

Comparative Analysis of MobileNetV2 and EfficientNetB0 for Face and Fingerprint Recognition in Machine Learning Enhanced Access Control

Paul Ndudiri Ohia, Friday Eleonu Onuodu, Ugochi Adaku Okengwu, Evaristus Chibuzor Nwoke

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

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

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

4Department of Computer Science, University of Agriculture and Environmental Sciences Umuagwo Imo state Nigeria

ABSTRACT

This paper presents a comparative analysis of MobileNetV2 and EfficientNetB0 for face and fingerprint recognition in a machine learning-enhanced access control system. The study was developed within an edge computing security framework where biometric verification was integrated with contextual risk analysis and Chinese Wall policy enforcement. MobileNetV2 was adopted for facial recognition because of its lightweight convolutional architecture and suitability for efficient image classification. EfficientNetB0 was adopted for fingerprint recognition because of its compound scaling strategy and strong feature extraction capability. The models were trained and evaluated using locally captured real-user biometric samples organized into ten identity classes. MobileNetV2 achieved approximately 97% target accuracy for face recognition, while EfficientNetB0 achieved approximately 93.36% accuracy for fingerprint recognition. Although the face model produced higher reported classification accuracy, the fingerprint model provided strong operational stability as a physiological verifier. The findings support the use of both models in a bimodal biometric access-control framework.

Keywords- MobileNetV2, EfficientNetB0, face recognition, fingerprint recognition, machine learning, deep learning, bimodal biometrics, access control, edge computing, biometric authentication.

I. INTRODUCTION

Access control systems regulate access to protected resources by authenticating users, enforcing authorization policies, and preventing unauthorized activity. In distributed and edge computing environments, access decisions must often be made close to the point of request, with low latency and strong identity assurance [1], [2]. Conventional approaches based on passwords, access cards, and static rules are increasingly limited because they can be stolen, shared, guessed, or manipulated [3].

The thesis work on which this paper is based addressed this limitation by introducing machine learning-based bimodal biometric verification into an enhanced access control management system. The system used facial and fingerprint recognition to confirm the physical identity of the requester before final access decisions were made. These biometric outputs were combined with contextual risk analysis and Chinese Wall policy enforcement to produce stronger and more explainable access decisions [4], [5].

This paper focuses on the comparative performance of the two deep learning models used in the biometric layer: MobileNetV2 for face recognition and EfficientNetB0 for fingerprint recognition. The comparison is important because both modalities support identity verification, but they differ in capture method, image structure, practical stability, and sensitivity to environmental conditions.

II. RELATED WORK

Deep learning has become a major technique in biometric authentication because convolutional neural networks can automatically learn discriminative identity features from image data [6], [7]. In face recognition, CNN models learn facial structure, texture, and spatial relationships. In

fingerprint recognition, CNN models learn ridge patterns, texture distributions, and local fingerprint structures that support identity classification and verification [8].

MobileNetV2 is suited to efficient computer vision tasks because it uses inverted residual blocks and depthwise separable convolution to reduce computational cost [9]. This makes it useful for edge computing environments where authentication should be fast and resource-aware. EfficientNetB0 uses compound scaling to balance network depth, width, and image resolution, making it a strong candidate for fingerprint image recognition where fine-grained texture features are important [10].

Although face and fingerprint recognition can operate as unimodal authentication methods, combining both in an access-control system can improve identity assurance [11], [12]. Face recognition is convenient and contactless, but may be affected by pose, lighting, expression, background, or camera quality. Fingerprint recognition is generally more stable because fingerprint ridge patterns are distinctive and persistent, but scanner quality, finger pressure, and placement can affect capture quality.

III. MATERIALS AND METHODS

A. Bimodal Biometric Access-Control Architecture

The implemented access-control system combined bimodal biometric verification, edge computing, and policy enforcement. MobileNetV2 was used for facial recognition, while EfficientNetB0 performed fingerprint recognition. Their outputs were fused to generate an identity-confidence

score. Biometric data were processed locally at the edge, reducing authentication delay, network traffic, cloud dependence, and exposure of sensitive biometric information. The Chinese Wall policy prevented conflict-of-interest access across protected datasets. The system combined biometric evidence and policy restrictions to produce a grant, step-up, or deny decision.

