

Comparative Evaluation of Contextual Only and Machine Learning-Enhanced Biometric Access Control Systems in Edge Computing

Paul Ndudiri Ohia^{1*}; Friday Eleonu Onuodu²; Dr. Ugochi Adaku Okengwu³

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

²Professor; Department of Information Technology, University of Port Harcourt, River State, Nigeria

³Department of Computer Science, University of Port Harcourt, River State, Nigeria

Corresponding Author: Paul Ndudiri Ohia^{1*}

Publication Date: 2026/09/28

Abstract: This paper presents a comparative evaluation of contextual-only and machine learning-enhanced biometric access-control systems in an edge computing environment. The contextual only baseline used device trust, known location, login time, access history, resource sensitivity, contextual risk prediction, and Chinese Wall policy enforcement to produce grant, step-up, or deny decisions. However, contextual trust alone cannot directly confirm that the requester is the genuine enrolled user. The enhanced system addressed this limitation by integrating MobileNetV2 face recognition, EfficientNetB0 fingerprint recognition, 1D CNN/Conv1D contextual analysis, biometric confidence scoring, and policy-aware authorization at the edge. Evaluation was carried out using training and validation curves, confusion matrices, FAR/FRR analysis, contextual-only and biometric-enhanced decision-outputs, decision transition heatmaps, and proportional decision composition graphs. The results show that biometric enhancement improves identity assurance, strengthens decision quality, and reduces overdependence on contextual signals in distributed edge access-control environments.

Keywords: Edge Computing, Bimodal Biometrics, Contextual Access Control, Machine Learning, MobileNetV2, EfficientNetB0, 1D CNN, Chinese Wall Policy, Access Decision.

How to Cite: Paul Ndudiri Ohia; Friday Eleonu Onuodu; Dr. Ugochi Adaku Okengwu (2026) Comparative Evaluation of Contextual Only and Machine Learning-Enhanced Biometric Access Control Systems in Edge Computing. *International Journal of Innovative Science and Research Technology*, 11(9), 1684-1697. <https://doi.org/10.38124/ijisrt/26sep945>

I. INTRODUCTION

Access control systems protect digital and physical resources by determining whether a requester should be granted, challenged, or denied access. In edge computing environments, this decision must be performed close to the user, device, or access point because distributed applications require low-latency and reliable responses [1], [2]. Edge deployment also increases exposure to compromised devices, stolen credentials, manipulated contextual attributes, and unauthorized local access attempts [3], [4].

A contextual-only access-control system can estimate risk from access conditions such as trusted device, known location, login hour, resource sensitivity, access history, and policy restrictions. This provides adaptive authorization, but it does not independently verify the physical identity of the requester. A request may appear normal from a contextual viewpoint even when it is being made with a stolen credential or a compromised endpoint.

The enhanced system evaluated in this paper closes that identity verification gap by combining contextual analysis with bimodal biometric verification. Face recognition and fingerprint recognition were integrated with contextual machine learning and Chinese Wall policy enforcement so that final decisions were based on identity evidence, contextual risk, and authorization policy together [5], [6]. The objective of this paper is to compare the earlier contextual-only decision path with the machine learning-enhanced biometric decision path in an edge computing environment.

II. RELATED WORK

Recent access control research emphasizes adaptive and context-aware authorization because static credentials and role assignments are often insufficient for distributed cyber-physical and edge systems [1], [7]. In such environments, access decisions may consider device trust, location, behavior, resource sensitivity, and previous access history. Attribute-based and risk-adaptive approaches improve

flexibility, but their effectiveness depends on the reliability of the observed contextual signals [8], [9].

Work on access control at the network edge has also explored machine learning for risk prediction and policy-sensitive authorization. CatBoost and other structured data models are useful because access records often contain categorical and numerical attributes [10]. The Chinese Wall policy remains relevant where conflict-of-interest restrictions must be enforced after a user accesses protected information domains [6]. However, contextual and policy mechanisms do not by themselves prove that the requester is the genuine identity holder.

Biometric authentication provides direct physiological evidence of identity. Face recognition is convenient and contact-light, while fingerprint recognition provides a distinctive identity factor. Deep convolutional neural networks have improved biometric recognition performance by learning discriminative image features from face and fingerprint samples [11], [12]. Multimodal biometric systems further improve reliability by combining complementary biometric traits rather than depending on a single modality [13], [14].

The present study contributes to this research direction by comparing a contextual-only baseline with an enhanced edge access-control system that combines MobileNetV2 face recognition, EfficientNetB0 fingerprint recognition, 1D CNN/Conv1D contextual analysis, biometric confidence scoring, and Chinese wall policy enforcement.

➤ Edge Computing Architecture

Edge computing refers to the deployment of computing resources close to end-user devices and data sources, such as sensors, cameras, smartphones, gateways, and biometric scanners. Instead of sending all data to distant cloud servers, edge computing allows data to be processed near the point where it is generated. This reduces latency, minimizes bandwidth use, improves response time, and supports real-time applications such as healthcare monitoring, smart grids, security systems, and biometric access control [1], [2], [3].

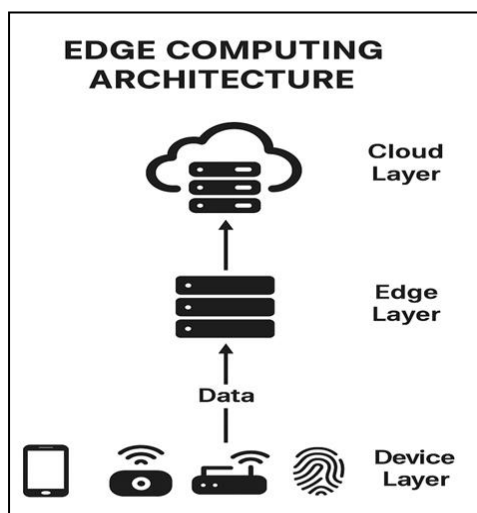


Fig 1 Architecture of Edge Computing [2].

Figure 1 shows the layered architecture of edge computing. The architecture consists of the device layer, edge layer, and cloud layer. The device layer includes sensors, cameras, biometric scanners, and user devices that generate data. The edge layer contains gateways, routers, and edge servers that process data close to the source for faster response. The cloud layer provides centralized storage, advanced analytics, and long-term system management [1].

III. MATERIALS AND METHODS

➤ Baseline Contextual Only System

The baseline system represented the earlier contextual-only decision path. In this architecture, access requests were evaluated using contextual risk reasoning and Chinese Wall policy enforcement. The system considered attributes such as user behaviour, device trust, login location, access time, requested resource, action type, resource sensitivity, and previous access history before producing a decision.

Based on these contextual and policy factors, the system could classify access requests into grant, step-up, or deny categories. However, its major limitation was the absence of direct biometric identity verification. This means that although the system could determine whether an access request appeared safe from a contextual point of view, it could not confirm whether the claimant was truly the genuine enrolled user.

Figure 2 shows the existing contextual-only access-control architecture, adapted from Muhammad et al. [5]. In this architecture, contextual attributes and chinese wall policy enforcement support access decisions without direct biometric identity confirmation.

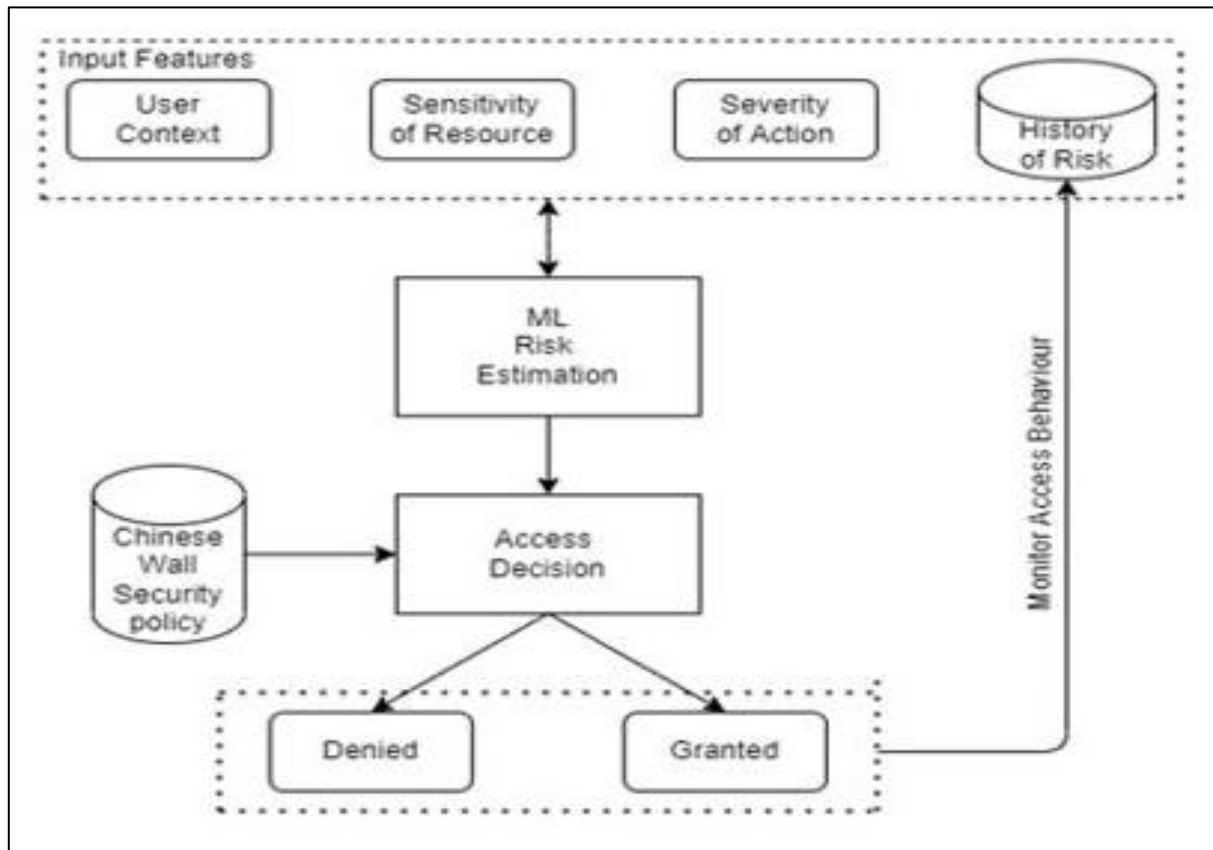


Fig 2 Architecture of the Existing Contextual-Only Access-Control System [5].

