
Epoch 1/25
+1m23/23+0m +[32m-----+0m+[37m-0m +[1m0s-0m 787ms/step - accuracy: 0.2404 - loss: 3.4220
Epoch 1: val_accuracy improved from None to 0.14103, saving model to C:\Users\Dpaulz\Documents\Myproject\app\models_dir\
fingerprint_cnn.keras
+1m23/23+0m +[32m-----+0m+[37m-0m +[1m28s-0m 884ms/step - accuracy: 0.3090 - loss: 3.1288 - val_accu
racy: 0.1410 - val_loss: 2.2261 - learning_rate: 5.0000e-04
Epoch 2/25
+1m23/23+0m +[32m-----+0m+[37m-0m +[1m0s-0m 786ms/step - accuracy: 0.4244 - loss: 2.3644
Epoch 2: val_accuracy did not improve from 0.14103
+1m23/23+0m +[32m-----+0m+[37m-0m +[1m19s-0m 841ms/step - accuracy: 0.4242 - loss: 2.4422 - val_accu
racy: 0.1410 - val_loss: 2.4380 - learning_rate: 5.0000e-04
Epoch 3/25
+1m23/23+0m +[32m-----+0m+[37m-0m +[1m0s-0m 809ms/step - accuracy: 0.4711 - loss: 2.2210
Epoch 3: ReduceLROnPlateau reducing learning rate to 0.0002500000118743628.
Epoch 3: val_accuracy did not improve from 0.14103
+1m23/23+0m +[32m-----+0m+[37m-0m +[1m20s-0m 867ms/step - accuracy: 0.4719 - loss: 2.2624 - val_accu
racy: 0.1410 - val_loss: 2.7153 - learning_rate: 5.0000e-04
Epoch 4/25
+1m22/23+0m +[32m-----+0m+[37m-0m +[1m0s-0m 846ms/step - accuracy: 0.5033 - loss: 2.0933

```

Figure 11. Fingerprint model training.

3.3.3. Model Performance Evaluation

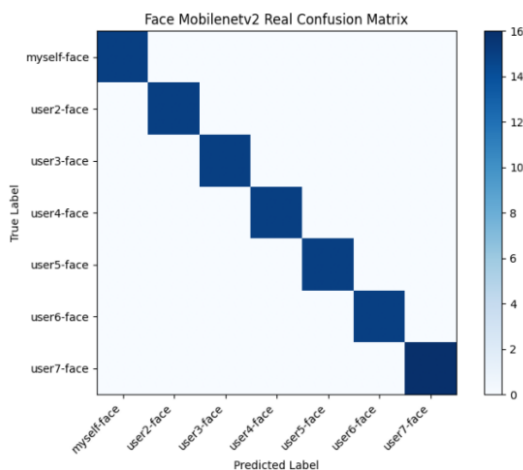


Figure 12. MobileNetV2 real face confusion matrix.

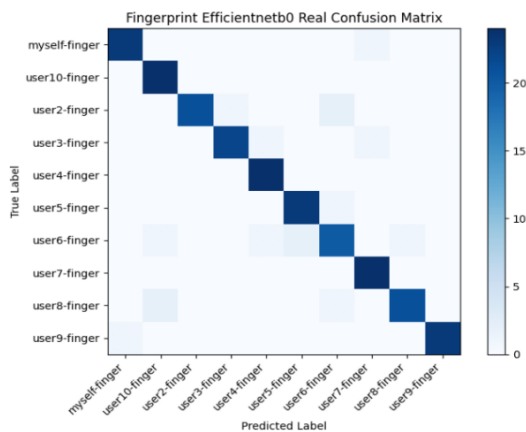


Figure 13. EfficientNetB0 real fingerprint confusion matrix.

