IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 11 ISSUE : 05 Print / Issue Publication Date: September 2026

ISSN : 2455-2143

Indexed In

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 05, ISSN No. 2455-2143, Pages 01-11
Published Online September 2026 in IJEAST (http://www.ijeast.com)

DESIGN AND SIMULATION OF AN ANN–CNN-BASED MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEM FOR IOT ACCESS CONTROL APPLICATIONS

U. M. Akpan, E. H. Johnson, U. S. Ukommi
Department of Electrical/Electronic Engineering,
Akwa Ibom State University, Ikot Akpaden, Nigeria

Abstract: **The Internet of Things (IoT) is growing fast, with smart devices spreading into just about every area you can imagine. But as the number and variety of these devices shoot up, so do the security headaches. Old-school authentication like passwords, PINs, or tokens just isn't cutting it anymore. These methods are easy targets for phishing, brute-force attacks, stolen credentials, and all sorts of spoofing tricks. And since most IoT devices don't have much computing power, you can't just throw heavy-duty security algorithms at the problem.**

Biometric authentication sounds like a solid step up, but it's not bulletproof either. Using a single kind of biometric, like a fingerprint or face scan, on its own leaves you open to spoofing, sensor issues, errors from the environment, and mistakes where people get wrongly accepted or turned away.

In this paper, we lay out a new take: a multimodal biometric authentication system built for IoT access control, powered by Artificial Neural Networks (ANN) and Convolutional Neural Networks (CNN). Here's how it works. The system uses an ANN to check fingerprints and a CNN to recognize faces. Then, it fuses the scores from both models, making the final decision more accurate and reliable. We built and tested the system in MATLAB/Simulink.

Results were promising. Fingerprint recognition with the ANN hit a 93.5% accuracy rate, and the CNN-based facial recognition scored 96.3%. But when we combined them, things got even better the fused model reached a training accuracy of 99.0% and a validation accuracy of 98.5%. Plus, it slashed both the False Acceptance Rate (FAR) and False Rejection Rate (FRR), making it a robust choice.

In all, this multimodal biometric system gives IoT environments a more secure, lightweight, and efficient way to manage access something that fits the limits of resource-constrained smart devices but doesn't compromise on security.

I. INTRODUCTION

The Internet of Things, or IoT for short, has completely changed how we live. Everywhere you look hospitals, city streets, offices, farms, factories, and even our homes smart devices are everywhere, all talking to each other and creating what people now call "smart everything." But as more and more of these devices go online, keeping them secure and making sure only the right people or machines can access sensitive IoT networks and data has turned into a tough problem.

Old-school logins like passwords, PINs, or security tokens just aren't cutting it. They're way too easy to steal, phish, or just plain forget. And honestly, people use the same password everywhere. That's why more folks are turning to biometric authentication. Stuff like fingerprints, face scans, or voice patterns those things are unique to each of us, which makes them much harder to fake.

For example, fingerprint recognition scans the ridges and patterns on your fingers, while facial recognition looks at the details of your face, usually with barely any effort from the user. But these systems have their downsides. If the sensor's dirty, or if the light's weird, or someone tries to fool the system with a fake fingerprint or photo, things can go wrong. Sometimes these systems also mess up, letting in the wrong person or locking out the right one. That's risky if you're protecting important stuff.

That's where this paper steps in. It suggests a better way: use a combination of fingerprint and facial recognition together. To pull this off, the system taps into an Artificial Neural Network (ANN) classifier for fingerprints and a Convolutional Neural Network (CNN) for faces. The cool part? It doesn't just pick one or the other it merges their results using score-level fusion to boost accuracy, make the system more robust, and cut down on both false accepts and false rejections. The team built and tested this setup in MATLAB/Simulink to see how well it could lock down access in IoT environments.

II. LITERATURE REVIEW

The Internet of Things (IoT) has really changed how we live, letting smart devices talk to each other and share data almost everywhere you look. At its core, IoT leans on two basic pieces: smart devices themselves and something called the Web of Things, or WoT, which helps these devices interact smoothly behind the scenes. That sounds great until you realize just how fast the number of connected gadgets is exploding. With all this growth, security worries are going through the roof, especially when it comes to making sure only the right people get access and keeping data safe.

Old-school methods like passwords, PINs, and smart cards just aren't cutting it anymore. Hackers steal credentials, pull off replay attacks, and have all sorts of tricks, from phishing to brute force to just plain guessing weak passwords. Because these methods have so many holes, people are moving toward biometric authentication, which checks your identity with something unique to you maybe it's your fingerprint, the way you look, or how you move. These are much tougher for a criminal to fake or steal compared to a password you might jot down on a sticky note.

Fingerprint recognition stands out for good reason. Nobody has the same pattern of ridges and valleys on their fingers as you do. And now, Artificial Neural Networks (ANNs) help systems learn these unique patterns even more accurately, since they're great at figuring out complex relationships in fingerprint details. But here's the catch: the network's only as good as the features you feed it in other words, if your fingerprint image is blurry or the system misses some details, recognition takes a hit.

Facial recognition, on the other hand, lets you skip physical contact entirely pretty handy, especially these days. Convolutional Neural Networks (CNNs) do the heavy lifting here, picking out all sorts of facial features at different layers and making sense of faces, no matter the lighting or the way someone's looking at the camera. That's why accuracy has jumped in recent years.

But there's a way to do even better: mix and match. Multimodal biometric systems use several types of biometrics at once maybe your fingerprint and your face when checking who you are. This combo not only ramps up accuracy and reliability but also makes it way harder for someone to trick the system. Plus, it keeps false acceptances and rejections low, adding an extra layer of security.

When it comes to combining different biometric sources, score-level fusion is a go-to choice. This method blends the results from each biometric check without bogging things down with too much math or slowing the process. So, you end up with a quick, practical way to lock down access in IoT setups covering all your bases and keeping systems both secure and efficient.

B. Empirical Review

Several studies on the biometric systems have already proposed ANN-based solutions for IoT security. The existing solutions based on ANN achieve excellent recognition accuracy in conditions of quality controlled fingerprint. However, in presence of Low quality of Fingerprints, the accuracy falls down.

A CNN-based facial recognition provides excellent class accuracy; however, the training time is much higher for that model.

In the existing literature, several solutions also presented with combinations of several biometrics like Fingerprintwith Face and with Voice. Their findings suggest that multimodal biometric systems give better results in term of accuracy and security compared to unimodal systems. Despite many benefits, a majority of solutions available on the market are still too computationally intensive for resource constrained IOTdevice. We present here the contribution in this domain by a Lightweight multimodal biometrics authentication based on ANN-CNN which can be implemented in MATLAB/ Simulink.