Table 1 Baseline Contextual-Only Access-Control Components.

Component	Role	Main limitation
Contextual risk model	Classifies access conditions using structured access records.	Cannot confirm the physical identity of the requester.
Chinese Wall policy	Prevents conflict-of-interest access across protected domains.	Enforces authorization policy after identity/context checks.
Decision layer	Produces grant, step-up, or deny decisions.	Depends on contextual signals that may be incomplete or manipulated.

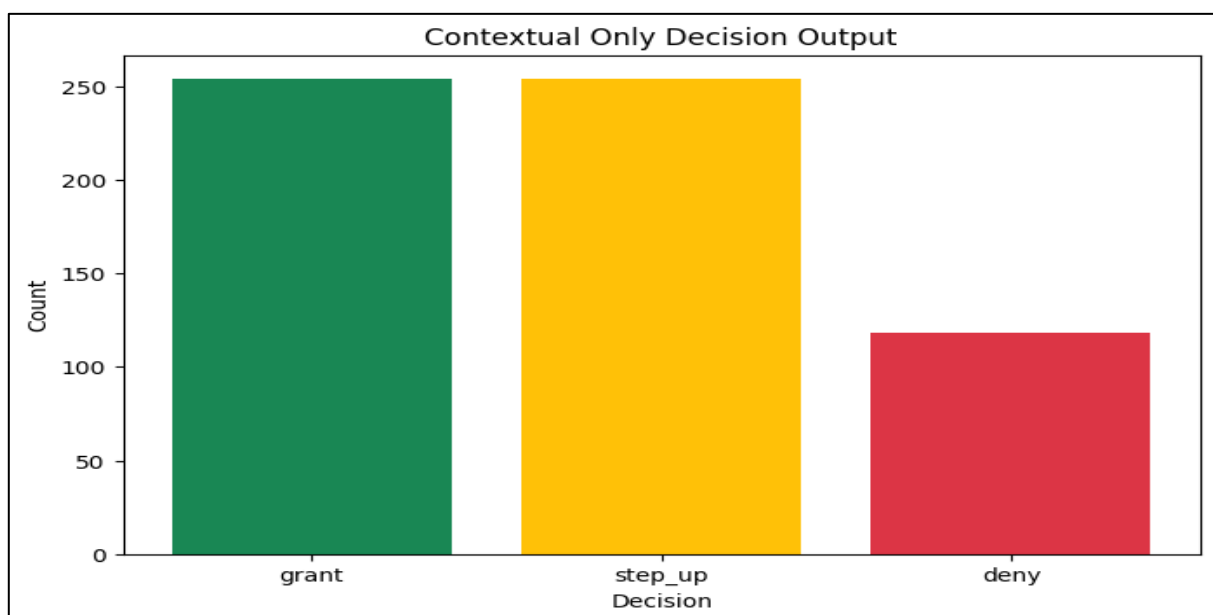


Fig 3 Contextual-Only Decision Output.

➤ *Machine Learning-Enhanced Biometric System*

The enhanced system retained contextual risk analysis and Chinese Wall policy enforcement but added biometric identity verification. MobileNetV2 was used for face recognition, EfficientNetB0 was used for fingerprint recognition, and a 1D CNN/Conv1D model was used for contextual access-state analysis. Biometric confidence, contextual risk, and policy restrictions were fused before the final decision was made at the edge. During an access

request, the user submits credentials and biometric evidence. The edge node captures face and fingerprint inputs, preprocesses them, extracts identity features through the trained CNN models, evaluates contextual attributes, checks Chinese Wall restrictions, and then returns a grant, step-up, or deny decision. This design supports fast local processing while reducing dependence on distant cloud-only authentication.

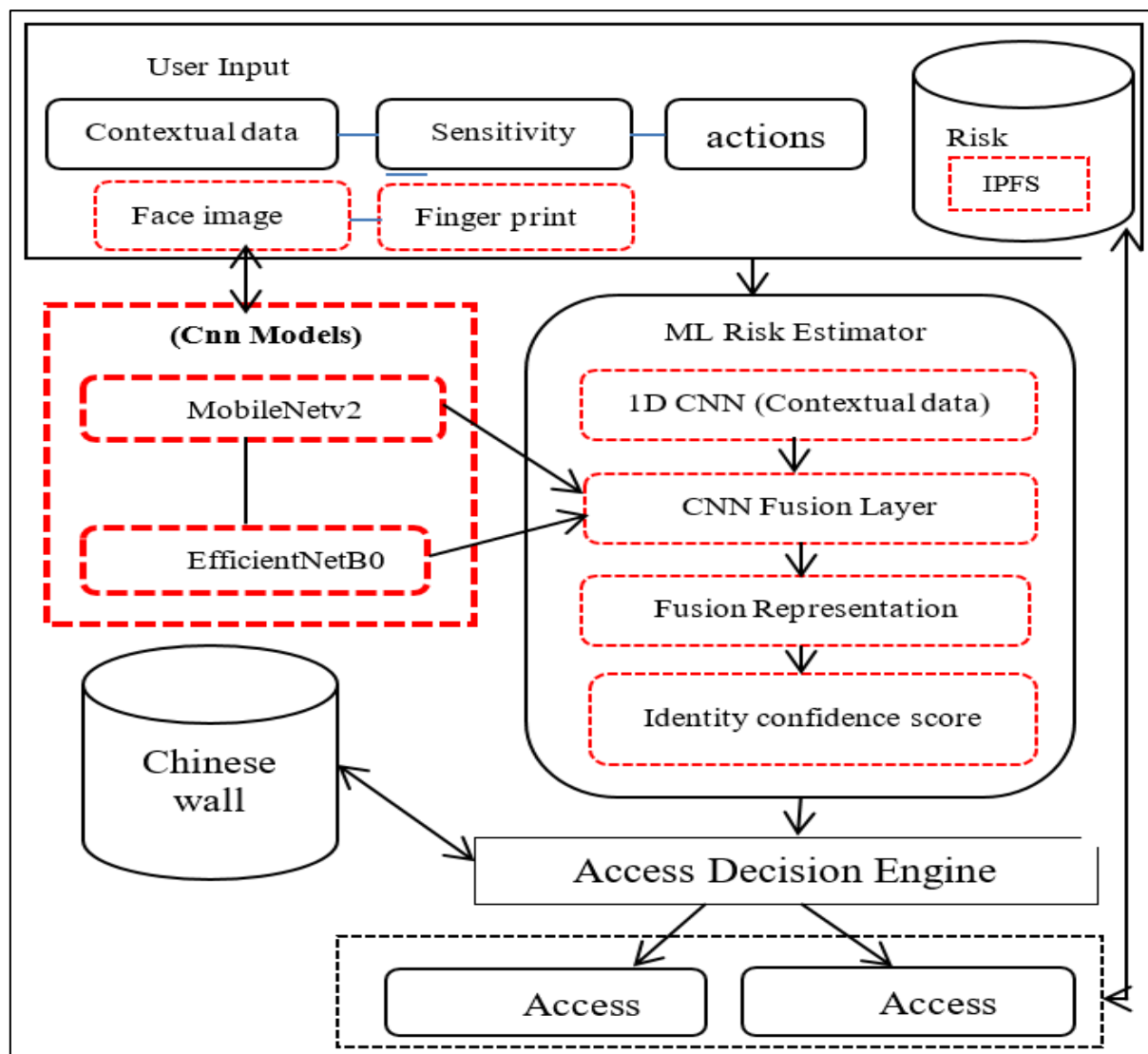


Fig 4 Proposed System Architecture for the Machine Learning-Enhanced Biometric Access-Control System.

Table 2 Enhanced Biometric Access-Control Components.

Component	System role	Contribution
MobileNetV2 face model	Processes face samples for identity verification.	Adds convenient biometric identity evidence.
EfficientNetB0 fingerprint model	Processes fingerprint samples for identity verification.	Adds stable physiological evidence.
1D CNN/Conv1D contextual model	Learns access-state patterns from contextual records.	Supports adaptive risk evaluation.
Chinese Wall policy	Restricts conflicting access even after successful authentication.	Ensures policy-aware authorization.
Final decision layer	Combines biometrics, context, risk, and policy.	Produces stronger grant, step-up, or deny outcomes.