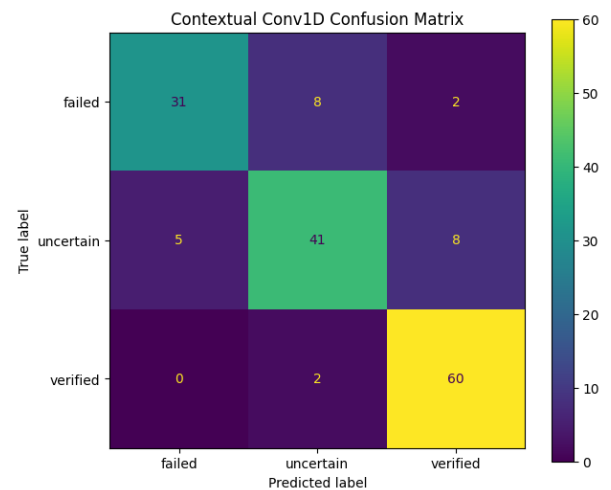


Figure 14. Contextual Conv1D confusion matrix.

Figures 12, 13, and 14 show the confusion matrices for the three intelligent models used in the proposed system. Figure 12 presents the MobileNetV2 face-recognition confusion matrix, showing how well the model classified enrolled face identities. Figure 13 shows the EfficientNetB0 fingerprint-recognition confusion matrix, indicating the model's ability to distinguish fingerprint classes. Figure 14 presents the Contextual Conv1D confusion matrix, which shows how accurately the contextual model classified access conditions for risk-aware decision-making. Together, the confusion matrices provide evidence of the classification performance of the biometric and contextual models used for final access control decisions.

3.4. System Deployment and Testing

System deployment and testing covered registration, biometric capture, login, contextual scoring, Chinese Wall enforcement, and administrative reporting. Functional testing

confirmed that enrolled face and fingerprint samples could be captured, stored, and evaluated within the unified application workflow.



Figure 15. Enrollment form page.

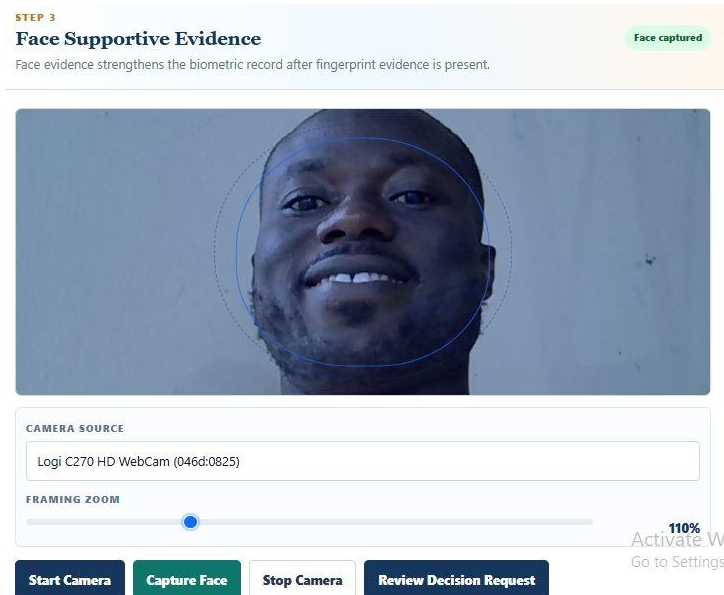


Figure 16. Biometric face-capture page.



Figure 17. Biometric fingerprint-capture page.

3.5. Proposed System Workflow

The proposed workflow begins when a user submits credentials and biometric evidence at an access point. The edge node captures face and fingerprint inputs, verifies them using MobileNetV2 CNN and EfficientNetB0 CNN, and evaluates contextual attributes such as device trust, location, login time, resource sensitivity, and access history using a 1D CNN Conv1D model. The system then applies Chinese Wall policy restrictions before producing a final grant, step-up, or deny decision.

3.6. Contexts-Aware Authorization and Policy Enforcement

Context-aware authorization remains essential because authentication alone does not determine what a verified user should be allowed to access under a specific situation. In the proposed system, a user first submits biometric and access-request information through the edge-aware application. The system then verifies identity using facial recognition and fingerprint recognition, while contextual attributes such as device trust, known location, login hour, resource sensitivity, access history, and conflict-of-interest status are evaluated before the final decision is made. The 1D CNN/Conv1D contextual model supports risk analysis from these access conditions, while the Chinese Wall policy prevents access where organizational conflicts exist. This workflow aligns with attribute-based and risk-adaptive access control principles by combining identity assurance, contextual risk evaluation, and policy enforcement within a real-time edge computing environment [8, 22, 28].