Our score level fusing system can provide an enhanced accuracy in recognition, while it can run on an IoT devices.

C. Research Gap

While, it has been established by several research papers, few disadvantages in prevailing systems are still in practice. In prevalent systems only a single modality biometric authentication approach has been used. This will make the system vulnerable against spoofing attacks, environmental conditions, and inaccurate authentication and matching. Additionally, it has also shown that some multimodal approach will use a higher computing capability to meet their matching results, which is not feasible for the lightweight devices available with IoT devices.

Our proposed model addresses the above disadvantages by proposing lightweight ANN-CNN–based multimodal biometric authentication framework using score level fusion. The proposed model provide better authentication accuracy, less computation and provide good security.

III. METHODOLOGY

We developed and simulated an Artificial Neural Network(ANN)–Convolutional Neural Network(CNN)-based multimodal biometric authentication system that is capable of secure Internet of Things(IoT) access control applications. Our multimodal authentication system that takes fingerprint authentication and facial authentication and then apply score level fusion so that we can improve the overall authentication and will be able to increase the false rejection rate and the false acceptance rate. The whole system simulated in MATLAB/Simulink environment.

The authentication developed has three main layers as shown in Figures 1 below:

1. Sensing Layer: It takes fingerprint and face as inputs using fingerprint sensor and Pi Camera.
2. Processing Layer: This layer handles the processing of the biometric image, extraction of feature, classification using ANN and CNN classifiers, score level fusion etc.
3. Communication and Actuation Layer: This layer controls the relay operation, sends GSM alerts and provides feedback to the administrator

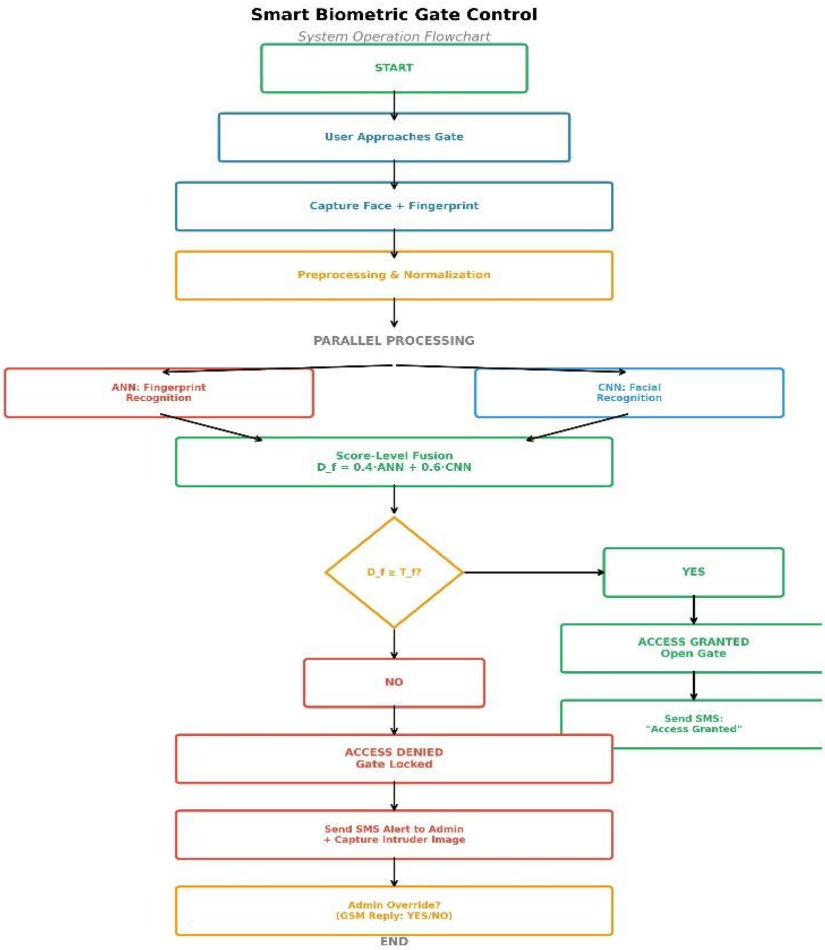


Figure 1. System Flowchart of the Smart Biometric Gate Control Process

3.1 Developed System Architecture:
The integrated biometric authentication framework defines a new authentication standard for determining user identity utilizing the spectrum of biometric modalities. The framework includes both fingerprint and face recognition; supports both score level fusion and GSM communication. The goal of this integrated system is to enhance the security associated with all facets of biometric identification and develop an integrated access control system for IoT applications. This type of system will provide a superior alternative to traditional single modality biometric systems by enabling the use of multiple modalities to make intelligent decisions when determining whether or not to grant/authenticate access; hence, reducing or eliminating the limitations associated with any one biometric modality, while providing a greater level of security against false acceptances and unauthorized accesses As shown in Figure 2 below.

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 05, ISSN No. 2455-2143, Pages 01-11
Published Online September 2026 in IJEAST (http://www.ijeast.com)