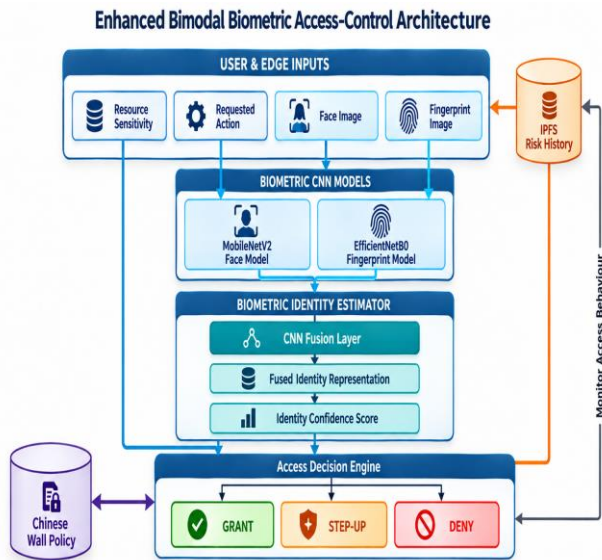


Fig.1: Architecture face and Fingerprint Recognition in Machine Learning Enhanced Access Control

B. Dataset Preparation

The face dataset was captured through the webcam interface of the developed system and organized into ten identity folders: myself-face and user2-face through user10-face. The fingerprint dataset was captured through the integrated fingerprint scanner and organized into ten corresponding identity folders: myself-finger and user2-finger through user10-finger. Each folder represented one enrolled user identity and acted as the class label for supervised model training.

The final local face dataset contained 1,090 real-user images, while the fingerprint dataset contained 1,013 real-user images. Images were reviewed, resized, normalized, label-encoded, and split into training and validation subsets. Face augmentation included controlled rotations, shifts, zoom, brightness variation, and horizontal flipping. Fingerprint augmentation was applied more conservatively to avoid distorting ridge structure.

TABLE I. DATASET AND MODEL SUMMARY

Dataset	Model	Classes	Samples	Training role
Face images	MobileNetV2	10	1,090	Facial identity classification and verification
Fingerprint images	EfficientNetB0	10	1,013	Fingerprint identity classification and verification



Fig.2: local face dataset sample.]

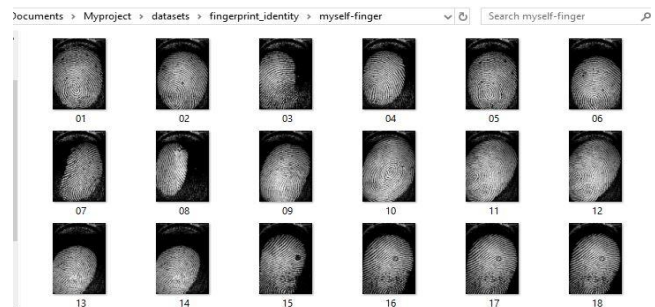


Fig3: local fingerprint dataset sample

C. Model Training Procedure

For face recognition, images were resized to the MobileNetV2 input dimension, normalized, label-encoded, and passed into the CNN training pipeline. The model was trained for 20 epochs and evaluated using training accuracy, validation accuracy, training loss, validation loss, precision, recall, F1-score, support, and confusion matrix interpretation.

For fingerprint recognition, samples were resized to 224 x 224 pixels, normalized, label-encoded, and trained using EfficientNetB0 for 20 epochs. The models were selected to support real-time access control in an edge computing environment. MobileNetV2 supports efficient facial feature extraction, while EfficientNetB0 supports strong fingerprint feature learning with manageable computational cost.

IV. RESULTS

A. MobileNetV2 Face Recognition Performance

The MobileNetV2 face recognition model showed strong progressive learning over 20 epochs. Training accuracy increased from 30.33% at Epoch 1 to 98.05% at Epoch 20. Validation accuracy increased from 56.79% at Epoch 1 to 97.14% at Epoch 20, with the highest validation accuracy of 98.10% recorded at Epoch 19. The classification report showed approximately 97% target accuracy, with macro and weighted precision, recall, and F1-score values of 97%.