4. Results

The biometric and contextual modules produced strong results. The MobileNetV2 face model achieved about 0.96 overall accuracy, while the enrolled-user face class recorded 0.92 precision, 0.94 recall, and 0.93 F1-score. The EfficientNetB0 fingerprint model achieved about 93.36% overall classification accuracy; the enrolled-user fingerprint class recorded 95.83% precision, 95.83% recall, and 95.83% F1-score, and the highest validation accuracy reached 93.78% during training. The contextual Conv1D model achieved 84.08% test accuracy on 157 records, with the verified class producing 96.77% recall and 90.91% F1-score. Integrated system testing showed that biometric evidence, contextual analysis, and Chinese Wall enforcement worked together to support real-time grant, step-up, and deny decisions.

4.1. Enhanced Performance Evaluation

Figures 18, 20, and 21 show the FAR versus FRR curve, risk-score distribution, and grant-by-identity-confidence output of the biometric-enhanced access-control system. The FAR/FRR curve was used to examine the balance between false acceptance and false rejection during biometric verification. The risk-score distribution shows how access requests were grouped according to their computed risk levels, while the grant-by-identity-confidence result shows how biometric confidence influenced access approval. Together, these outputs demonstrate how the proposed system combines biometric reliability and contextual risk analysis to support secure access-control decisions.

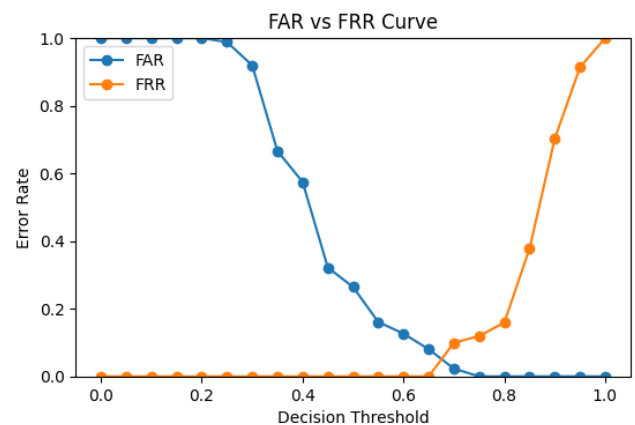


Figure 18. FAR versus FRR curve.

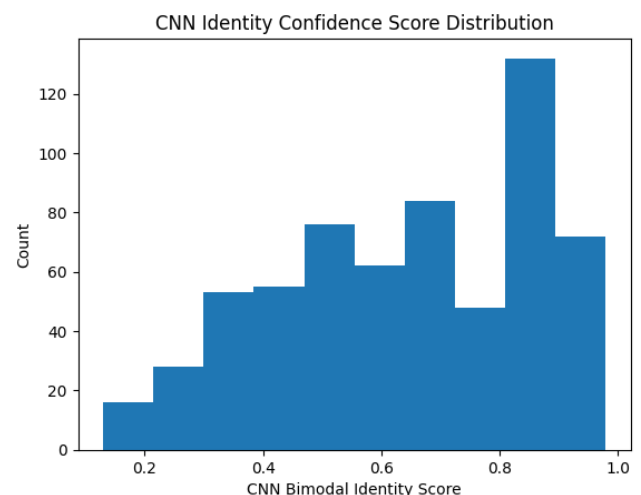


Figure 19. CNN identity confidence score distribution.