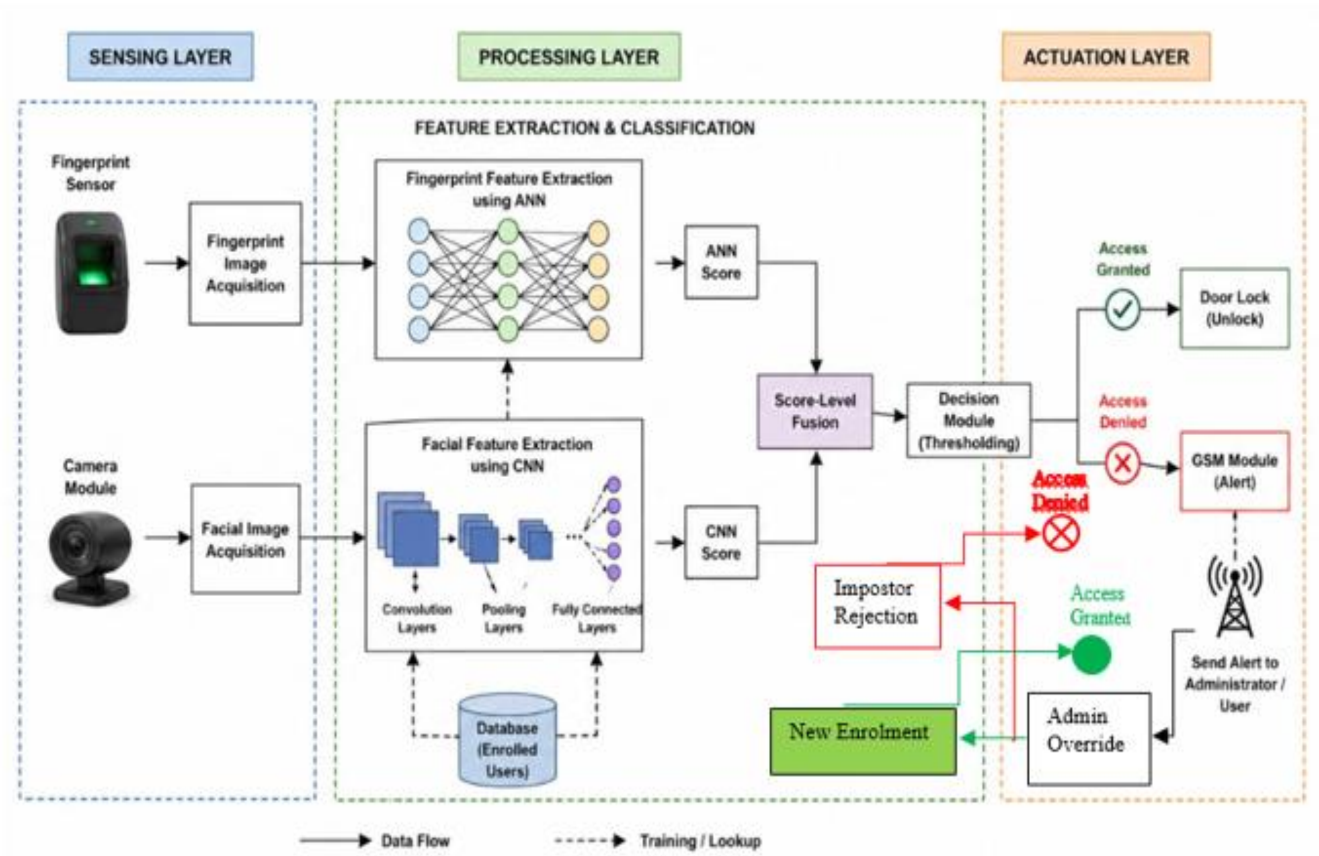


Figure 2. Block Diagram of Smart Biometric Gate Control System

The proposed system utilizes the ANN to process the fingerprint image to identify the unique biometric characteristics within the fingerprint. The facial image will also be processed by a CNN in a similar manner. Finally, the output from each of the neural networks will be combined using score level fusion to generate a single score for authentication, which will be compared against a saved threshold score for access determination. Upon successful authentication, the relay based access control system will allow entry into the controlled area, and, the GSM communication module will alert the administrator that further authentication may be required.

3.2 Software Architecture

The architecture of the program created consists of MATLAB programs that communicate sequentially as part of the authentication process. There are six major programs which are: FacialVerification.m, Fingerprint Verification.m , ScoreFusion.m , SendSMS.m , ReceiveAuthorization.m and GateControl.m. The FacialVerification.m program processes and verifies facial images utilizing Convolutional Neural Networks (CNN). The FingerprintVerification.m program processes and authenticates fingerprints with Artificial Neural Networks (ANN). The ScoreFusion.m program merges together the matching scores produced by both classifiers, thus giving a final authentication decision. The SendSMS.m program sends an alert to the system administrator when additional verification is required and the ReceiveAuthorization.m program receives authorization from the administrator.

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 05, ISSN No. 2455-2143, Pages 01-11
Published Online September 2026 in IJEAST (http://www.ijeast.com)

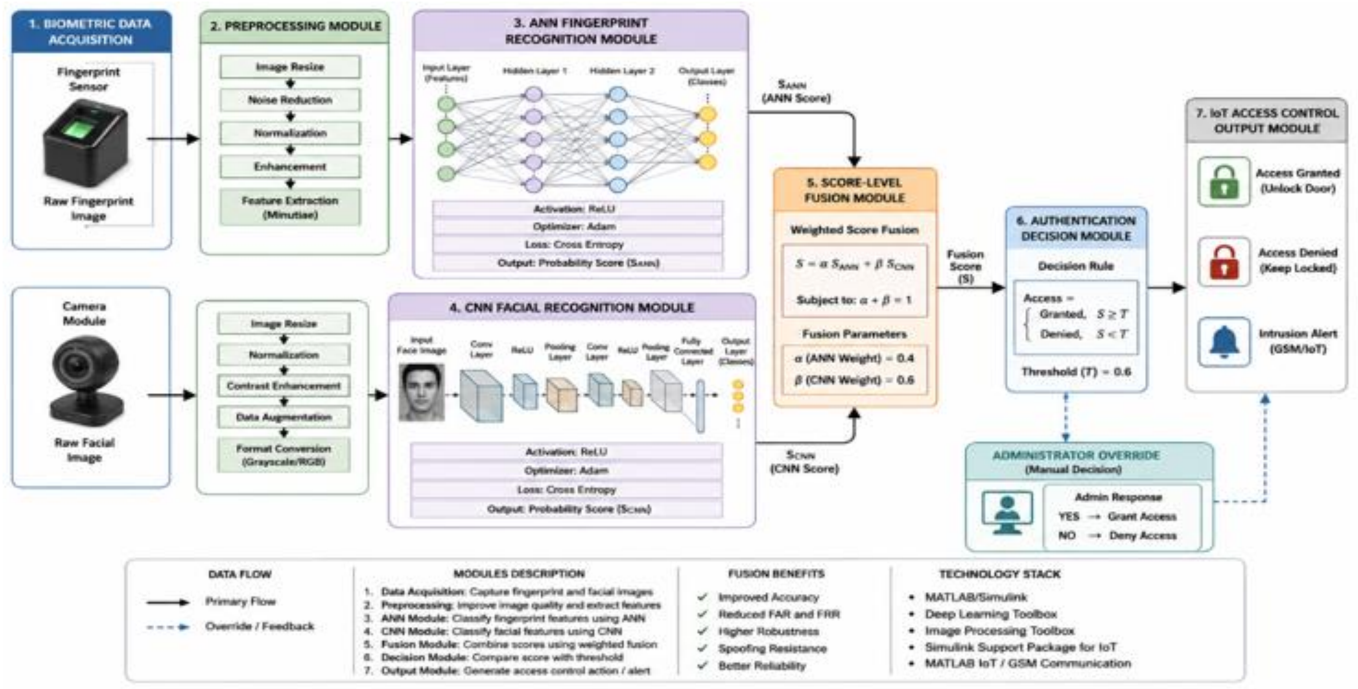


Figure 3. ANN–CNN Fusion Software Architecture Block

The GateControl.m program manages the relay based access control mechanism, allowing or denying access depending on the authentication results. Hence, all these programs are able to perform biometric recognition, score fusion, GSM communication, administrator authorization and the relay activation together, thus forming an efficient and secure multimodal biometric authentication system for IoT Access Control Applications as depicted in Figure 3 above.