TABLE II. MOBILENETV2 FACE RECOGNITION RESULT

Metric	Result
Initial training accuracy	30.33% at Epoch 1
Final training accuracy	98.05% at Epoch 20

Initial validation accuracy	56.79% at Epoch 1
Final validation accuracy	97.14% at Epoch 20
Highest validation accuracy	98.10% at Epoch 19
Target classification accuracy	Approximately 97%
Macro/weighted average	97% precision, recall, and F1-score

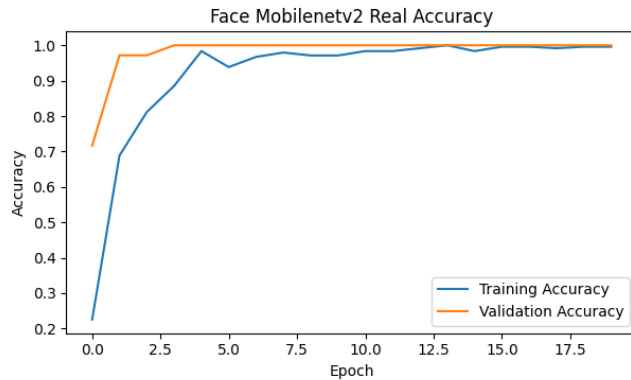


Fig.4: MobileNetV2 face training accuracy and validation accuracy graph.

This graph shows the training and validation accuracy of the MobileNetV2 face recognition model across epochs. It indicates how well the model learned facial identity features from the training dataset and how effectively it generalized to unseen validation samples.

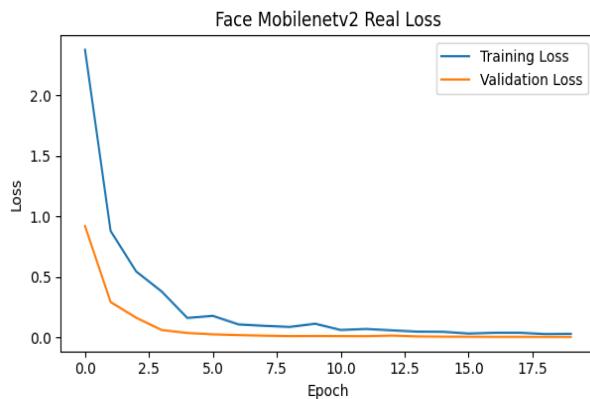


Fig.5: MobileNetV2 face training loss and validation loss graph.

This graph presents the training and validation loss of the MobileNetV2 face recognition model. A decreasing loss trend shows that the model improved during training, while the gap between training and validation loss helps indicate whether over fitting occurred.

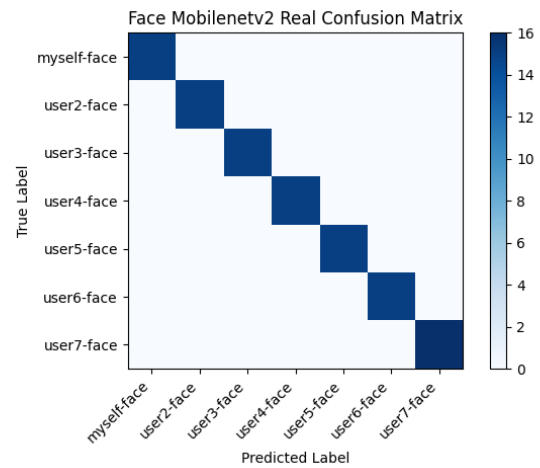


Fig.6: MobileNetV2 face confusion matrix

This confusion matrix shows the classification performance of the MobileNetV2 face recognition model across enrolled face classes. It helps identify correct predictions, misclassifications, and the overall reliability of the face recognition model.

B. EfficientNetB0 Fingerprint Recognition Performance

The EfficientNetB0 fingerprint recognition model also showed consistent improvement during training. Validation accuracy increased from 54.36% at Epoch 1 to 90.04% at Epoch 10. The highest validation accuracy was 93.78% at Epoch 17, while the final evaluation produced approximately 93.36% accuracy. The classification report showed 0.94 weighted precision, 0.93 weighted recall, and 0.93 weighted F1-score across 241 support samples.