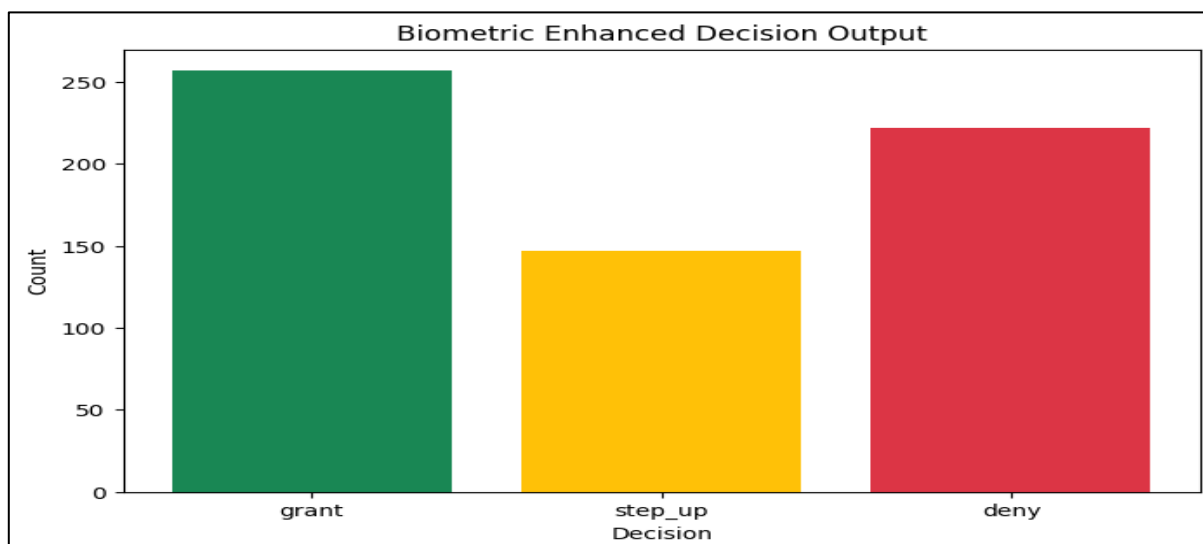


Fig 5 Biometric-Enhanced Decision Output.

➤ Dataset and Training Summary

The enhanced system used both public benchmark datasets and locally captured samples. VGGFace2 and SOCOFing supported early experimentation, while the final operational evaluation emphasized locally captured enrolled user biometric data because it reflected the actual deployment devices, lighting conditions, capture settings, and user interaction patterns [15], [16].

The local face dataset contained 1,090 real-user face images across ten enrolled identities, while the fingerprint dataset contained 1,013 real-user fingerprint images across ten enrolled identities. The contextual dataset contained structured access records derived from system logs and

insider-threat-style contextual records. These records represented attributes such as device trust, known location, login time, access history, resource sensitivity, and decision class.

Preprocessing included image resizing, normalization, label encoding, feature scaling, and class-balancing steps. Face and fingerprint samples were organized into identity-based folders for supervised CNN training, while contextual records were encoded as tabular feature vectors for 1D CNN/Conv1D analysis. The datasets were split into training and testing subsets, and performance was assessed using accuracy, precision, recall, F1-score, confusion matrices, and functional access-decision testing.

Table 3 Model and Dataset Summary.

Model	Input/data type	Dataset basis	Reported result
MobileNetV2	Face images	1,090 local face samples across 10 users	Approximately 97% target accuracy
EfficientNetB0	Fingerprint images	1,013 local fingerprint samples across 10 users	Approximately 93% final accuracy
1D CNN/Conv1D	Structured contextual records	157 evaluation records across failed, uncertain, and verified classes	84.08% accuracy

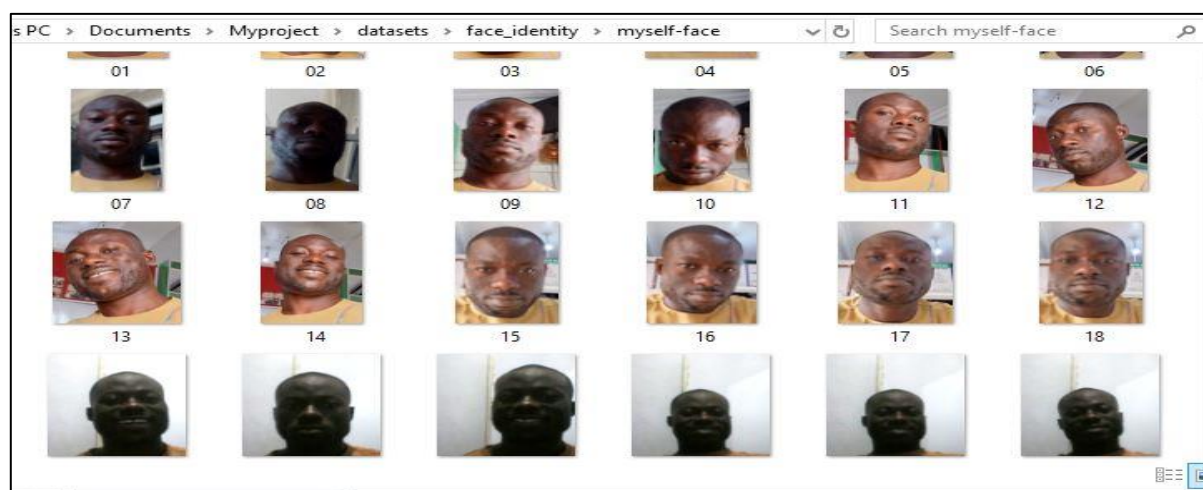


Fig 6 Biometric Data Capture Device.

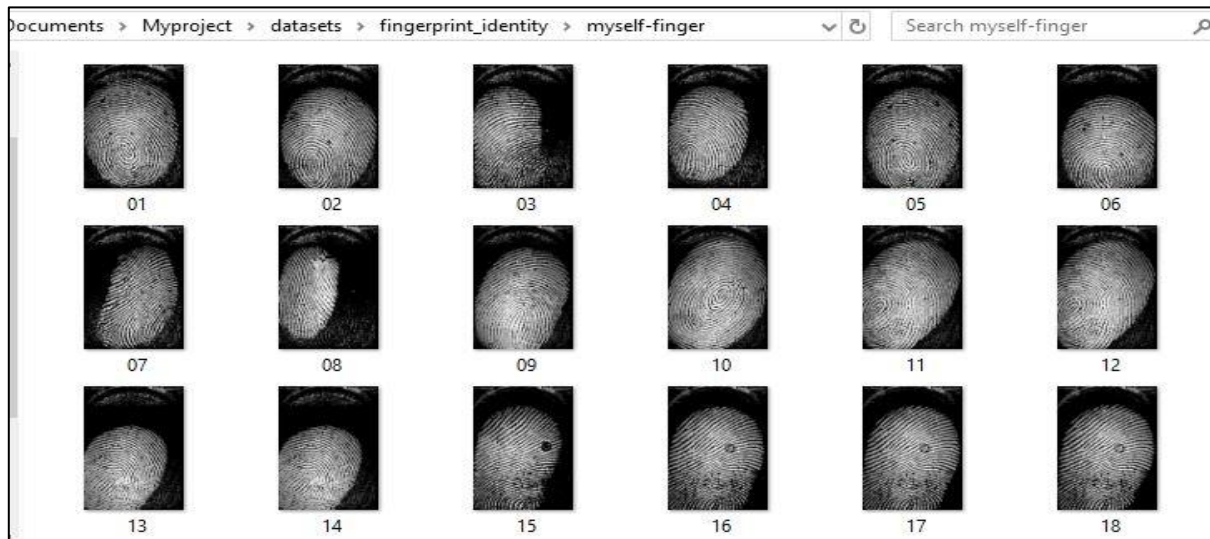


Fig 7 Local Captured Fingerprint Dataset.

```

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
[0000 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 appropri
ate 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
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+ [1m30/30+ [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
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+ [1m30/30+ [0m + [32m-----+ [0m+ [37m+ [0m + [1m38s+ [0m 1s/step - accuracy: 0.1770 - loss: 2.8142 - val_accura
cy: 0.1356 - val_loss: 2.2814 - learning_rate: 5.0000e-04
Epoch 2/25
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+ [1m30/30+ [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
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+ [1m30/30+ [0m + [32m-----+ [0m+ [37m+ [0m + [1m30s+ [0m 984ms/step - accuracy: 0.2068 - loss: 2.5197 - val_accu
racy: 0.1356 - val_loss: 2.2964 - learning_rate: 5.0000e-04
Epoch 3/25
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+ [1m30/30+ [0m + [32m-----+ [0m+ [37m+ [0m + [1m0s+ [0m 878ms/step - accuracy: 0.2132 - loss: 2.4512
Epoch 3: ReduceLROnPlateau reducing learning rate to 0.0002500000118743628.
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+ [1m30/30+ [0m + [32m-----+ [0m+ [37m+ [0m + [1m28s+ [0m 944ms/step - accuracy: 0.2431 - loss: 2.4266 - val_accu

```

Fig 8 Model Training Process for Facial Biometric Data.

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

Fig 9 Contextual Dataset.