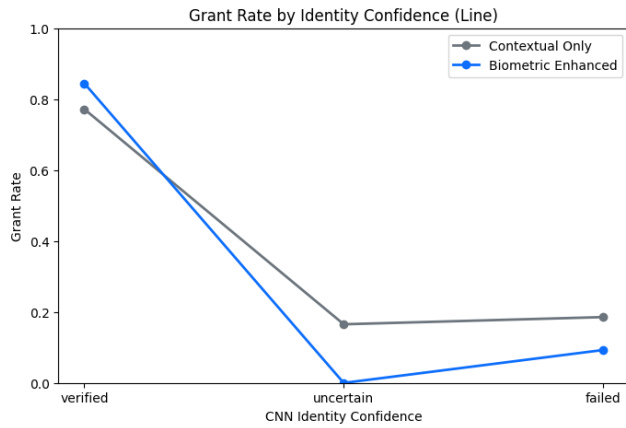


Figure 20. Grant identity confidence score distribution.

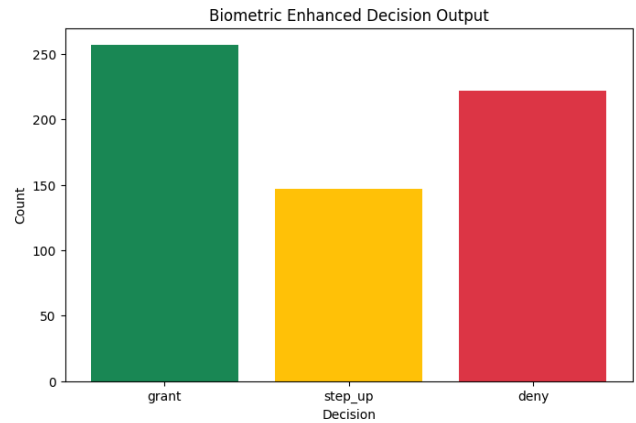


Figure 22. Biometric-enhanced decision output.

4.2. Result Summary

The results indicate that the proposed system improves on context-only access control by adding direct biometric identity assurance to edge-based authorization. The study also showed that locally captured biometric samples improved operational dependability because they reduced the domain gap between training data and live deployment conditions. The proposed system shows clear improvements over context-only access control based on the following findings

1. Added direct identity verification to context-based access control.
2. Reduced the risk of granting access based only on trusted device or location.
3. Improved detection of uncertain or weak identity-confidence cases.
4. Supported better grant, step-up, and deny decision separation.
5. Strengthened edge-based authorization by combining biometric evidence, contextual risk, and policy enforcement.

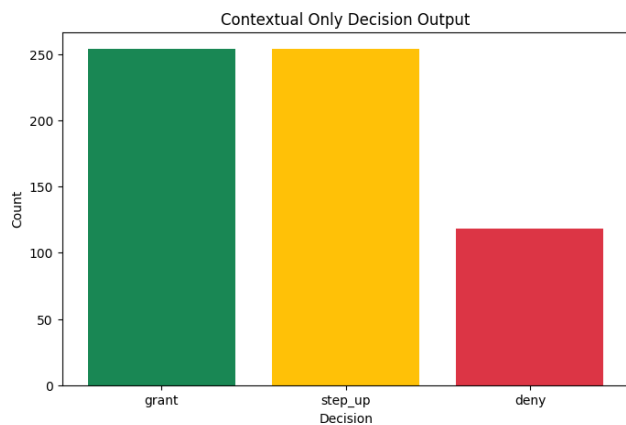


Figure 21. Contextual-only decision output.

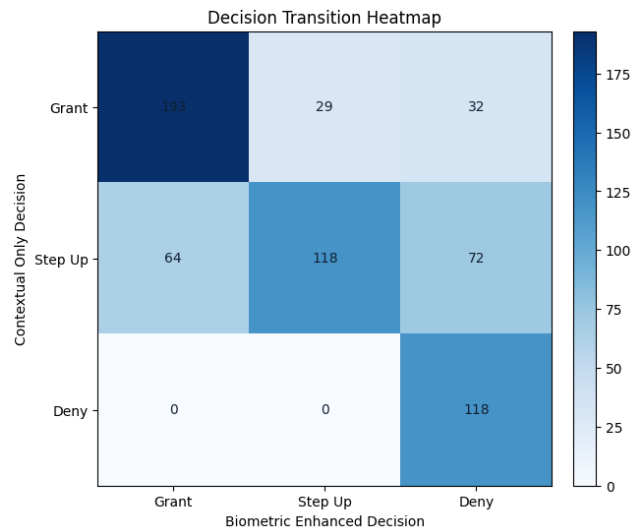


Figure 23. Decision transition heatmap.