TABLE III. EFFICIENTNETB0 FINGERPRINT RECOGNITION RESULT

Metric	Result
Initial training accuracy	21.82% at Epoch 1
Final training accuracy	84.62% at Epoch 20
Initial validation accuracy	54.36% at Epoch 1
Final validation accuracy	93.36% at Epoch 20
Highest validation accuracy	93.78% at Epoch 17
Final classification accuracy	Approximately 93%
Macro/weighted average	0.94 precision, 0.93 recall, and 0.93 F1-score

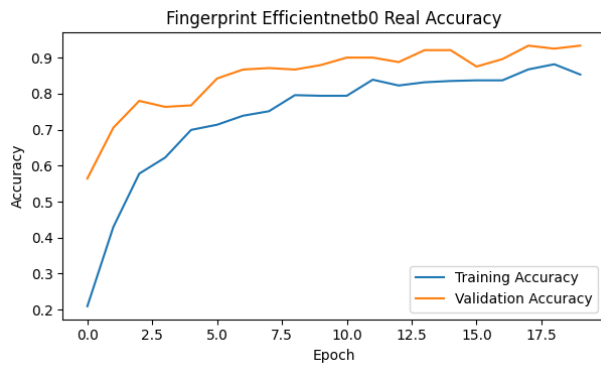


Fig.7: EfficientNetB0 fingerprint training accuracy and validation accuracy graph.

This graph shows how the EfficientNetB0 fingerprint model improved during training. The training and validation accuracy indicate how well the model learned fingerprint patterns and how effectively it performed on unseen validation samples.

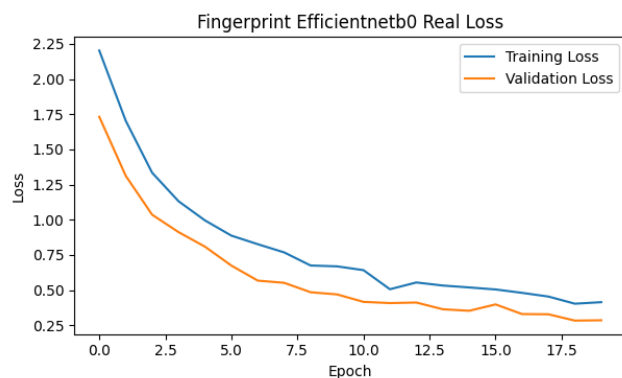


Fig.8: EfficientNetB0 fingerprint training loss and validation loss graph.

This graph shows the training and validation loss across epochs. A decreasing loss value means the model was learning effectively, while the difference between training and validation loss helps show whether the model was over fitting or generalizing well.

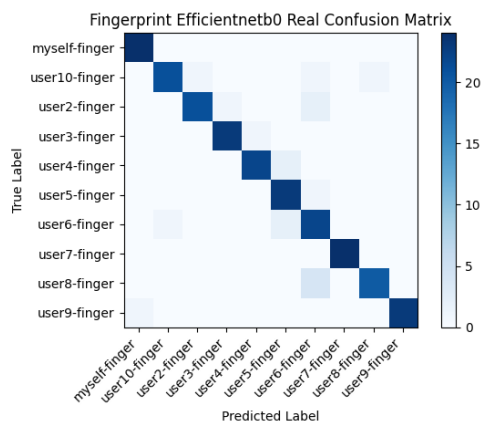


Fig.9: EfficientNetB0 fingerprint confusion matrix

The confusion matrix shows the number of correct and incorrect fingerprint classifications across different user classes. It helps identify how accurately the model recognized enrolled fingerprints and where misclassification occurred.

C. Comparative Model Analysis

A direct comparison shows that MobileNetV2 achieved the higher reported target classification accuracy, while EfficientNetB0 demonstrated strong practical stability as a biometric verifier in the implemented system. The face model reached approximately 97% target accuracy and showed high class-level precision, recall, and F1-score. The fingerprint model reached approximately 93% final accuracy and showed strong weighted averages.

The comparison also shows that the two models serve complementary roles. MobileNetV2 provides fast and convenient face-based evidence, while EfficientNetB0 provides fingerprint-based physiological evidence. In an access-control system, this complementarity is useful because the weakness of one modality can be reduced by the strength of the other.