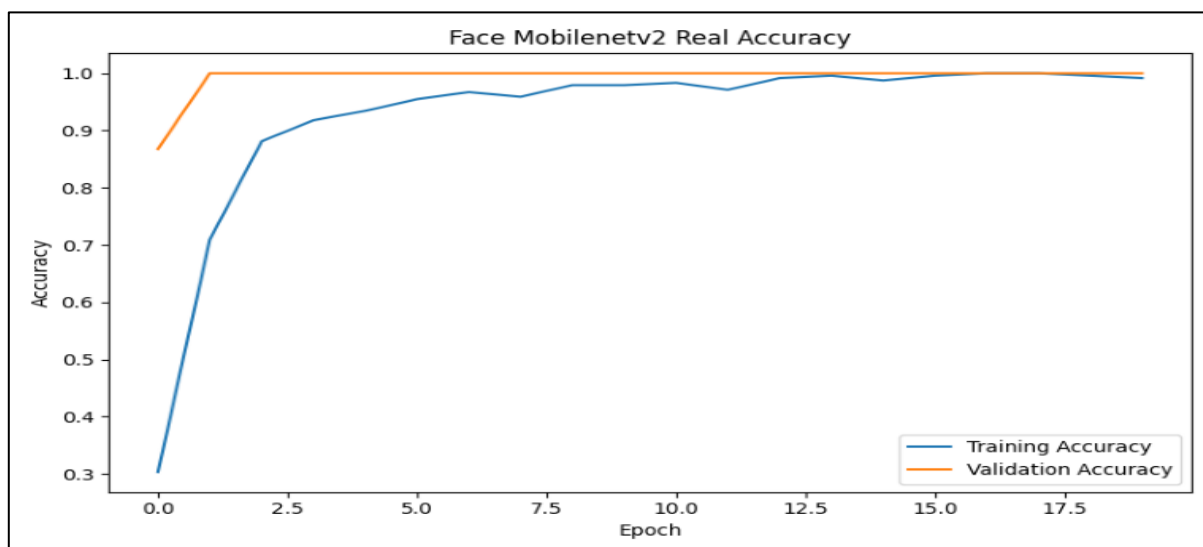


Fig 10 MobileNetV2 Face Accuracy.

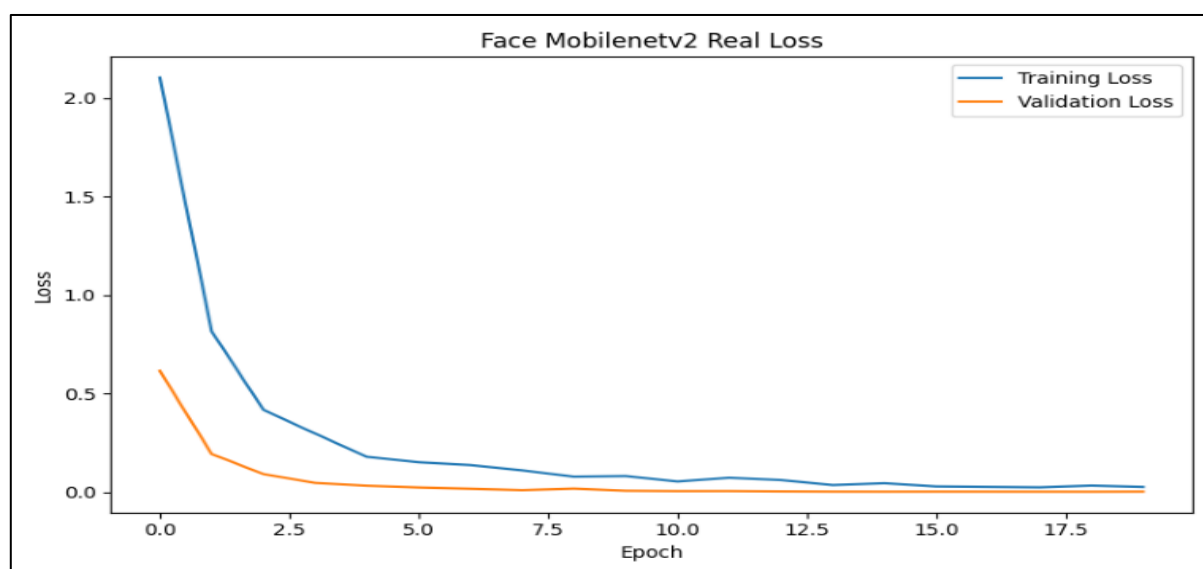


Fig 11 MobileNetV2 Face Loss.

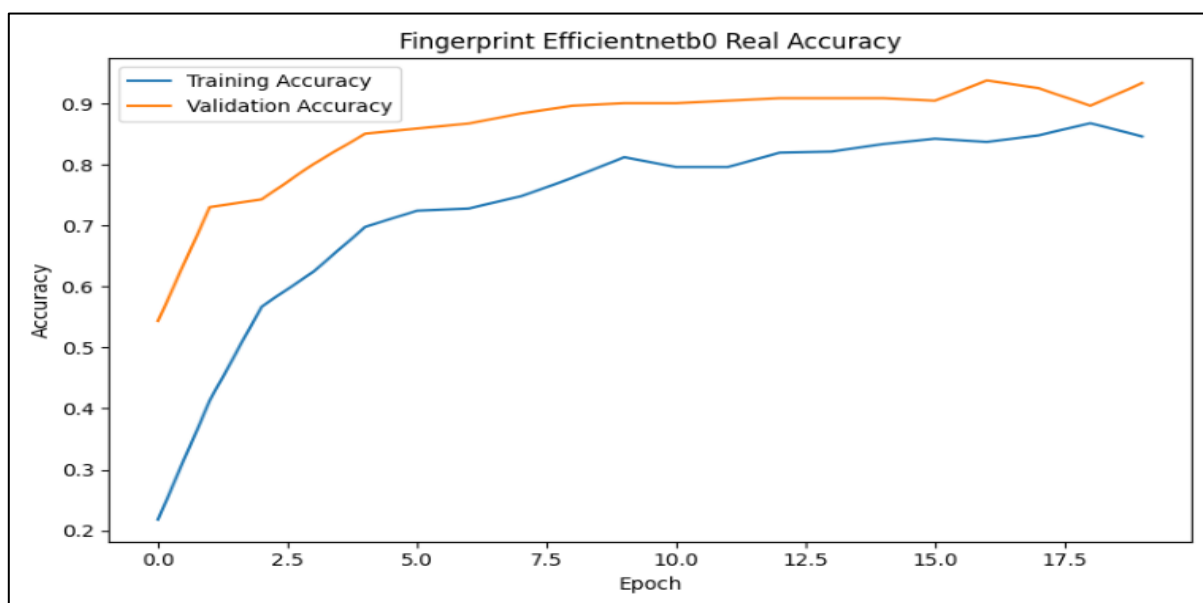


Fig 12 EfficientNetB0 Fingerprint Accuracy.

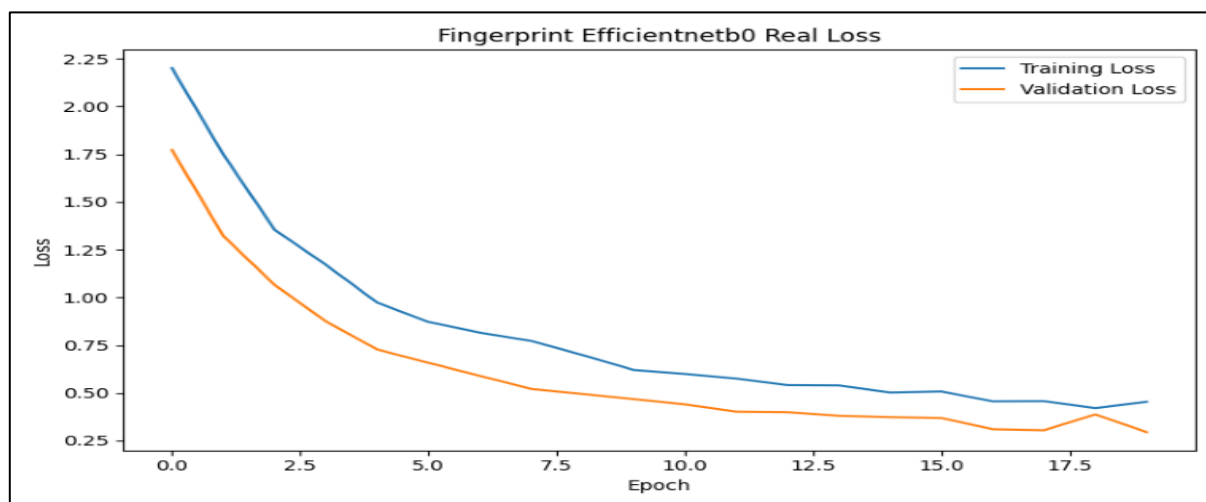


Fig 13 EfficientNetB0 Fingerprint Loss.

➤ Evaluation Procedure

The evaluation compared the contextual-only decision path with the biometric-enhanced decision path. The contextual-only path was assessed using grant, step-up, and deny outputs generated from contextual risk analysis and Chinese Wall enforcement. The enhanced path was assessed after adding face and fingerprint verification to the same contextual and policy framework.

The comparison used model performance metrics, confusion matrices, contextual-only and biometric-enhanced decision-output graphs, a direct contextual-versus-enhanced comparison graph, a decision transition heatmap, FAR/FRR analysis, and proportional decision-composition charts. These

outputs made it possible to observe whether biometric evidence preserved, strengthened, or changed earlier contextual decisions.

