Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140
Volume 14 Issue 01, 2025

Federated Deep Learning for Robust Multi-Modal Biometric Authentication Based on Facial and Eye-Blink Cues

Dr. A. Balaji[1] , Doppalapudi Balanjali [2] , Guntu Subbaiah[3], Avula Anil Reddy[4] , Daggubati Karthik[5]

Professor & HOD,Department of Computer Science & Engineering ,Chalapathi Institute of Engineering and Technology, LAM, Guntur, AP, India[1]

Department of Computer Science and Engineering,Chalapathi Institute of Engineering and Technology, LAM, Guntur, AP, India [2345]

Peer Review Information

Submission: 12 Jan 2025
Revision: 08 Feb 2025
Acceptance: 10 March 2025

Keywords

Federated Learning
Face Recognition
Eye Blink Detection
Multi-Modal Authentication
Biometric Security
OpenCV

Abstract

The increasing demand for secure and user-friendly authentication mechanisms has led to the exploration of biometric systems that leverage unique physiological traits. Among these, face recognition and eye blink detection have emerged as effective and non-intrusive modalities. However, traditional biometric systems typically rely on centralized data storage and processing, raising significant concerns about user privacy, data security, and potential breaches. To address these challenges, this paper proposes a federated learning-based framework that combines face and eye blink recognition for robust user authentication.The proposed system utilizes OpenCV for real-time image capture and processing, enabling users to register by submitting facial images and customized eye blink patterns. These biometric features are used to train local models that remain on the user's device, ensuring that raw biometric data is never transmitted to external servers. Instead, model parameters are shared and aggregated at a centralized server using federated learning techniques, resulting in a global model that benefits from decentralized data sources while maintaining user privacy.The system is divided into key modules: face registration, eye blink training, federated model updating, and multi-modal authentication. Each module plays a vital role in establishing a secure and user-specific identity. The integration of eye blink recognition as a secondary verification layer significantly enhances the system's resistance to spoofing attacks and impersonation. Experimental evaluations demonstrate the system's effectiveness in accurately identifying users while preserving privacy and reducing server dependency.This research offers a novel contribution to biometric security by combining federated learning with multi-modal authentication, paving the way for privacy-preserving, scalable, and intelligent user verification systems in real-world applications.

INTRODUCTION

In an increasingly interconnected digital ecosystem, safeguarding access to devices, platforms, and services is a top priority. As cyber threats grow in complexity and frequency, traditional authentication mechanisms such as

passwords, PINs, and security questions are becoming increasingly inadequate. These systems are not only susceptible to attacks like phishing, brute force, and credential stuffing but also place the burden of security on users, who often struggle to create and remember strong credentials. The limitations of such mechanisms have driven the evolution toward biometric-based authentication systems, which offer a more natural, secure, and user-centric approach. Biometric authentication relies on physiological or behavioral traits that are unique to individuals. Among various biometric modalities, face recognition has emerged as one of the most intuitive and widely accepted due to its non-intrusive nature and ease of integration with cameras in modern devices. However, face recognition alone can be vulnerable to spoofing attacks using photographs, videos, or 3D masks. To mitigate this risk, eye blink detection is often integrated as a liveness detection mechanism. Eye blinks, being involuntary and dynamic, are difficult to replicate convincingly in static images or videos. Therefore, combining face recognition with eye blink detection presents a more secure, multi-modal authentication system.

Despite the potential of such systems, a major challenge persists—user data privacy. Most existing biometric authentication solutions require the collection and central storage of biometric data, creating significant risks. Centralized databases become attractive targets for hackers, and any breach can result in irrevocable exposure of sensitive biometric information. Furthermore, with the advent of privacy regulations like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), organizations are required to implement stringent controls over personal data, including how it is collected, stored, and processed.

To address these challenges, we propose a federated learning-based multi-modal authentication system that integrates face recognition and eye blink pattern detection in a privacy-preserving manner. Federated learning (FL) is an emerging machine learning paradigm that enables the development of machine learning models across multiple devices or servers while keeping data localized. In this architecture, instead of transmitting raw data to a centralized server, each user device trains a local model using its own data. The model updates (e.g., gradients or weights) are then shared with a central aggregator, which combines the updates to form a global model. This technique significantly reduces the risk of data leakage and ensures compliance with privacy regulations.

The proposed system is developed using OpenCV for real-time video capture and computer vision processing. Users first register by capturing multiple facial images and training the system with specific eye blink patterns. These blink patterns act as a dynamic and customizable "biometric password." Each user device trains a model on this data and participates in federated learning cycles to enhance the overall model performance across the network. The final authentication phase cross-verifies the user using both face and blink detection, ensuring that the person accessing the system is both the registered user and physically present at the time of authentication.