3.3 Mathematical Model of the Developed ANN–CNN Fusion System

The developed fusion system is made up of ANN and CNN models, their separate mathematical models are combined to form the ANN-CNN fusion model as shown in Equations 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15 and 16.

The system is model as a multimodal biometric classifier as shown below.

$\boldsymbol{S}: (\boldsymbol{X_f}, \boldsymbol{X_p}) \rightarrow \{\boldsymbol{0}, \boldsymbol{1}\}$ (1)Where:

$\boldsymbol{X_f}$ = face image

$\boldsymbol{X_p}$ = fingerprint image

Output 1 = Access Granted

Output 0 = Access Denied

3.2.1.1 Face CNN Model

The mathematical model represent the face (image) Input to the CNN as shown,

$$\boldsymbol{X_f} \in \mathbb{R}^{HxWxC} \quad (2)$$

Where:

H = height

W = width

C = number of Channels (RGB = 3)

3.2.1.2 Face CNN Model Convolution Operation

At layer l, convulsion is model as

$$\boldsymbol{Z^{(l)}} = \boldsymbol{W^{(l)}} \star \boldsymbol{A^{(l-1)}} + \boldsymbol{b^{(l)}} \quad (3)$$

Where:

$\boldsymbol{W^{(l)}}$ = convolution kernel

$\boldsymbol{A^{(l-1)}}$= previous layer activation

$\boldsymbol{b^{(l)}}$ = bias

$\star$ = convolution operation

3.2.1.3 CNN Image Model Activation Function

Using ReLU:

$$\boldsymbol{A^{(l)}} = \boldsymbol{max}(\boldsymbol{0}, \boldsymbol{Z^{(l)}}) \quad (4)$$

3.2.1.4 CNN Image Model Pooling Operation

Max pooling:

$$\boldsymbol{A^{(l)}_{pool}} = \boldsymbol{max_{i,j} A^{(l)}(i, j)} \quad (5)$$

3.2.1.5 CNN Image Model Final Feature Vector Extraction

After performing multiple convolution and pooling layers the face feature embedding vector is obtained using the model shown:

$$\boldsymbol{F_f} = \boldsymbol{CNN_f(X_f)} (6)$$

Where:

$$\boldsymbol{F_f} \in \mathbb{R}^{\boldsymbol{1xn}} \quad (7)$$

3.2.2 ANN Fingerprint Mathematical Model

The proposed biometric system uses ANN to capture fingerprint feature and analyse them using minutiae features.

3.2.2.1 Minutiae features Extraction

Minutiae features is extracted using the model shown:

$$X_f = [x_1, x_2 \ldots\ldots x_k] \quad (8)$$

The hidden layers are obtained using the model shown:

$$H = \sigma(W_1 X_p + b_1) \quad (9)$$

Likewise the Output feature vector is obtained using the model,

$$F_p = W_2 H + b_2 \quad (10)$$

Where:

$\sigma = activation\ function$ (ReLU or sigmoid) and $F_p \in \mathbb{R}^{1xm}$

3.2.3 ANN – CNN Fusion Mathematical Model

The scores obtained from the ANN and CNN models are fused weighted using the mathematical model shown below:

$$F = \alpha F_f + \beta F_p \quad (11)$$

Where:

F = weighted fusion probability score

α = CNN face image probability constant

β = ANN fingerprint probability constant.

Subject to the probability summation of $\alpha + \beta = 1$ (12)

3.2.4 Decision Rule Mathematical Model

Let threshold = θ

$$\text{Decision} = \begin{cases} 1 & if\ \mathrm{F}(Fusion) \geq \theta \\ 0 & if\ F(Fusion) < \theta \end{cases} \quad (13)$$

Where typically θ = 0.6

3.2.5 Administrator Token Mathematical Model

This defines the override function as shown;

G(Y, R) (14)

Where:

Y = Classifier output

R = Administrator response

Therefore,

$$\text{G(Y, R)} = \begin{cases} 1 & if\ Y = 1 \\ 1 & if\ Y = 0 \wedge R = \mathbf{YES} \\ 0 & \mathbf{if\ R = NO} \end{cases}$$

If classifier output is 0 (Unknown or Intruder) system captures image, $\mathbf{I_u}$ and transmit to the administrator as represented by the Transmission function, T;

$$\text{T = GSM} (\mathbf{I_u}) \quad (15)$$

Where:

GSM = Network Carrier

$\mathbf{I_u}$ = Captured image.

Administrator the returns token, R $\in$ (YES, NO). The final decision is then taken by the system as shown in the access model as:

$$\text{Access} = \begin{cases} 1 & \mathbf{if\ R = YES} \\ 0 & \mathbf{if\ R = NO} \end{cases}$$

It returns yes for access and No for Denied. The high-quality spoof faces and finger print features are adjusted to make them appear "normal" and applied to the random "normal" face images as well as the finger print features to create an impostor (+2) and genuine (-2) distribution. They obtain the final fusion decision score, F, by normalizing the probability decision scores, $\mathbf{\alpha F_f}$ and $\mathbf{\beta F_p}$, as shown in Equation 9. The adaption weight coefficient α, β is set to 0.4 and 0.6 (40% ANN and 60% CNN). The final decision outcome is compared with the threshold.

If the Fusion decision score is greater or equals to the fusion threshold, Tf access is granted. Both models extract feature such as ridges, contours, and facial positions of the features such as eyes, nose, and mouth, respectively, and generate decision scores from 0 to 1. These scores are normalized using the minimum and maximum scaling function in Equation 16 to generate normalized score as in Table 1.

$$\mathrm{D}' = \frac{\mathrm{D} - \mathrm{D_{min}}}{\mathrm{D_{max}} - \mathrm{D_{min}}} \quad (16)$$

IV. RESULTS AND DISCUSSION

4.1 Performance Evaluation of Individual Biometric Models

The performance of the developed multimodal biometric authentication system was evaluated using MATLAB R2025b. The ANN fingerprint recognition model, CNN facial recognition model, and the integrated ANN–CNN fusion model were analysed based on training accuracy, validation accuracy, convergence behaviour, and authentication performance.