IV. RESULTS

➤ Contextual Machine Learning Performance

The contextual 1D CNN/Conv1D model achieved 84.08% accuracy across 157 evaluation records. The verified class recorded the strongest F1-score at 90.91%, while failed and uncertain classes recorded F1-scores of 80.52% and 78.10%, respectively. These results show that contextual features were useful for access-state classification, but they did not remove the need for independent identity verification.

Table 4 Contextual 1D CNN/Conv1D Classification Result.

Class	Precision	Recall	F1-score	Support
Failed	86.11%	75.61%	80.52%	41
Uncertain	80.39%	75.93%	78.10%	54
Verified	85.71%	96.77%	90.91%	62
Accuracy	-	-	84.08%	157
Macro average	84.07%	82.77%	83.17%	157
Weighted average	83.99%	84.08%	83.79%	157

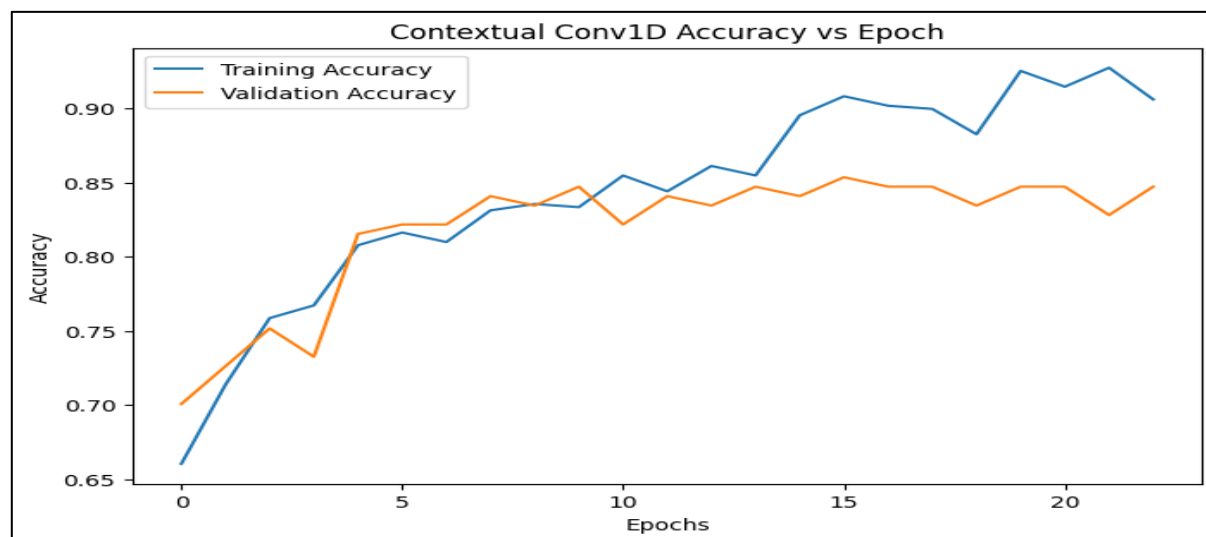


Fig 14 Contextual Conv1D Accuracy and Loss.

➤ *Biometric Model Performance*

The biometric layer provided direct identity evidence. The MobileNetV2 face model achieved approximately 97% target accuracy, with macro and weighted precision, recall, and F1-score values of about 97%. The EfficientNetB0 fingerprint model achieved approximately 93% final

accuracy, with weighted precision of 0.94, weighted recall of 0.93, and weighted F1-score of 0.93. Both biometric modalities contributed to stronger access decisions by adding measurable identity confidence before authorization was finalized.

Table 5 Biometric Model Performance Summary.

Metric	MobileNetV2 face model	EfficientNetB0 fingerprint model
Dataset size	1,090 local face images	1,013 local fingerprint images
Final/target accuracy	Approximately 97%	Approximately 93%
Best validation accuracy	98.10% at Epoch 19	93.78% at Epoch 17
Weighted precision	97%	0.94
Weighted recall	97%	0.93
Weighted F1-score	97%	0.93
Operational role	Primary identity-confidence evidence	Supporting physiological verifier

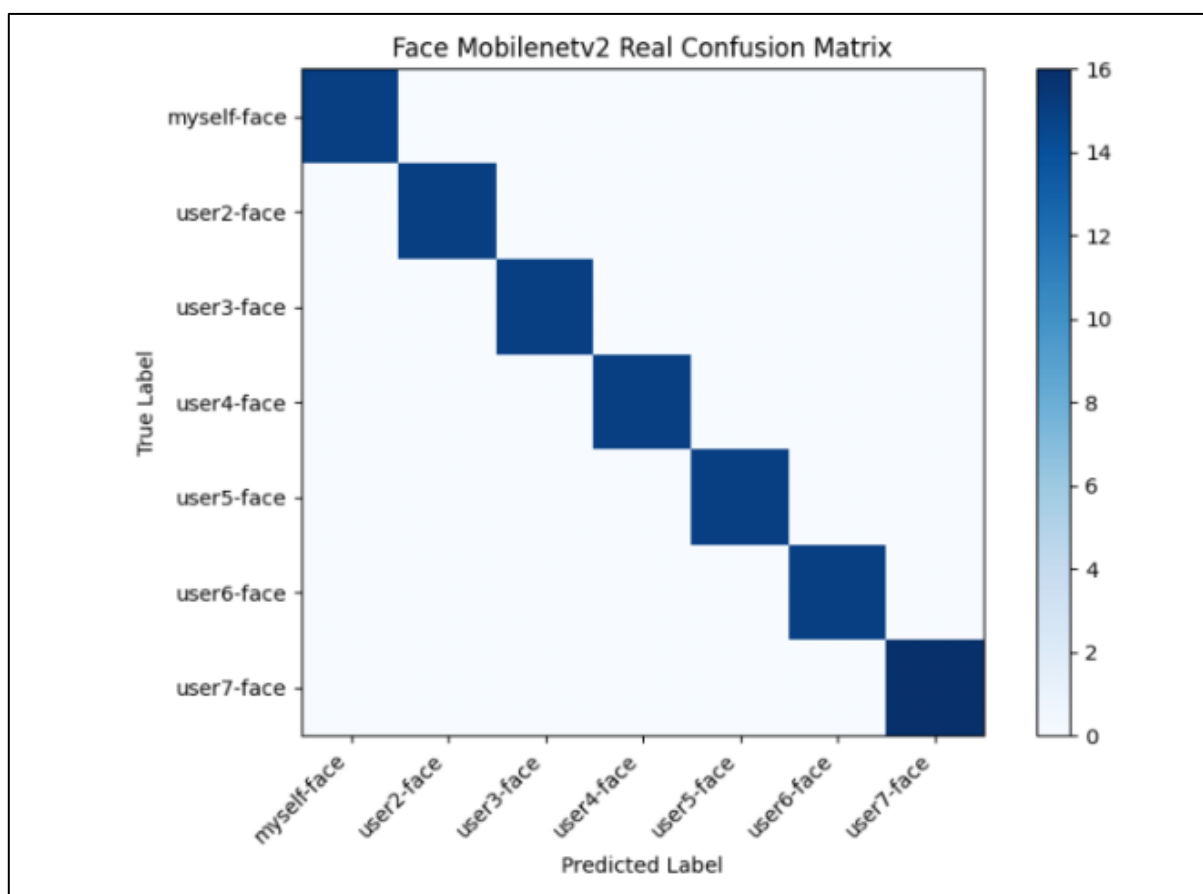


Fig 15 MobileNetV2 Face Confusion Matrix.