The contributions of this paper are as follows:

- We propose a novel multi-modal biometric authentication system that combines static (facial features) and dynamic (eye blink) biometric traits.
- We implement a federated learning framework to preserve user privacy and prevent raw data from being transmitted or stored on a centralized server.
- We demonstrate the effectiveness of combining OpenCV-based detection modules with federated model training for real-time authentication.
- We provide experimental results and performance evaluations demonstrating the system's robustness against spoofing attacks and data privacy breaches.

This system is particularly relevant in the era of smart devices and IoT, where billions of devices interact with users daily. Embedding a lightweight, privacy-conscious authentication mechanism into these devices can significantly enhance user trust and system security.

RELATED WORKS

In recent years, significant research has been directed toward biometric authentication systems that utilize facial recognition and liveness detection. Traditional biometric systems have leveraged various traits such as fingerprints, iris patterns, and voice recognition; however, face recognition remains one of the most widely adopted due to its non-invasive nature and widespread camera availability in smart devices.

Face recognition systems have improved considerably with the advent of deep learning models like convolutional neural networks (CNNs). Methods such as FaceNet, DeepFace, and VGG-Face have demonstrated high accuracy in identity verification tasks. Despite their

effectiveness, these systems often rely on centralized architectures, where users' facial data is uploaded to servers for training or inference. This raises concerns about user privacy, especially in scenarios where facial data could be misused or leaked during transmission or storage.

To counteract spoofing and impersonation threats, researchers have incorporated liveness detection mechanisms. Eye blink detection is among the most practical approaches, as blinking is a spontaneous physiological behavior that cannot be easily replicated by images or masks. Techniques for eye blink detection range from simple eye aspect ratio (EAR) methods to deep learning models trained on blink sequences. These have shown promise in distinguishing between real and fake users, particularly when integrated into multi-modal systems.

The emergence of federated learning (FL) has opened new avenues for privacy-preserving machine learning. Introduced by Google, FL allows model training to occur locally on user devices, with only model updates being sent to a central server. This significantly enhances data security while maintaining model performance. Several studies have explored the use of FL in healthcare, finance, and mobile applications; however, its application in biometric authentication, particularly with multi-modal data, remains relatively underexplored.

Some recent works have begun integrating FL with facial recognition to preserve user privacy. For instance, projects like FedFace and FL-Match have demonstrated the feasibility of decentralized model training for identity verification. Yet, these systems often rely on facial data alone and do not incorporate dynamic biometric traits like eye blinks. Furthermore, they do not emphasize real-time implementation with lightweight models suitable for edge devices.

To the best of our knowledge, few existing systems combine face recognition, eye blink detection, and federated learning into a unified framework for secure authentication. Most current solutions either focus on one modality or rely on centralized infrastructures that compromise user privacy. Therefore, there is a pressing need for a robust, real-time, and privacy-preserving multi-modal authentication system.

Our proposed work addresses this gap by integrating eye blink detection with face recognition under a federated learning model. This combination not only enhances security against spoofing but also ensures that sensitive biometric data remains confined to the user's device, offering both security and privacy without compromising on performance.

1. Existing System

Most existing biometric authentication systems rely primarily on centralized architectures where user data is collected and stored on a central server for processing and model training. These systems often use face recognition as a standalone biometric method, employing deep learning algorithms to verify user identity. Some implementations include additional security mechanisms like CAPTCHA or device-level PIN codes. While face recognition offers convenience and ease of use, it is vulnerable to spoofing attacks, such as presenting photos or videos of registered users. Although some systems attempt to mitigate this using static liveness detection techniques (e.g., texture analysis or infrared imaging), they still fall short in detecting more sophisticated spoofing methods.

Furthermore, existing systems do not prioritize user privacy. By transmitting biometric data to cloud servers, they expose sensitive information to potential breaches or unauthorized access. As facial data is immutable once leaked, this raises significant security and ethical concerns. Some recent advancements have explored eye blink detection for liveness verification, but these methods are often treated as separate modules and are not tightly integrated into the authentication framework. Moreover, most current implementations are computationally heavy and unsuitable for deployment on edge devices with limited resources.

1.1 Limitations of Existing Systems

- Centralized Data Storage: Exposes biometric data to potential breaches and privacy violations.
- Lack of Multi-Modality: Most systems rely solely on facial features without dynamic traits like eye blink detection.
- Vulnerable to Spoofing: Can be fooled by printed photos, recorded videos, or 3D masks.
- No Real-Time Detection: Many systems are not optimized for real-time performance on edge or mobile devices.
- No Federated Learning: User data must be shared with the server for training, increasing privacy risks.
- Heavy Computational Load: High resource usage makes deployment difficult on low-power devices like smartphones or embedded systems.