5. Discussion

The Contextual Only Decision Output represents the baseline system, where access decisions were based on factors such as device trust, location, login time, access history, resource sensitivity, and policy restrictions. Although useful, this approach could still grant access when context appeared normal without confirming the requester's real identity. The Biometric Enhanced Decision Output shows the improved model after face and fingerprint verification were added. This made the system more identity-aware and reduced overdependence on contextual trust. The Decision Transition Heatmap shows that some requests previously granted by the contextual-only model were changed to step-up or deny decisions when biometric confidence was weak, confirming stronger and more reliable access control.

6. Conclusions and Future Work

The study demonstrates that combining bimodal biometrics, contextual CNN analysis, and Chinese Wall policy enforcement can produce a more secure and adaptive access-control framework for edge computing environments. The final system delivered stronger identity verification, improved decision reliability, and practical real-time operation through edge-aware processing. Future work should expand the locally captured biometric dataset, refine multimodal score fusion, and validate the framework with a larger user population and more deployment sites.

Abbreviations

ABAC	Attribute-Based Access Control
CNN	Convolutional Neural Network
CID	Content Identifier
IPFS	InterPlanetary File System
MEC	Multi-Access Edge Computing
RBAC	Role-Based Access Control

Acknowledgments

I sincerely appreciate my supervisors, Professor F. E. Onuodu and Dr. (Mrs.) U. A. Okengwu, for their guidance, encouragement, constructive criticism, and scholarly support throughout this research. I also thank the Acting Head of the Department of Computer Science, Dr. (Mrs.) M. O. Musa, for her commitment to the growth of the department and its academic programme. My appreciation further goes to the post-graduate lecturers, including Professor P. O. Asagba, Professor L. N. Onyejebu, Professor C. Ugwu, Professor B. O. Eke, Professor E. E. Ogheneovo, Professor F. Egbono, and others, for their contributions to knowledge and academic development.

Appendix



Figure 24. Futronic fingerprint-capture device.

Author Contributions

Paul Ndudiri Ohia: Conceptualization, Methodology, Software, Validation, Formal Analysis, Investigation, Data curation, Visualization, Writing - original draft

Friday Eleonu Onuodu: Supervision, Methodology, Resources, Validation, Writing - review and editing

Ugochi Adaku Okengwu: Supervision, Project administration, Validation, Writing - review and editing

Funding

This work is not supported by any external funding.

Data Availability Statement

Public benchmark datasets referenced in this study include VGGFace2 for face-recognition experimentation, SOCOFing for fingerprint-recognition experimentation, and the KiltHub Insider Threat Test Dataset for contextual access-record analysis. VGGFace2 is available at https://github.com/ox-vgg/vgg_face2, SOCOFing is available at <https://www.kaggle.com/ruizgara/socofing>, and the KiltHub Insider Threat Test Dataset is available at https://kilthub.cmu.edu/articles/dataset/Insider_Threat_Test_Dataset/12841247. Locally captured biometric samples and implementation artifacts are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare no conflicts of interest.



Figure 25. Fingerprint captured dataset.

Contextual and Decision Comparison

TIME	USER	GROUP	RESOURCE	IDENTITY CONFIDENCE	CHINESE WALL	TRUSTED DEVICE	KNOWN LOCATION	HOUR	GEO LOCATION	LANGUAGE	TIMEZONE
2026-08-19 17:27:51	giant	public	logged_in_account_access	verified (0.91)	allow	yes	yes	18	4.9021,6.9226	en-US	Africa/Lagos
2026-08-19 03:56:21	realtime_user_03	oil_company_a	oil_well_production_report	verified (0.83)	deny	yes	yes	13	Lagos, Nigeria	en-GB	Africa/Lagos
2026-08-19 03:30:51	giant	public	logged_in_account_access	verified (0.90)	allow	yes	yes	4	4.9021,6.9226	en-US	Africa/Lagos
2026-08-19 03:29:22	dpauz1	public	logged_in_account_access	failed (0.72)	allow	no	no	4	4.9021,6.9226	en-US	Africa/Lagos

Figure 26. Contextual data interface.