4.1.1 ANN Fingerprint Recognition Performance

The developed ANN fingerprint recognition model demonstrated 94.2% training accuracy and 93.5% for validation accuracy as illustrated in (Figure 4) below. The model convergence rate throughout training was rapid and it achieved a minimum value of 0.056 for validation loss suggesting effective learning, good convergence, and minimal over fitting have occurred. During the training and validation phases, the training and validation curve shapes generally mirrored one another indicating consistent performance by the model and good generalization potential. These results suggest that the ANN successfully acquired adequate knowledge of discriminative fingerprint minutiae features for accurate user authentication. As such, this ANN fingerprint recognition model provides reliable performance for fingerprint recognition and is a vital element of the proposed multimodal system for biometric user authentication.

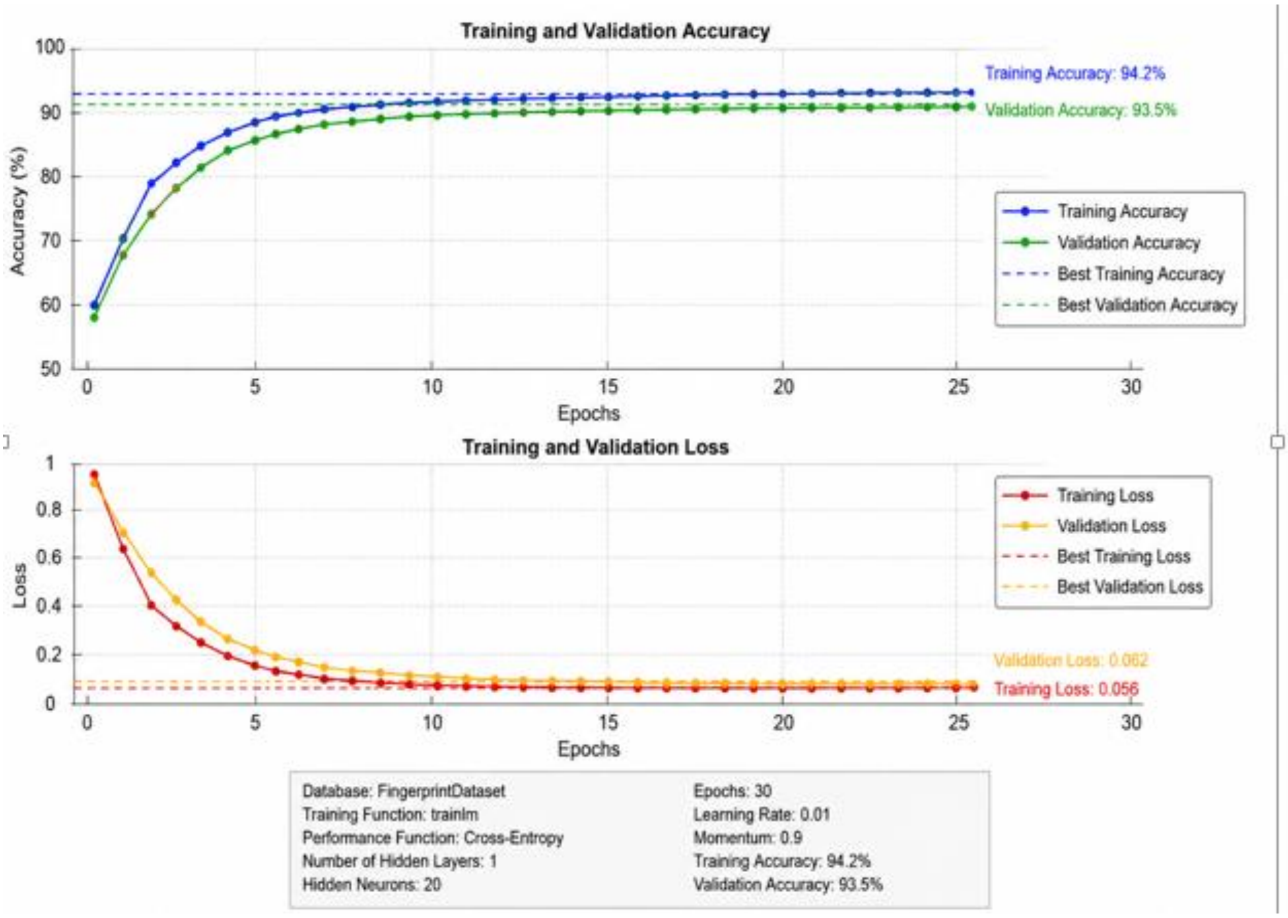


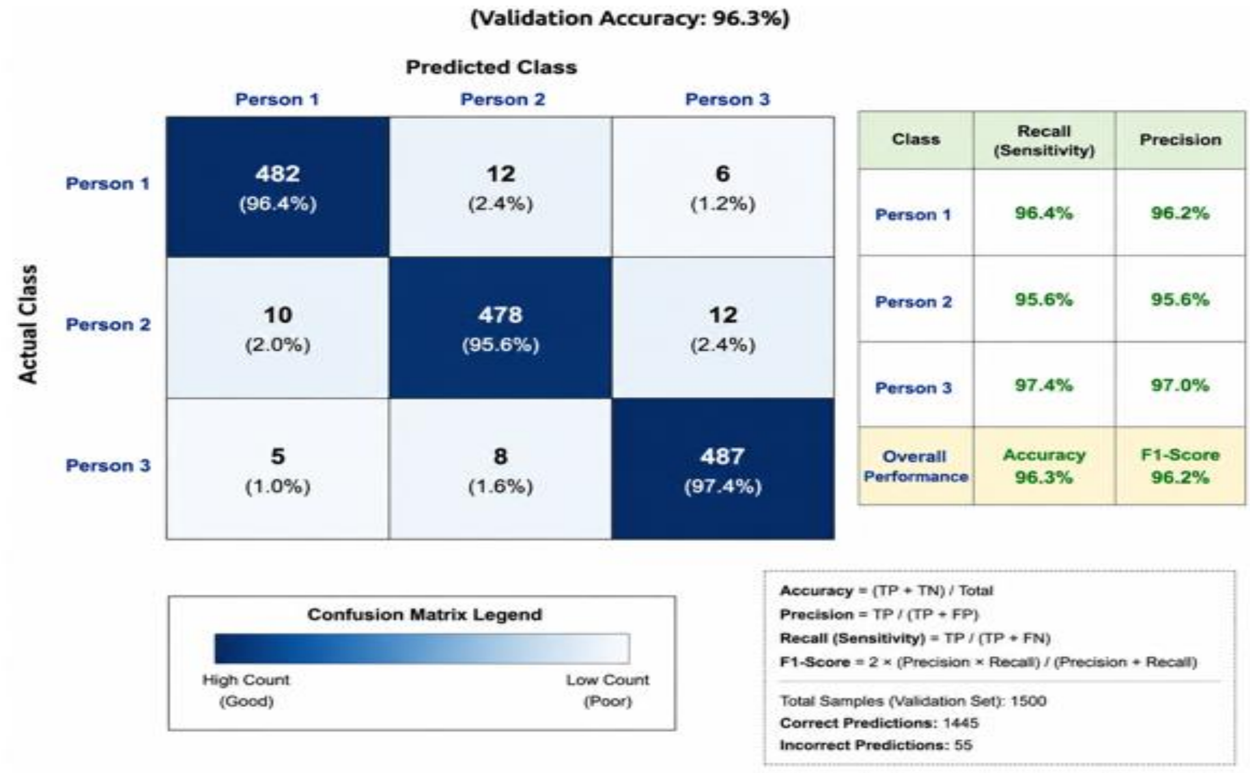
Figure 4. ANN Fingerprint Training and Validation Performance