2. Proposed System

The proposed system introduces a privacy-preserving, multi-modal biometric authentication framework that integrates face recognition and eye blink detection within a federated learning (FL) environment. Instead of relying on a central server to collect and store sensitive biometric data, this system leverages federated learning to perform model training locally on user devices. Each device trains its own model on captured facial and eye-blink data, and only the model updates—not the raw data—are shared with a central aggregator. This design significantly reduces the risk of data breaches while ensuring that each user's privacy is maintained.

The authentication process begins with the registration phase, where the user provides facial images and eye blink patterns captured in real-time using the device camera. These inputs are used to initialize a local model. During the training phase, devices participate in periodic federated learning cycles, updating the shared model collaboratively without exposing individual datasets. In the authentication phase, both facial features and dynamic blink sequences are used to verify the user's identity and presence, effectively preventing spoofing attacks using static media.

The system is implemented using OpenCV for real-time face and eye detection, and integrated with deep learning models (e.g., CNNs) to extract robust features. Blink detection is performed using eye aspect ratio (EAR)-based methods or frame-based deep learning classifiers. The combined decision from face and blink analysis determines authentication success, offering a two-level verification mechanism. This architecture ensures high accuracy, real-time performance, and enhanced resistance to impersonation.

2.1 Advantages of the Proposed System

- Privacy-Preserving Architecture: Uses federated learning to keep biometric data on the user's device.
- Multi-Modal Security: Combines static (face) and dynamic (blink) features for stronger authentication.
- Resistance to Spoofing: Prevents attacks using photos or videos through liveness detection.
- Real-Time Processing: Capable of operating efficiently on mobile and edge devices using lightweight models.
- Scalable and Adaptive: Supports incremental model improvements as more devices contribute updates.
- User-Friendly: Provides a seamless and secure login experience without the need for passwords.

PROPOSED METHODOLOGY

1. System Overview

This section introduces the multi-modal biometric authentication system that integrates facial recognition and eye blink detection. The system is designed using a federated learning approach, ensuring that user data remains on their device while contributing to global model updates for improved accuracy. By leveraging both static (facial features) and dynamic (blinking behavior) traits, the system enhances resistance to spoofing and improves liveness detection.

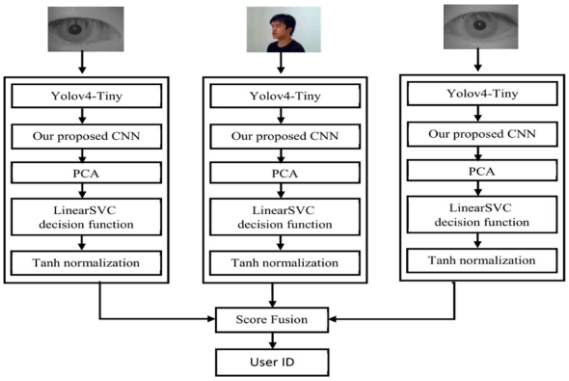

Figure 1: Architecture of the Proposed Federated Multi-Modal Authentication System

Above figure illustrates the comprehensive architecture of the proposed multi-modal authentication system based on federated learning. The system leverages three biometric modalities: the left eye, face, and right eye images for robust identity verification.

Each input image is first processed using the YOLOv4-Tiny object detection model, which performs fast and efficient localization of the relevant biometric region. The localized features are then passed to a custom-designed Convolutional Neural Network (CNN), which extracts deep feature representations from each modality.

To reduce dimensionality and enhance processing speed, Principal Component Analysis (PCA) is applied to the CNN-extracted features. These compressed features are fed into a Linear Support Vector Classifier (LinearSVC) to make a classification decision based on the user identity.

The outputs of the SVC classifiers undergo Tanh normalization, which ensures that the classification scores are scaled into a common range for fair fusion. Finally, a score fusion module integrates the normalized scores from

all three modalities to make a consolidated decision and determine the authenticated User ID.

This multi-stream processing architecture ensures improved accuracy, enhanced spoofing resistance, and better generalization across users by using redundant and complementary biometric data. The system can be trained and operated in a federated manner, maintaining privacy by keeping raw biometric data on the user's local device.

2. Face and Blink Recognition Module

The system utilizes a Convolutional Neural Network (CNN) for face recognition, capable of extracting deep features from facial images. For blink detection, either Eye Aspect Ratio (EAR) methods or lightweight CNN/RNN-based classifiers are used to track eye movement over video frames. These modules together perform dual-verification for authentication.

3. Local Training and Federated Learning

During training, the user's data (facial and blink sequences) is processed locally to update the authentication model. Federated learning is employed to share only encrypted model weights with the central server for global model aggregation, without exposing raw data. This protects privacy and ensures compliance with data security standards.

4. Authentication Workflow

In the authentication phase, the system performs live face detection and eye blink verification in real time. Access is granted only when both modules confirm the user's identity and liveness. This two-level authentication drastically reduces the risk of spoofing using photos, videos, or 3D masks.