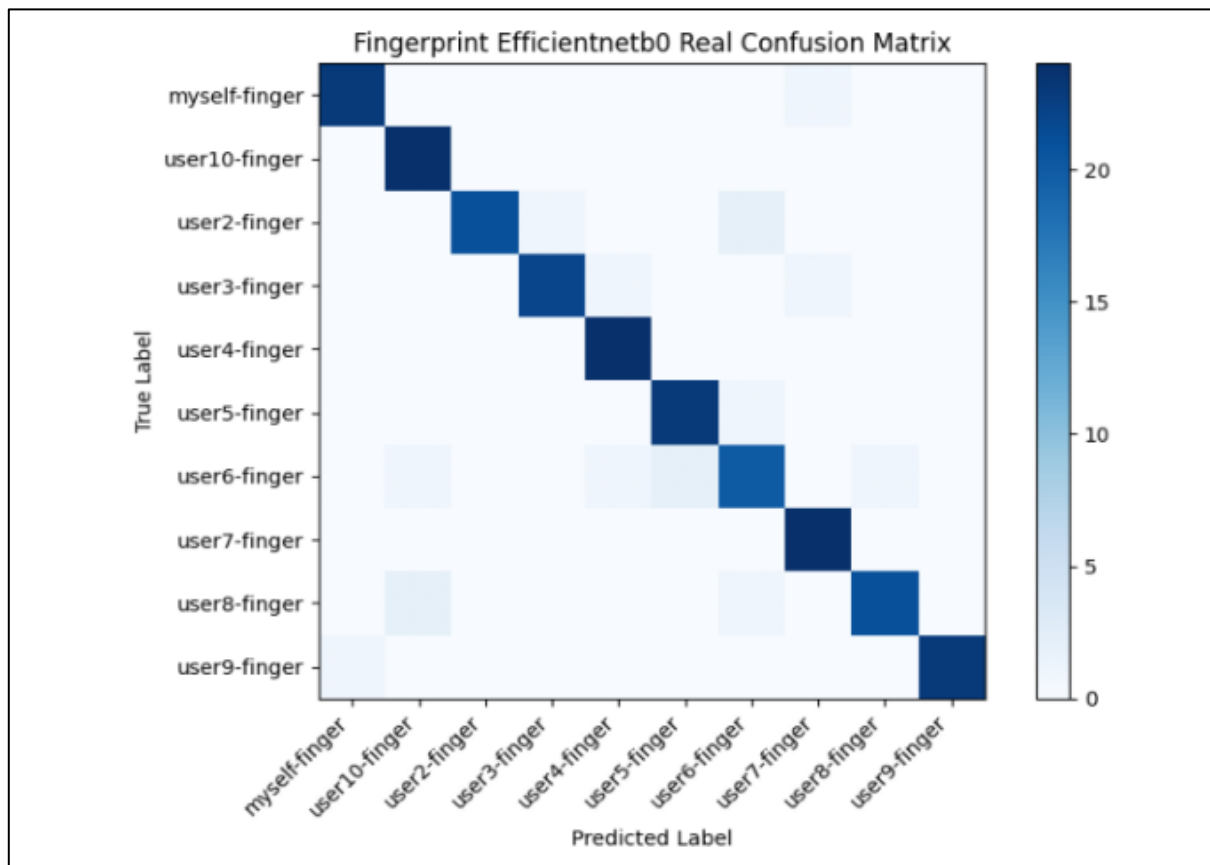


Fig 16 EfficientNetB0 Fingerprint Confusion Matrix.

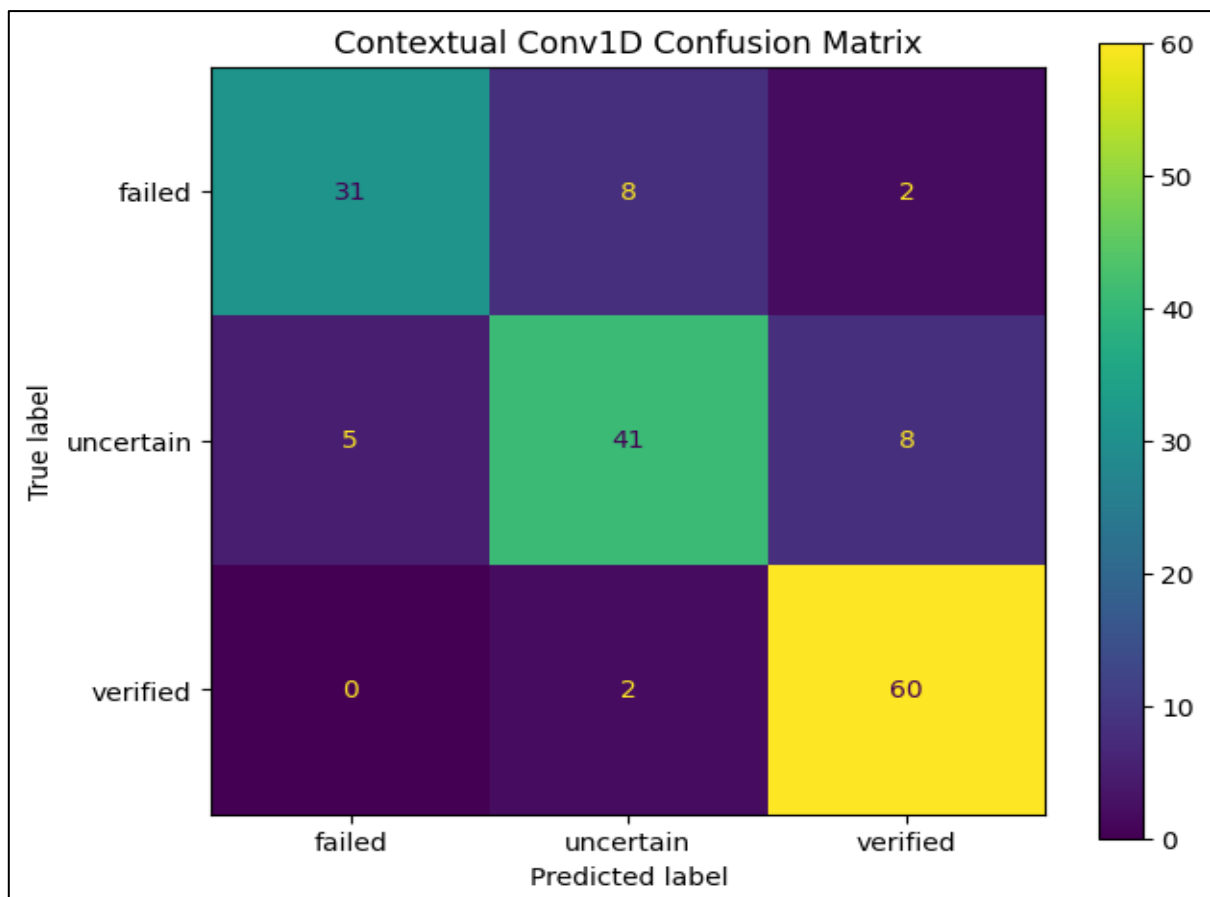


Fig 17 Contextual Conv1D Confusion Matrix.

➤ Decision Output Comparison

The contextual-only decision output established the baseline behavior of the earlier system. In that configuration, grant, step-up, and deny outcomes were produced without direct biometric identity confirmation. The biometric-enhanced decision output showed how final decisions changed after face and fingerprint evidence were introduced.

The direct contextual-versus-enhanced comparison graph and the decision transition heatmap showed that biometric verification did not merely duplicate the contextual result. Some requests that appeared acceptable under context alone were redirected to step-up or deny decisions when biometric confidence was weak. This confirms that biometric integration strengthened the final decision logic and reduced overdependence on contextual trust.

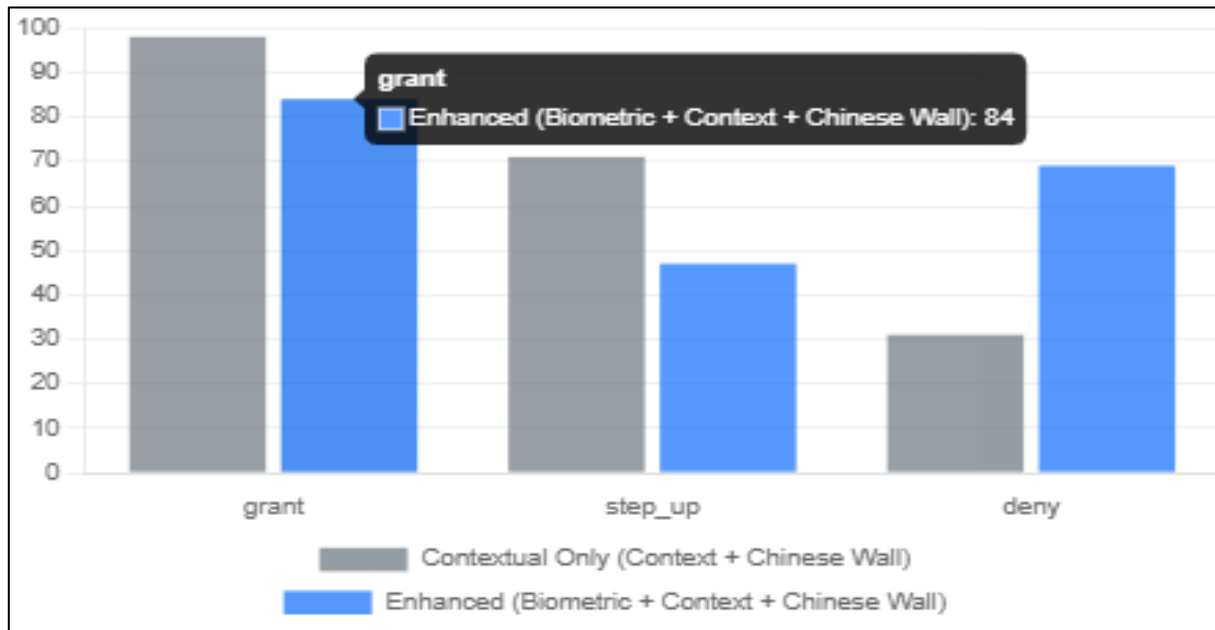


Fig 18 Contextual Versus Biometric-Enhanced Decision Comparison.