Figure 27. User dashboard page design layout.

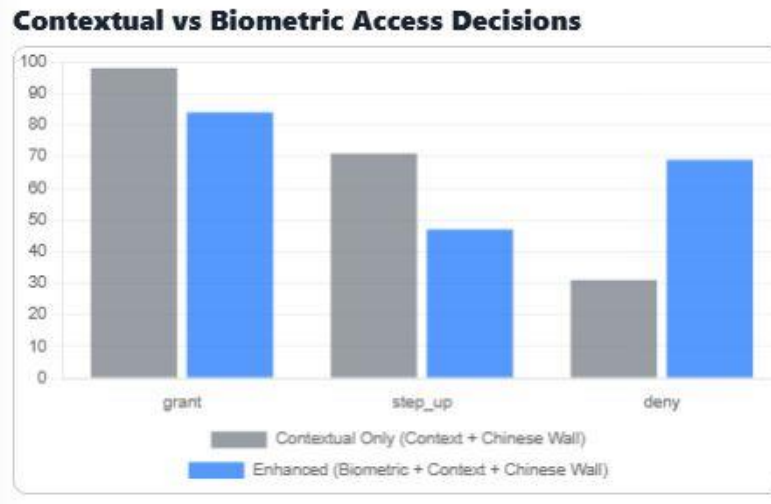


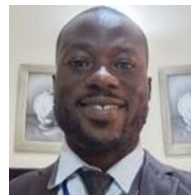
Figure 28. Contextual versus biometric access decisions.

References

- [1] Hameed, S., et al. Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. *Cyber Security and Applications*. 2023, 1, 100015. <https://doi.org/10.1016/j.csa.2023.100015>
- [2] Shakarami, A., et al. Contemporary advances in multi-access edge computing: A survey of fundamentals, architecture, technologies, deployment cases, security, challenges, and directions. *Journal of Network and Computer Applications*. 2023, 219, 103726. <https://doi.org/10.1016/j.jnca.2023.103726>
- [3] Kaur, N. A systematic review on security aspects of fog computing environment: Challenges, solutions and future directions. *Computer Science Review*. 2024, 54, 100688. <https://doi.org/10.1016/j.cosrev.2024.100688>
- [4] Chandramouli, R., Butcher, Z. A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments. NIST Special Publication 800-207. National Institute of Standards and Technology. 2023. <https://doi.org/10.6028/NIST.SP.800-207A>
- [5] Alam, T., et al. Differential privacy in edge computing-based smart city applications: Security issues, solutions and future directions. *Array*. 2023, 19, 100293. <https://doi.org/10.1016/j.array.2023.100293>
- [6] Xu, G., Ren, J., Zhang, Y., Lin, C. A multimodal biometric authentication scheme for mobile edge computing. *Information Sciences*. 2021, 553, 1-15. <https://doi.org/10.1016/j.ins.2020.11.029>
- [7] Yao, H., Zhang, J., Liu, X., Wang, Y. Multimodal biometric authentication by federated learning. *Biomedical Signal Processing and Control*. 2023, 85, 104932. <https://doi.org/10.1016/j.bspc.2023.104932>
- [8] Hu, V. C., Ferraiolo, D. F., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST SP 800-162. National Institute of Standards and Technology. 2015. <https://doi.org/10.6028/NIST.SP.800-162>
- [9] Muhammad, B. A., Garba, M., Gabi, D., Suru, H. U., Argungu, M. S. Dynamic access control at the network edge using an adaptive risk-based access control system (ad-RACs). 2024, 1(2), 12-19.
- [10] Goudarzi, H., Liao, X., Zhang, Q. A review on edge computing architecture and its applications in IoT and AI. *Future Generation Computer Systems*. 2023, 142, 312-328.