During the training and validation phases, the training and validation curve shapes generally mirrored one another indicating consistent performance by the model and good generalization potential. These results suggest that the ANN successfully acquired adequate knowledge of discriminative fingerprint minutiae features for accurate user authentication. As such, this ANN fingerprint recognition model provides reliable performance for fingerprint recognition and is a vital element of the

4.1.2 CNN Facial Recognition Performance

The CNN facial recognition model produced a 97.0% training accuracy and a 96.3% validation accuracy as shown (Figure 5). The confusion matrix showed that the classifier can distinguish between genuine users and imposters, as very few samples were misclassified in the validation phase. The performance of the recognition analysis proves that the CNN model has the capability to learn how to automatically identify unique characteristics of a face by extracting such features from input images. The CNN model also displayed a high level of durability when being tested against different kinds of facial expression changes, lighting conditions, and angles when viewing faces. This allowed for accurate authentication across many different operating conditions. The results demonstrated that this particular CNN model was effective for use in a multimodal biometric authentication

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 05, ISSN No. 2455-2143, Pages 01-11
Published Online September 2026 in IJEAST (http://www.ijeast.com)



.

Figure 5. CNN Facial Recognition Confusion Matrix

The CNN model also displayed a high level of durability when being tested against different kinds of facial expression changes, lighting conditions, and angles when viewing faces. This allowed for accurate authentication across many different operating conditions. The results demonstrated that this particular CNN model was effective for use in a multimodal biometric authentication system for facial recognition.

4.1.3 Performance of the Proposed ANN–CNN Fusion Model

The proposed multimodal biometric authentication system produced the highest overall performance as shown Table 1. By combining the outputs of the ANN fingerprint classifier and the CNN facial recognition classifier through score-level fusion, the developed model achieved a training accuracy of 99.0% and a validation accuracy of 98.5%. The fusion approach significantly reduced both the False Acceptance Rate (FAR) and the False Rejection Rate (FRR), thereby improving authentication reliability.

Model	Training Accuracy (%)	Validation Accuracy (%)	Epochs
ANN (Fingerprint)	94.2	93.5	20
CNN (Facial)	97.0	96.3	20
Fusion ANN–CNN	99.0	98.5	20

Table 1. Validation Accuracy of the Developed ANN–CNN Fusion Model

The fusion approach significantly reduced both the False Acceptance Rate (FAR) and the False Rejection Rate (FRR), thereby improving authentication reliability.

4.2 Convergence Behaviour and Learning Efficiency

The convergence characteristics of the three developed models were compared using training accuracy, validation accuracy, and validation loss. The ANN–CNN fusion model converged faster than the individual ANN model while maintaining a lower validation loss. This indicates that integrating complementary biometric modalities improves learning efficiency and system stability.

4.3 ROC Analysis and Discriminative Performance

By developing biometric authentication models the ROC curves for the ANN, CNN & Fused (ANN-CNN) models as seen in (Figure 6)& analysed receiver a number similarly, closely matched the ideal point of maximum true positive rate with a minimum false positive rate in the upper left corner of the ROC space showing that they all produce excellent classification performance. Besides the superior performance by the ANN-CNN fusion model at separating genuine users from impostors, the hybrid method of score level fusion of words on the two modalities produced greater discrimination performance. In addition, the training & validation performance curves supporting the fusion models show convergence stability with very low values for validation loss, further developing confidence in the robustness and generalisation capabilities of the multimodal framework for secure IoT access control as shown in Figure 6.