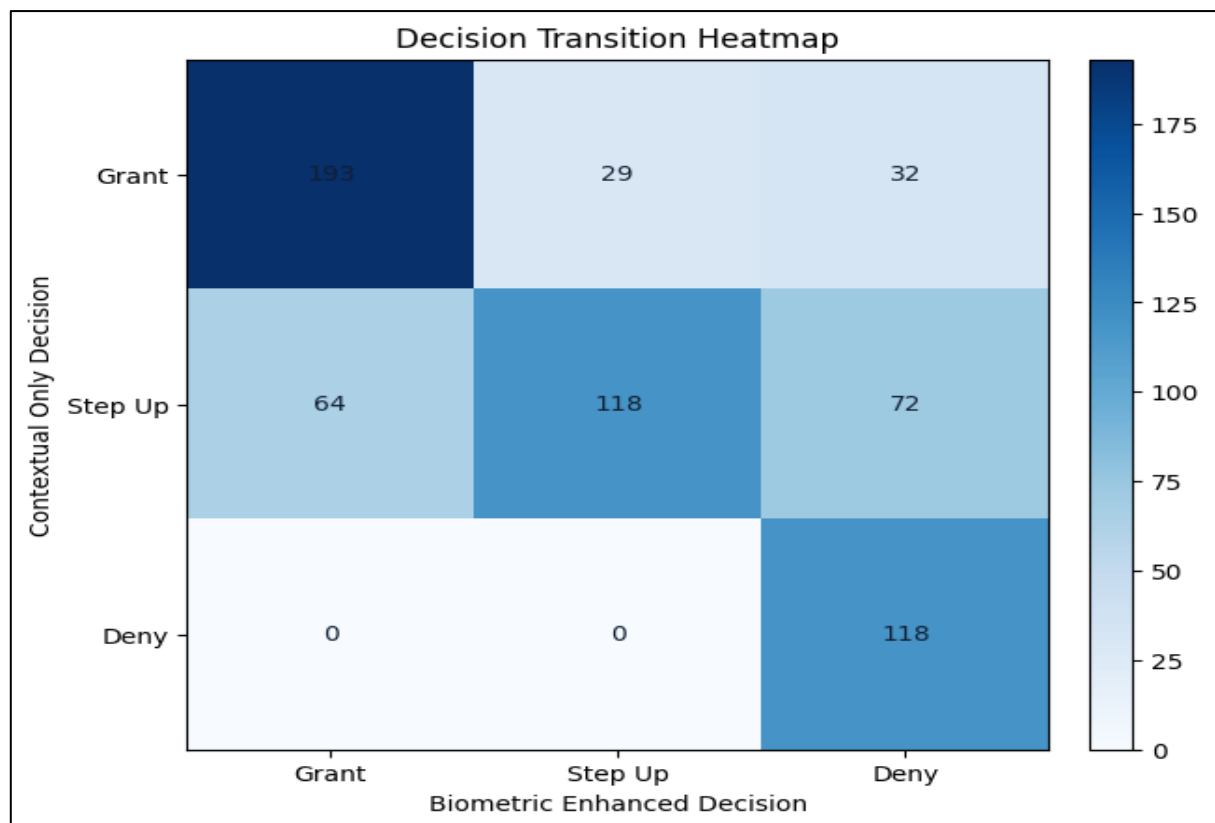


Fig 19 Decision Transition Heatmap.

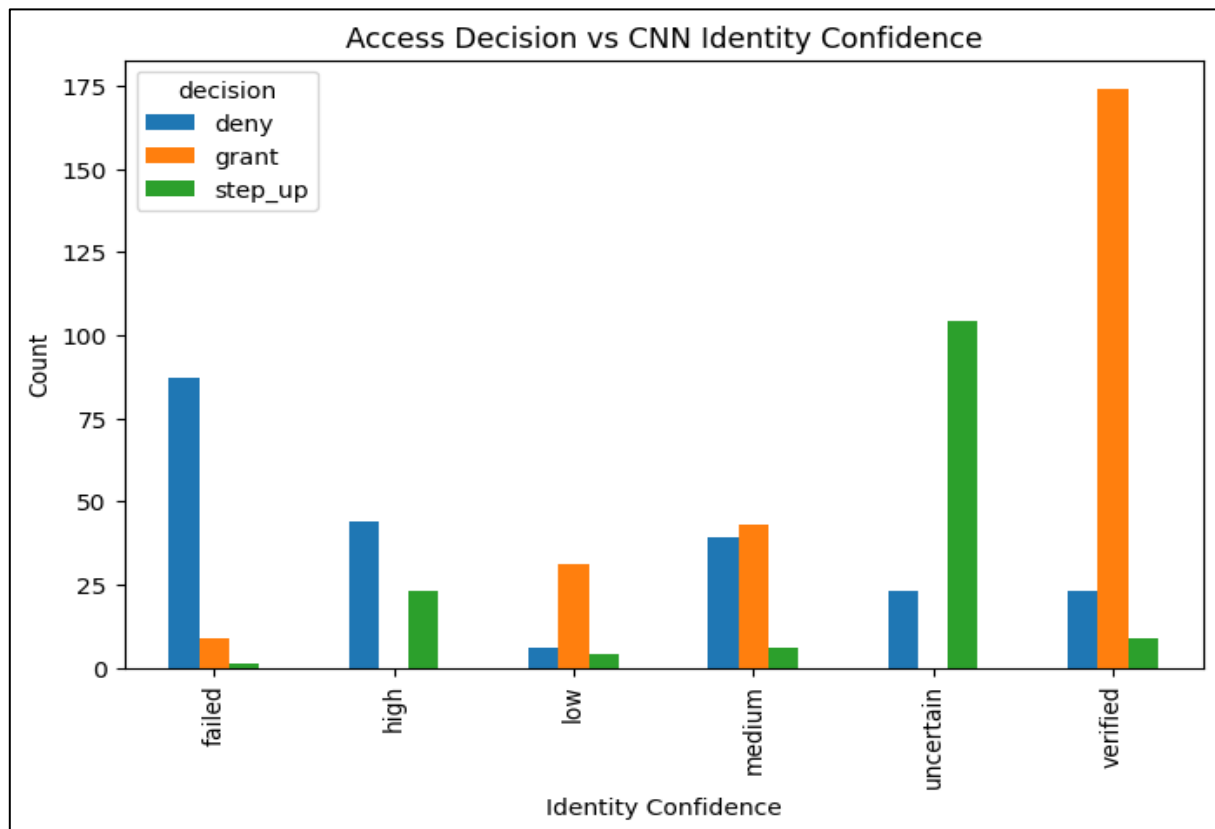


Fig 20 Access Decision Versus CNN Identity Confidence.

➤ FAR/FRR and Security-Sensitive Evaluation

The FAR and FRR analysis supported the practical security interpretation of the enhanced system. The FAR versus FRR curve showed the expected trade-off between false acceptance and false rejection as the biometric threshold changed. A lower false acceptance rate reduces the chance of unauthorized access, while a lower false rejection rate protects usability for genuine users.

This security-sensitive evaluation is important because an edge access-control system should not be judged by raw accuracy alone. The threshold selected for deployment must balance protection against impersonation with reliable service for legitimate users.

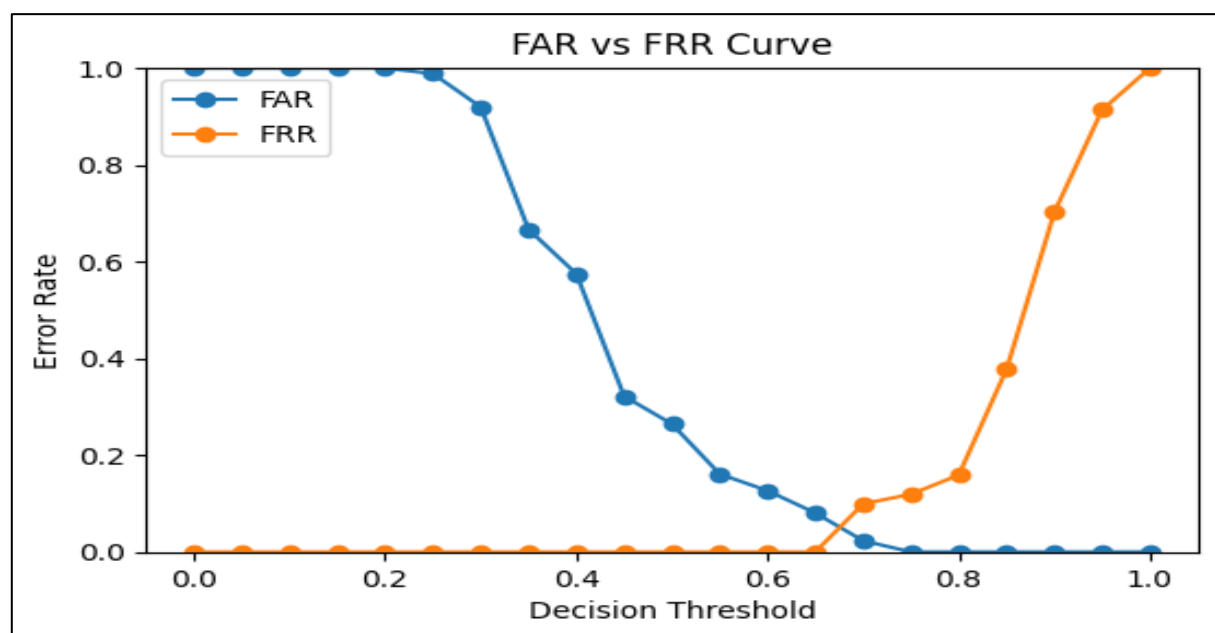


Fig 21 FAR Versus FRR Curve.