Table Iv. Comparative Analysis Of The Two Biometric Models

Comparison item	MobileNetV2 face model	EfficientNetB0 fingerprint model
Biometric modality	Face recognition	Fingerprint recognition
Local samples	1,090 face images	1,013 fingerprint images
Final reported accuracy	Approximately 97%	Approximately 93.36%
Best validation accuracy	98.10% at Epoch 19	93.78% at Epoch 17
Operational role	Convenient identity evidence	Stable physiological verifier
Main sensitivity	Lighting, pose, expression, camera distance	Finger pressure, placement, scanner quality

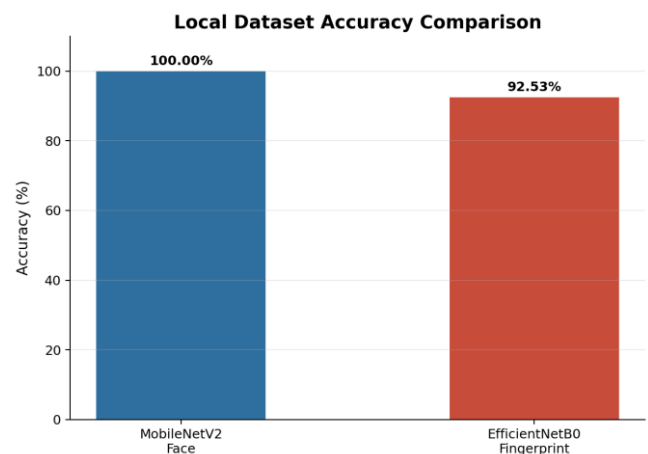


Fig.10: comparison chart of MobileNetV2 and EfficientNetB0 accuracy.

Fig.10: comparison graph compares the performance of the

two biometric models on the locally captured dataset. MobileNetV2 achieved higher face recognition accuracy, while EfficientNetB0 also showed strong fingerprint recognition performance, demonstrating that both models are suitable for local biometric access control.

D. Security Interpretation

In access control, biometric model performance must be interpreted beyond ordinary classification accuracy. A model that performs well in training must also support secure, dependable, and usable identity verification. The MobileNetV2 model contributes convenience because face recognition is contactless and fast. However, it may be influenced by environmental conditions such as lighting and pose.

The EfficientNetB0 fingerprint model contributes strong physiological distinctiveness and was found to be stable in the implemented system, but it depends on scanner quality and user placement consistency. The combined use of both models improves the access-control system because the weakness of one biometric modality can be compensated by the strength of the other.

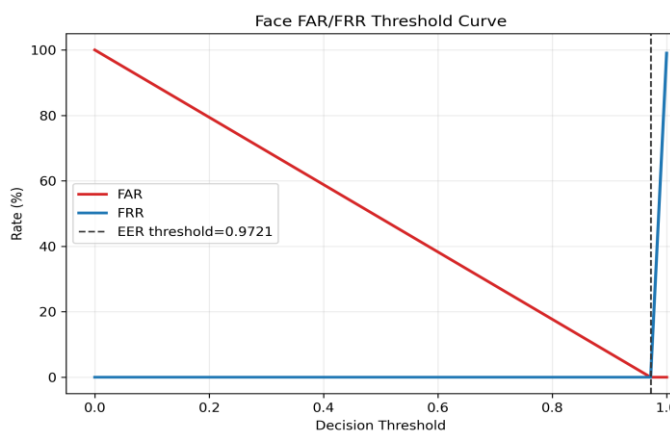


Fig.11: FAR/FRR curve or biometric threshold analysis.

This graph shows how the face recognition model balances false acceptance and false rejection at different thresholds. A low FAR means impostors are rarely accepted, while a low FRR means genuine users are rarely rejected.

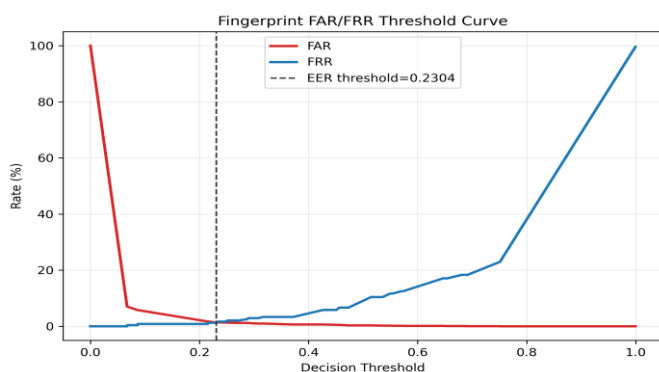


Fig.12: Fingerprint FAR/FRR curve.