- [11] Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L. Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal*. 2016, 3(5), 637-646. <https://doi.org/10.1109/JIOT.2016.2579198>
- [12] Satyanarayanan, M. The Emergence of Edge Computing. *Computer*. 2017, 50(1), 30-39. <https://doi.org/10.1109/MC.2017.9>
- [13] XenonStack. Edge Computing Solutions and Capabilities. Available from: <https://www.xenonstack.com/enterprise/edge-computing/> (accessed 15 September 2026).
- [14] Jain, A. K., Ross, A., Prabhakar, S. An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*. 2004, 14(1), 4-20. <https://doi.org/10.1109/TCSVT.2003.818349>
- [15] Ratha, N. K., Connell, J. H., Bolle, R. M. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*. 2001, 40(3), 614-634. <https://doi.org/10.1147/sj.403.0614>
- [16] Jain, A. K., Ross, A. Introduction to Biometrics. In *Handbook of Biometrics*. Springer. 2008, pp. 1-22. https://doi.org/10.1007/978-0-387-71041-9_1
- [17] Maltoni, D., Maio, D., Jain, A. K., Prabhakar, S. *Handbook of Fingerprint Recognition*. 2nd ed. Springer. 2009. <https://doi.org/10.1007/978-1-84882-254-2>

- [18] Li, S. Z., Jain, A. K., editors. Handbook of Face Recognition. 2nd ed. Springer. 2011.
<https://doi.org/10.1007/978-0-85729-932-1>
- [19] Sandler, M., Howard, A., Zhu, M., Zhmoginov, A., Chen, L. C. MobileNetV2: Inverted Residuals and Linear Bottlenecks. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2018, pp. 4510-4520.
<https://doi.org/10.1109/CVPR.2018.00474>
- [20] Tan, M., Le, Q. V. EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. Proceedings of the 36th International Conference on Machine Learning. 2019, 97, 6105-6114.
- [21] Nobi, M. Machine learning in access control systems: A survey. ACM Computing Surveys. 2022, 55(3), 1-36.
<https://doi.org/10.48550/arXiv.2207.01739>
- [22] Rahman, M. S., Li, X., Chen, J. Risk-adaptive access control using reinforcement learning. IEEE Transactions on Information Forensics and Security. 2023, 18, 408-421.
<https://doi.org/10.1109/TIFS.2022.3218593>
- [23] LeCun, Y., Bengio, Y., Hinton, G. Deep learning. Nature. 2015, 521, 436-444. <https://doi.org/10.1038/nature14539>
- [24] Abbas, N., Zhang, Y., Taherkordi, A., Skeie, T. Mobile edge computing: A survey. IEEE Internet of Things Journal. 2018, 5(1), 450-465. <https://doi.org/10.1109/JIOT.2017.2770187>
- [25] Jahan, N., Reno, S., Ahmed, M. Securing E-Passport Management Using Private-Permissioned Blockchain and IPFS. In 3rd International Conference on Electrical, Computer and Communication Engineering. 2023.
<https://doi.org/10.1109/ECCE57851.2023.10101496>
- [26] Cao, Q., Shen, L., Xie, W., Parkhi, O. M., Zisserman, A. VGG-Face2: A dataset for recognising faces across pose and age. 13th IEEE International Conference on Automatic Face and Gesture Recognition. 2018, pp. 67-74.
<https://doi.org/10.1109/FG.2018.00020>
- [27] Ruiz Garcia, S. SOCOFing Dataset. Kaggle. Available from: <https://www.kaggle.com/datasets/ruizgara/socofing> (accessed 15 September 2026).
- [28] Brewer, D. F. C., Nash, M. J. The Chinese Wall Security Policy. Proceedings of the IEEE Symposium on Security and Privacy. 1989, pp. 206-214.
<https://doi.org/10.1109/SECPRI.1989.36295>

Biography



Paul Ndudiri Ohia holds B.Sc., M.Sc., and Ph.D. degrees in Computer Science. He has over 12 years of experience in software and web application development.

Research Field

- 1) Access control, edge computing, biometric authentication, fingerprint recognition, face recognition, contextual risk analysis, applied machine learning
- 2) include software engineering, web applications, biometric systems, databases, machine learning, and data analytics.