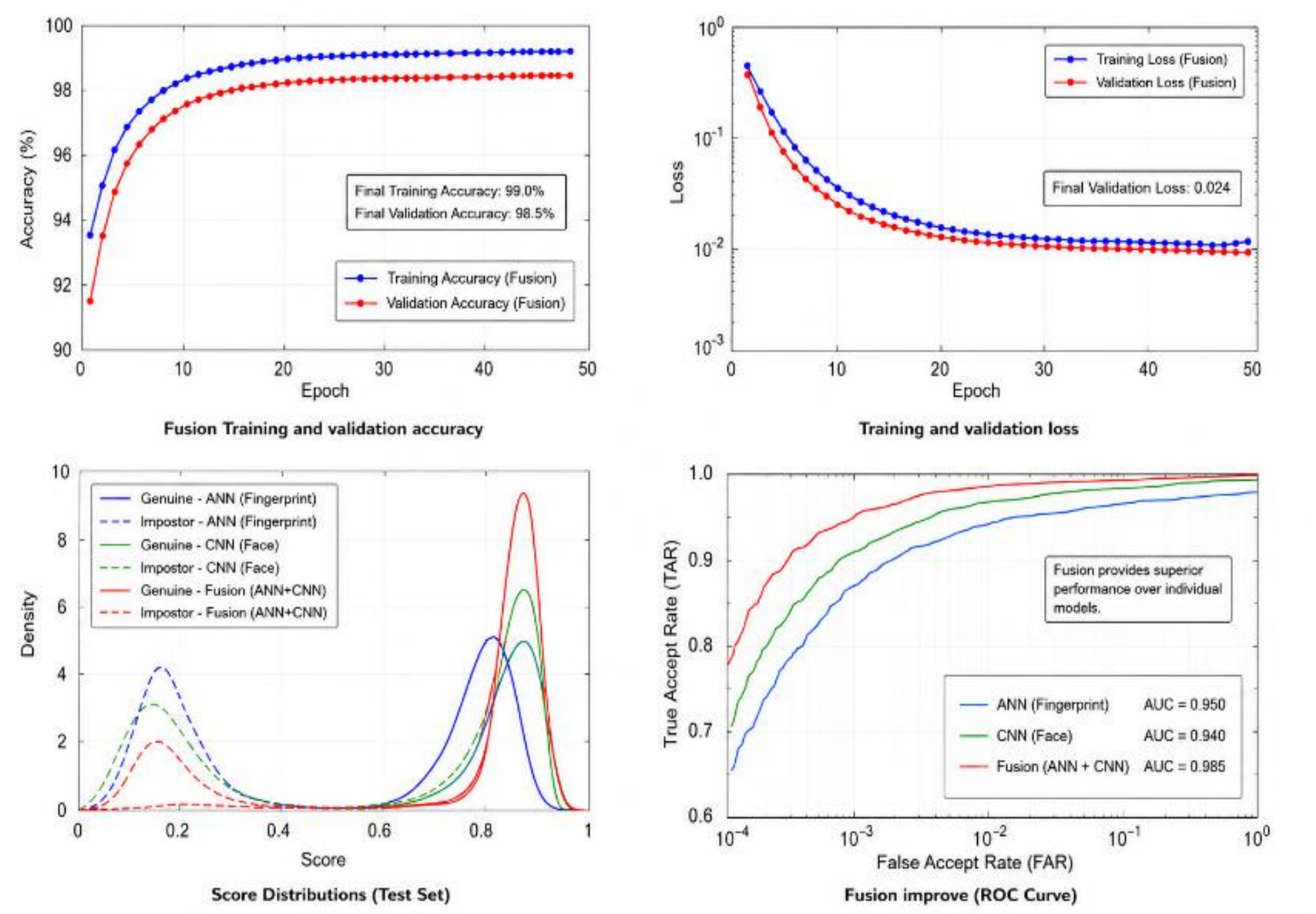


Figure 6. Fusion Training, Validation, Loss and ROC Performance Graphs

In addition, the training & validation performance curves supporting the fusion models show convergence stability with very low values for validation loss, further developing confidence in the robustness and generalisation capabilities of the multimodal framework for secure IoT access control as shown in Figure 6 above.

The ANN-CNN fusion model had more effective discrimination power and more consistently authenticating performance than other models. As shown in **Figure 7**, the ROC curves indicate that the fusion model achieved the largest Area under the curve (AUC) and that its ROC curve is located closest to the upper-left part of the ROC space. As such, it is evident that the fusion model has a superior level of precision and ability to distinguish a legitimate user from an imposter while producing few erroneous alarms.

The greater performance of the proposed fusion model results from fusing the scores from the fingerprint and face recognition analyses of the two biometric systems being used. This process allowed the fusion model to use both biometric modalities' complementary strengths. The proposed fusion model also produced lower rates of false acceptance (FAR) and false rejection (FRR) than either the ANN or CNN classifier, thus improving authentication accuracy, reliability, and system strength. Therefore, the proposed fusion model gives reliable, consistent performance under diverse operating conditions, making it

an ideal solution for secure IoT access control. Additionally, given the near-zero FAR and FRR values, this provides further confirmation of the proposed system's effectiveness in preventing unauthorized access, and that legitimate users will be accurately and efficiently authenticated.