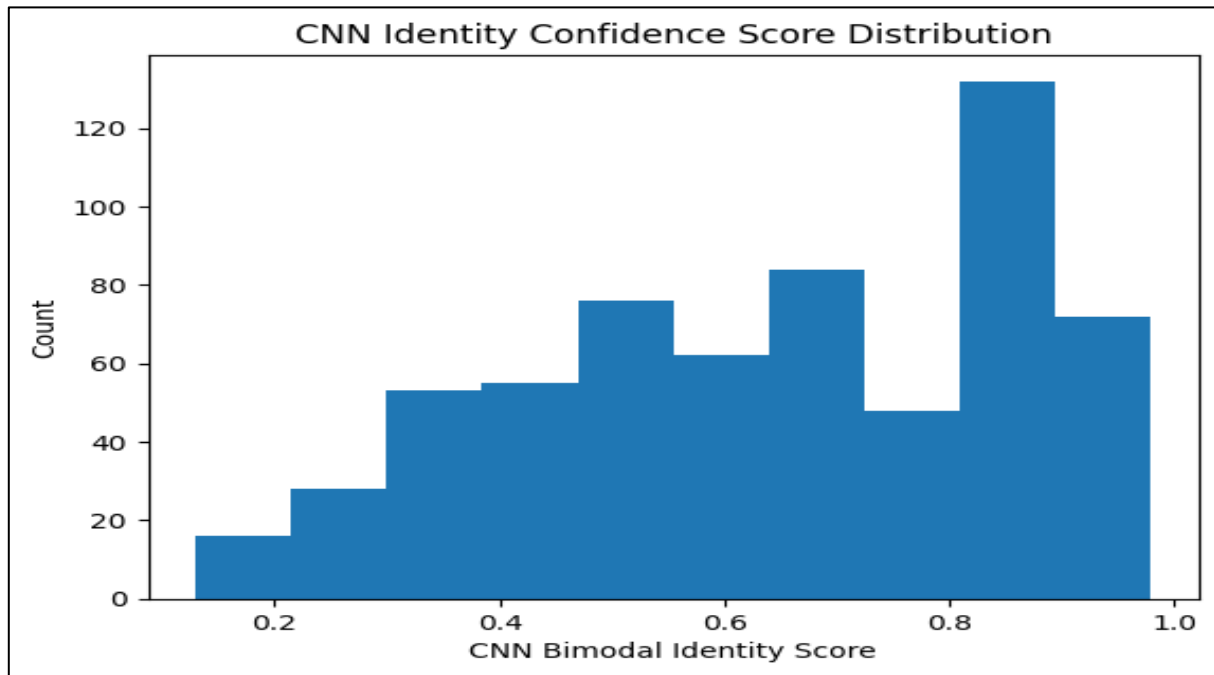


Fig 22 Risk Score Distribution.

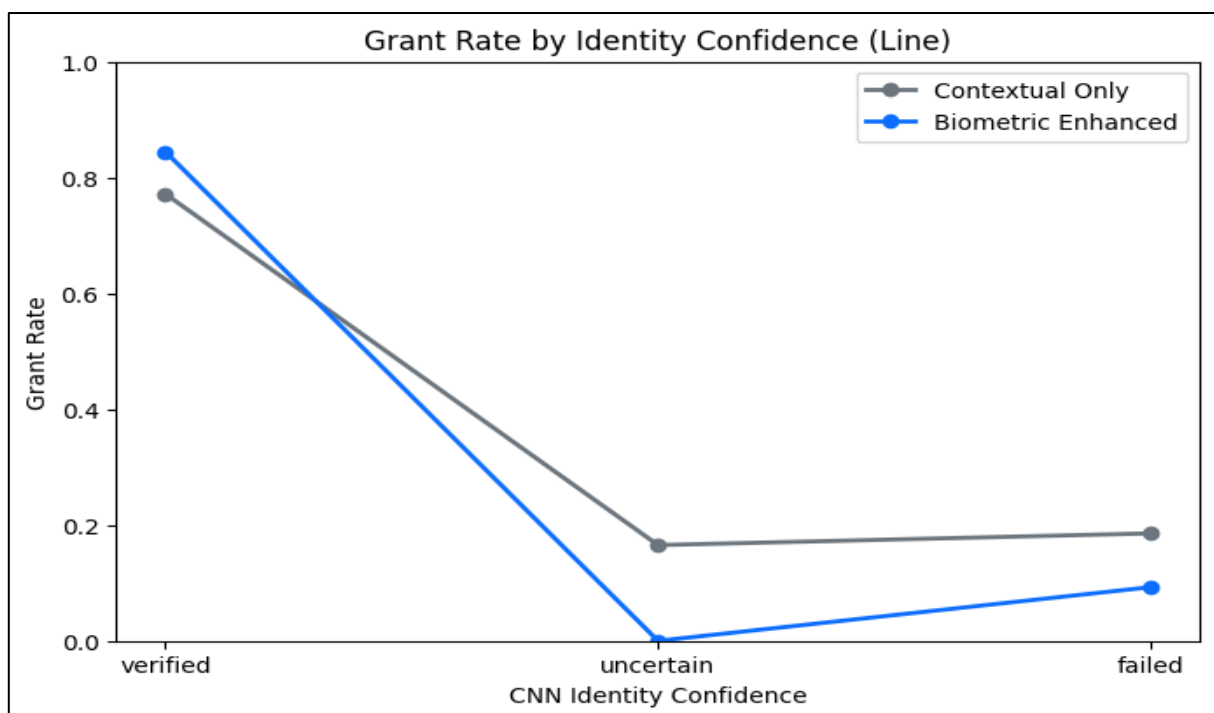


Fig 23 Grant by Biometric Identity Confidence in the Enhanced System.

V. DISCUSSION

The results indicate that contextual-only access control is useful but incomplete. Contextual models can identify suspicious conditions and support adaptive responses, but they cannot directly prove who is making the access request. This weakness is critical in edge environments, where compromised devices, stolen credentials, and manipulated attributes may create apparently legitimate access contexts.

The machine learning-enhanced biometric system improved the baseline by adding direct physical identity

evidence. Face recognition provided a convenient and strong identity-confidence signal, while fingerprint recognition supplied an additional physiological verifier. By combining both modalities with contextual risk and Chinese Wall policy enforcement, the system made final decisions using identity, context, and authorization policy together.

The decision-output comparison strengthens the publication value of the work. The contextual-only output shows baseline behavior, the biometric-enhanced output shows the improved behavior after biometric infusion, and the transition heatmap shows how individual decisions moved

between grant, step-up, and deny states. Together, these outputs demonstrate that biometric integration improved decision quality rather than simply adding another login step.

The findings also support edge deployment. Processing authentication and authorization near the access point improves responsiveness and limits unnecessary transmission of sensitive biometric evidence. This makes the framework suitable for universities, hospitals, banks, data centers, and distributed enterprise systems that require rapid but security-aware access decisions.

VI. CONCLUSION

This paper evaluated contextual-only and machine learning-enhanced biometric access-control systems in an edge computing environment. The contextual-only baseline supported adaptive risk reasoning and Chinese Wall policy enforcement, but it lacked direct identity verification. The enhanced system addressed this limitation by integrating MobileNetV2 face recognition, EfficientNetB0 fingerprint recognition, 1D CNN/Conv1D contextual analysis, biometric fusion, and policy-based authorization. The results show that the enhanced approach provides stronger identity assurance, improved decision quality, and better suitability for real-time edge access-control deployment.

RECOMMENDATIONS

Future work should expand the local biometric dataset to improve generalization across more users, devices, and capture conditions.

Further threshold calibration should be carried out to reduce false acceptance and false rejection rates.

The contextual and biometric fusion strategy should be tested in larger real-world edge deployments.

Future experiments should compare contextual-only, biometric-only, and fully fused access-control decisions.

Additional biometric modalities such as iris recognition may be introduced to evaluate tri-modal access-control performance.

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*, vol. 1, p. 100015, 2023.
- [2]. Satyanarayanan, M., "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30-39, 2017.
- [3]. 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*, vol. 219, p. 103726, 2023.
- [4]. Kaur, K., Garg, S., Aujla, G. S., Kumar, N., Rodrigues, J. J. P. C., and Guizani, M., "Edge computing in the industrial Internet of Things environment: Software-defined-networks-based edge-cloud interplay," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 44-51, 2018.
- [5]. Muhammad, A., et al., "Dynamic access control at the network edge using adaptive risk-based access control systems," 2024.
- [6]. Brewer, D. F. C. and Nash, M. J., "The Chinese Wall security policy," *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 206-214, 1989.
- [7]. Chandramouli, R. and Butcher, Z., "A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments," *National Institute of Standards and Technology*, 2023.
- [8]. Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., and Scarfone, K., "Guide to Attribute Based Access Control (ABAC) Definition and Considerations," *NIST Special Publication 800-162*, 2014.
- [9]. Rahman, A., et al., "Risk-adaptive access control using machine learning for cyber-physical systems," 2022.
- [10]. Prokhorenkova, L., Gusev, G., Vorobev, A., Dorogush, A. V., and Gulin, A., "CatBoost: Unbiased boosting with categorical features," *Advances in Neural Information Processing Systems*, 2018.
- [11]. Sandler, M., Howard, A., Zhu, M., Zhmoginov, A., and Chen, L. C., "MobileNetV2: Inverted residuals and linear bottlenecks," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 4510-4520, 2018.
- [12]. Tan, M. and Le, Q. V., "EfficientNet: Rethinking model scaling for convolutional neural networks," *Proceedings of the International Conference on Machine Learning*, pp. 6105-6114, 2019.
- [13]. Jain, A. K., Ross, A., and Prabhakar, S., "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20, 2004.
- [14]. Ross, A. and Jain, A. K., "Multimodal biometrics: An overview," *Proceedings of the European Signal Processing Conference*, pp. 1221-1224, 2004.
- [15]. Cao, Q., Shen, L., Xie, W., Parkhi, O. M., and Zisserman, A., "VGGFace2: A dataset for recognising faces across pose and age," *Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition*, pp. 67-74, 2018.
- [16]. Ruiz Garcia, S., "SOCOFing: Sokoto Coventry Fingerprint Dataset," *Kaggle*, 2018.