This graph shows the threshold behavior of the fingerprint model. It helps identify the point where fingerprint verification provides a good balance between security and user convenience.

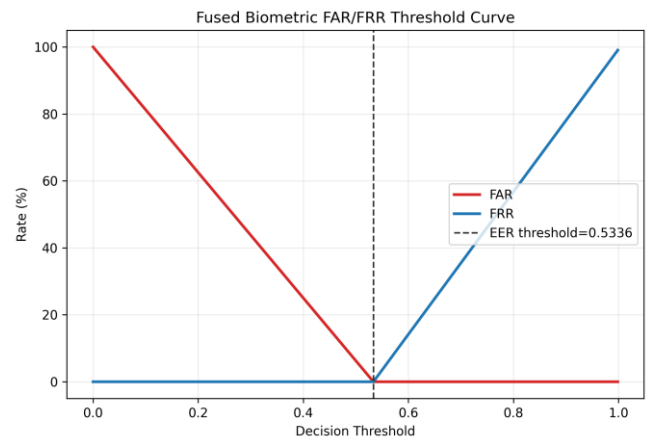


Fig.13: Fused face and fingerprint biometric FAR/FRR curve

This graph combines face and fingerprint verification scores. It gives a stronger overall decision because both biometric traits are considered together, reducing dependence on one model alone.

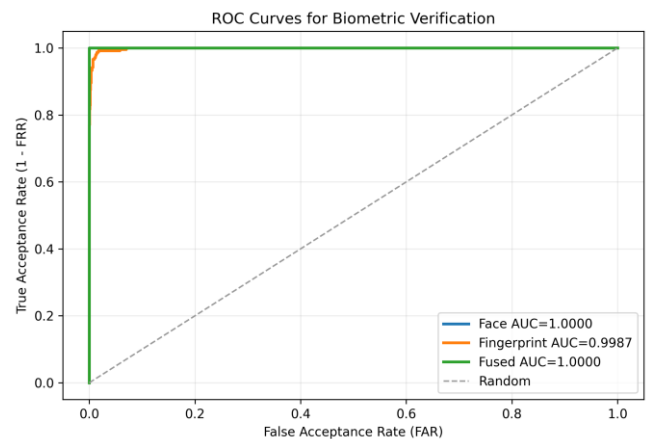


Fig.14: ROC curves for face, fingerprint, and fused biometric verification

The ROC curves show the ability of each system to separate genuine users from impostors. Curves closer to the top-left corner indicate stronger verification performance. The FAR/FRR curve shows how the biometric system performs at different decision thresholds. FAR represents the rate at which impostors are wrongly accepted, while FRR represents the rate at which genuine users are wrongly rejected. As the threshold changes, the system balances security and usability. A lower FAR improves security, while a lower FRR improves user convenience. The point where FAR and FRR are closest helps identify a suitable

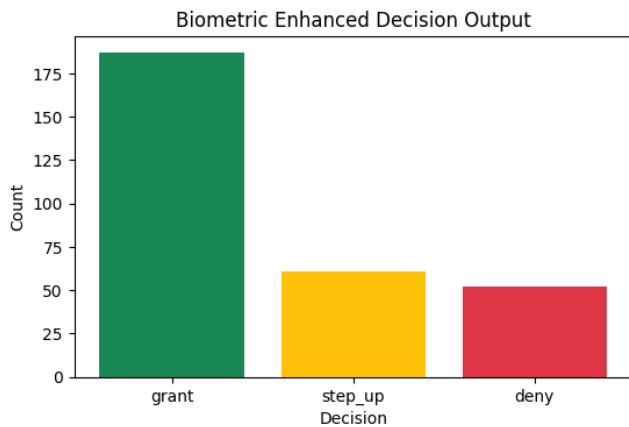


Fig.15: biometric-enhanced access decision output

This graph shows the final access decisions after biometric verification was added to the system. Instead of relying only on contextual factors such as device, location, time, or risk level, the system also considers face and fingerprint identity confidence before granting access.