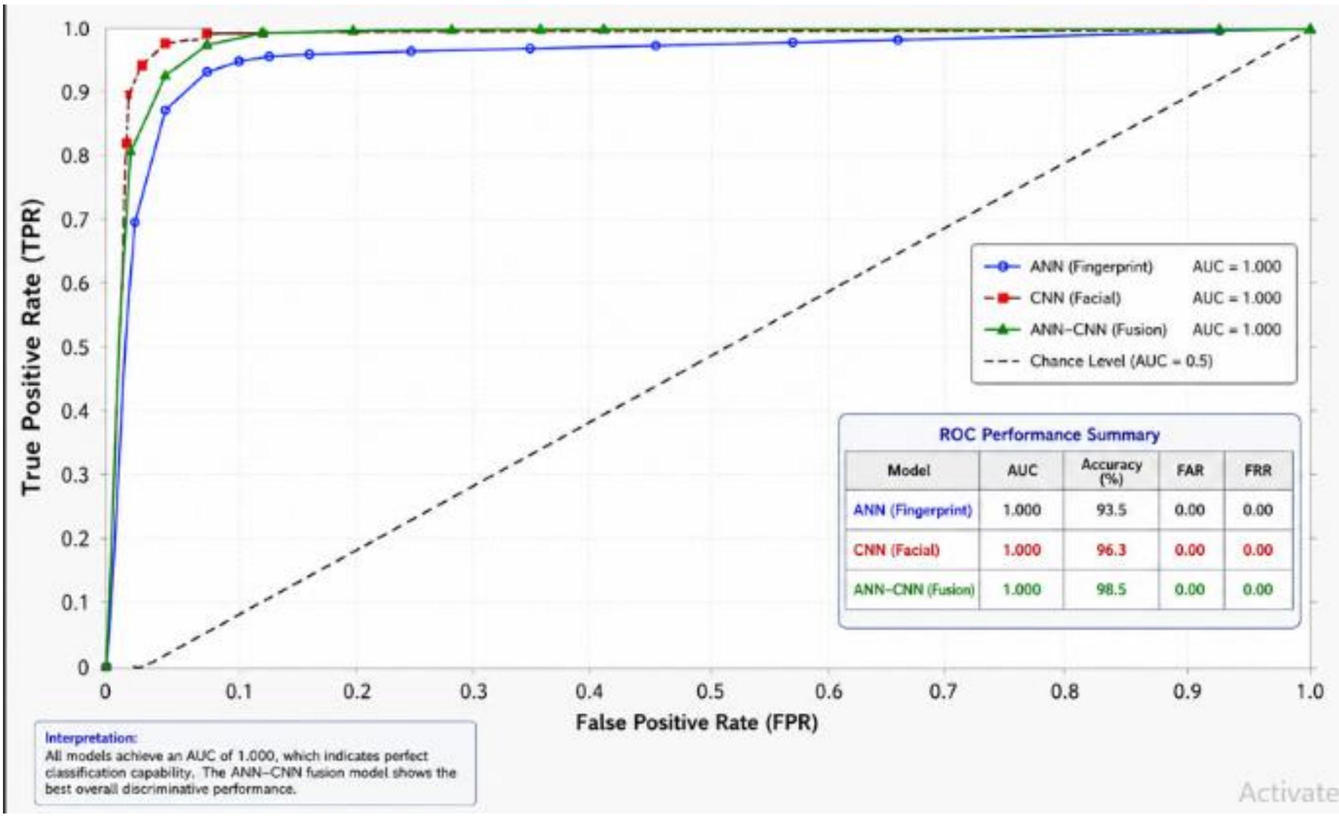


Figure 7: Training ROC curves for ANN, CNN and FUSION Models

The greater performance of the proposed fusion model results from fusing the scores from the fingerprint and face recognition analyses of the two biometric systems being used. This process allowed the fusion model to use both biometric modalities' complementary strengths. The proposed fusion model also produced lower rates of false acceptance (FAR) and false rejection (FRR) than either the ANN or CNN classifier, thus improving authentication accuracy, reliability, and system strength. Therefore, the proposed fusion model gives reliable, consistent performance under diverse operating conditions, making it an ideal solution for secure IoT access control. Additionally, given the near-zero FAR and FRR values, this provides further confirmation of the proposed system's effectiveness in preventing unauthorized access, and that legitimate users will be accurately and efficiently authenticated.

V. CONCLUSION

This study successfully developed and simulated an Artificial Neural Network (ANN)–Convolutional Neural Network (CNN)-based multimodal biometric authentication system for Internet of Things (IoT) access control applications. The proposed authentication framework integrates fingerprint recognition using ANN with facial recognition using CNN through a score-level fusion strategy to improve authentication accuracy and system reliability.

Simulation results demonstrated that the ANN fingerprint classifier achieved a validation accuracy of 93.5%**,** while the CNN facial recognition classifier achieved 96.3% validation accuracy. The integrated ANN–CNN fusion model produced the highest performance with 99.0% training accuracyand 98.5% validation accuracy, while significantly reducing the False Acceptance Rate (FAR) and False Rejection Rate (FRR). These findings confirm that combining multiple biometric modalities provides superior authentication performance compared with individual biometric systems.

Furthermore, the developed model is computationally efficient and suitable for deployment on lightweight IoT devices with limited processing resources. The incorporation of administrator override capability and GSM-based notification further enhances system security and operational flexibility.

The proposed multimodal authentication system therefore provides a secure, reliable, lightweight, and intelligent access control solution for modern IoT applications. Future research may consider implementing the developed model on physical embedded hardware and extending the authentication framework by incorporating additional biometric modalities such as iris recognition, voice recognition, or palm-vein authentication to further improve system robustness.

VI. REFERENCES

[1]. A. K. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, Jan. 2004. Doi:10.1109/TCSVT.2003.818349.

[2]. S. Li, L. D. Xu, and S. Zhao, "The Internet of Things: A Survey," Information Systems Frontiers, vol. 17, no. 2, pp. 243–259, 2015.

[3]. P. Gope and T. Hwang, "A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks," IEEE Transactions on Industrial Electronics, vol. 63, no. 11, pp. 7124–7132, Nov. 2016.

[4]. M. A. Ferrag, L. Maglaras, H. Janicke, J. Jiang, and S. Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey," Security and Communication Networks, vol. 2017, Article ID 6562953, 2017.

[5]. N. K. Ratha, J. H. Connell, and R. M. Bolle, "An Analysis of Minutiae Matching Strength," Proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), pp. 223–228, 2001.

[6]. Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," Nature, vol. 521, no. 7553, pp. 436–444, May 2015. doi:10.1038/nature14539.

[7]. A. Ross and A. K. Jain, "Information Fusion in Biometrics," Pattern Recognition Letters, vol. 24, no. 13, pp. 2115–2125, Sept. 2003.

[8]. J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294–1312, Third Quarter, 2015.

[9]. K. Ashton, "That 'Internet of Things' Thing," RFID Journal, June 22, 2009.

[10]. A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics. Boston, MA, USA: Springer, 2006.

[11]. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, 2nd ed. London, U.K.: Springer, 2009.

[12]. A. K. Jain and A. Ross, "Multibiometric Systems," Communications of the ACM, vol. 47, no. 1, pp. 34–40, Jan. 2004.

[13]. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

[14]. F. Chollet, Deep Learning with Python, 2nd ed. Shelter Island, NY, USA: Manning Publications, 2021.

[15]. R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models," IEEE Computer, vol. 29, no. 2, pp. 38–47, Feb. 1996.

[16]. W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Harlow, U.K.: Pearson Education, 2020.

[17]. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York, NY, USA: John Wiley & Sons, 1996.

[18]. J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Biometric Systems: Technology, Design and Performance Evaluation. London, U.K.: Springer, 2005.

[19]. A. Kumar and D. Zhang, "Personal Recognition Using Hand Shape and Texture," IEEE Transactions on Image Processing, vol. 15, no. 8, pp. 2454–2461, Aug. 2006.

[20]. S. Marcel and M. S. Nixon (Eds.), Handbook of Biometric Anti-Spoofing: Presentation Attack Detection, 2nd ed. Cham, Switzerland: Springer, 2019.

[21]. Z. Zhang, L. Wen, and J. Shi, "Deep Learning-Based Face Recognition: A Survey," IEEE Access, vol. 8, pp. 187139–187158, 2020.

[22]. H. Gunes and M. Piccardi, "Biometric Fusion for Human Identification: A Survey," Pattern Analysis and Applications, vol. 12, no. 4, pp. 345–356, Nov. 2009.

[23]. A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," Communications of the ACM, vol. 60, no. 6, pp. 84–90, June 2017.

[24]. M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A Survey on the Security of IoT Frameworks," Journal of Information Security and Applications, vol. 38, pp. 8–27, 2018.

[25]. R. Das, E. Piciucco, E. Maiorana, and P. Campisi, "Convolutional Neural Network-Based Multimodal Biometric Recognition Using Score-Level Fusion," IEEE Access, vol. 8, pp. 12145–12158, 2020.

IJEAST

INTERNATIONAL JOURNAL OF ENGINEERING APPLIED SCIENCE AND TECHNOLOGY

AUTHORS

- U. M. Akpan
- E. H. Johnson
- U. S. Ukommi

2455-2143