A) Impact on Access Control

The biometric-enhanced output improves access control by reducing the chance of granting access to an impostor using a trusted device or location. It strengthens identity assurance, supports better grant, step-up, and deny decisions, and makes the access control system more secure and reliable in an edge computing environment.

V. DISCUSSION

The results indicate that MobileNetV2 and EfficientNetB0 are both suitable for machine learning-enhanced biometric access control, but they contribute different operational advantages. MobileNetV2 produced the stronger headline accuracy in the face-recognition task. This supports its usefulness where fast facial identity recognition is needed in an edge-based access point.

EfficientNetB0 produced slightly lower final classification accuracy, but its fingerprint modality remained important as a stable physiological verifier. This distinction is important because the best model for access control is not always the one with the highest classification percentage. Security systems require dependable capture behavior, consistent verification, and resistance to practical misuse.

The comparative findings also support the decision to use bimodal biometrics rather than a unimodal design. A face-only system may be convenient but more sensitive to environmental changes, while a fingerprint-only system may be stable but requires direct sensor contact and consistent user placement. Combining both modalities improves identity assurance and makes the access-control decision more robust.

VI. CONCLUSION

This paper compared MobileNetV2 and EfficientNetB0 for face and fingerprint recognition in a machine learning-enhanced access-control system. MobileNetV2 achieved approximately 97% target accuracy for face recognition, while EfficientNetB0 achieved approximately 93.36% final accuracy for fingerprint recognition. The face model produced higher reported classification performance, while the fingerprint model contributed strong physiological verification. The study concludes that both models are valuable in a bimodal biometric access-control framework, with MobileNetV2 supporting convenient facial verification and EfficientNetB0 strengthening fingerprint-based identity assurance.

VII. CONTRIBUTION TO KNOWLEDGE

- I. This study contributes to knowledge by demonstrating the value of locally captured biometric datasets in real-time access control systems. It shows that models trained with local face and fingerprint samples can better reflect the actual users, devices, and environmental conditions of the deployment setting, leading to more reliable authentication decisions.
- II. The study also highlights the practical benefit of adopting local datasets for real-time systems. When an access control system is trained on data collected from its real users, it can improve recognition accuracy, reduce false rejection of genuine users, and strengthen detection of unauthorized attempts. This makes local dataset training useful for secure, responsive, and operationally ready access control in environments such as offices, schools, hospitals, and banking systems.

VIII. RECOMMENDATIONS

Future work should expand the real-user face and fingerprint datasets to improve model generalization and reduce false acceptance and false rejection rates.

Threshold calibration should be strengthened so the system can balance security and usability under different access-risk levels.

Further experiments should test model performance on larger enrolled-user populations and in real deployment locations such as universities, healthcare facilities, banks, and enterprise offices.

Future work should explore score-level fusion between MobileNetV2 and EfficientNetB0 outputs to improve final biometric confidence estimation.

A third modality such as iris recognition may be introduced to compare bimodal and tri-modal biometric access-control performance.

REFERENCES

- [1] Satyanarayanan, M., “The emergence of edge computing,” *Computer*, vol. 50, no. 1, pp. 30-39, 2017.
- [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*, vol. 219, p. 103726, 2023.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] Goodfellow, I., Bengio, Y., and Courville, A., *Deep Learning*. Cambridge, MA: MIT Press, 2016.
- [7] 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.
- [8] Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S., *Handbook of Fingerprint Recognition*. London, U.K.: Springer, 2009.
- [9] 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.
- [10] 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.
- [11] Ross, A. and Jain, A. K., “Multimodal biometrics: An overview,” *Proceedings of the European Signal Processing Conference*, pp. 1221-1224, 2004.
- [12] Alay, N., Al-Bashish, D., Alsmirat, M., Alsswey, A., Alawin, A., and Maqableh, W., “Deep-learning multimodal biometric system using face, iris, and fingerprint images,” 2020.
- [13] LeCun, Y., Bengio, Y., and Hinton, G., “Deep learning,” *Nature*, vol. 521, pp. 436-444, 2015.