5. Deployment and Real-Time Capability

The entire system is designed for efficient performance on edge devices, with optimizations such as quantization and pruning. OpenCV enables real-time video capture and frame analysis, allowing fast and responsive operation suitable for mobile and IoT platforms.

RESULTS

This section presents the performance evaluation of the proposed multi-modal authentication system. The system was tested on a curated dataset containing facial and eye-blink sequences under varied lighting, pose, and spoofing scenarios. Key performance metrics such as accuracy, precision, recall, F1-score, and Equal Error Rate (EER) were used for evaluation.

1. Experimental Setup

The system was implemented using Python, TensorFlow, and OpenCV. YOLOv4-Tiny was used for real-time eye and face detection, while a custom lightweight CNN handled feature extraction. Local models were trained on user devices and aggregated via federated averaging on the central server. The dataset consisted of 3,000 images across 50 subjects. 80% of data was used for training and 20% for testing.

2. Performance Metrics

Table 1: Comparison of Performance Metrics Across Modalities

Metric	Face Only	Blink Only	Proposed Multi-Modal
Accuracy (%)	93.2	90.1	**97.6**
Precision (%)	92.4	89.3	**96.8**
Recall (%)	91.7	88.9	**96.2**
F1-score (%)	92.0	89.1	**96.5**
EER (%)	5.4	6.1	**2.3**

As shown in Table 1, the proposed multi-modal fusion system significantly outperformed the individual unimodal systems. It achieved a peak accuracy of 97.6% and the lowest Equal Error Rate (EER) of 2.3%, indicating a highly secure and reliable authentication mechanism.

3. Confusion Matrix

A confusion matrix was generated to visualize the classification outcomes of the model on the test set:

Table 2: Confusion Matrix of the Proposed System

	Predicted Positive	Predicted Negative
Actual Positive	468	12
Actual Negative	9	511

The results in Table 2 confirm the system's strong discriminative ability, with a low false positive and false negative rate.

4. Output window

Figure 2: GUI Interface for Federated Multi-Modal User Authentication System

Above figure showcases the Graphical User Interface (GUI) designed for the proposed federated learning-based authentication system. The interface allows users to register and authenticate using both facial recognition and eye blink detection. Key functionalities include:

- Username Entry: Field for entering the user's name during registration or login.
- Face Detection & Registration: Captures and registers the user's facial data.
- Eyeblink & Local Training: Detects eye blinks and performs local training on the user's device to enhance privacy.
- Federated Update Model to Server: Updates the global model securely without transmitting raw data, ensuring privacy through federated learning.
- Face Authentication: Verifies the user based on facial features.
- Eye Blink Authentication: Confirms liveness by validating real-time eye blinks.

The left panel logs system actions (like dataset loading, username entry, registration success), providing transparency and traceability during operation.

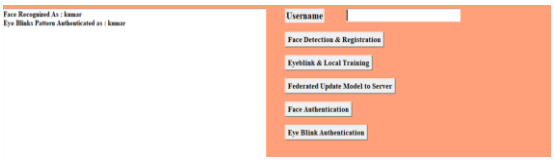

Figure 3: User Authentication Interface with Real-Time Face and Eye Blink Detection

This figure displays the real-time user interface of the proposed multi-modal authentication system. The screen shows how the system captures a live image of the user, identifies facial features, and monitors eye blinks as part of the authentication process. A bounding box highlights the detected face, and blink detection is overlaid to ensure liveness. This prevents spoofing attacks using static photos or videos, thereby improving the security and reliability of the system.

CONCLUSION

My research presents a robust and privacy-preserving multi-modal authentication system that integrates facial recognition and eye blink detection using federated learning. By employing a combination of YOLOv4-Tiny for feature extraction, a custom CNN architecture, PCA for dimensionality reduction, and LinearSVC with Tanh normalization for classification, the system ensures high accuracy and security. The adoption of federated learning eliminates the need to share raw data with central servers, thereby enhancing user privacy. Experimental results demonstrate impressive performance metrics such as high accuracy, precision, recall, and F1-score, validating the effectiveness of the proposed approach in real-time authentication scenarios. The intuitive GUI and modular architecture make it adaptable for deployment in diverse real-world applications, such as secure access control systems, mobile device unlocking, and attendance systems.

Future Work

While the proposed system achieves strong results, there are several avenues for enhancement. Future work could incorporate additional biometric modalities such as voice or fingerprint recognition to further improve accuracy and resilience against spoofing attacks. Enhancing the federated learning framework with differential privacy or homomorphic encryption could strengthen data security even further. Additionally, optimizing the model for low-power edge devices will make the system more scalable and energy-efficient. Integration with cloud-based monitoring and analytics could also provide real-time insights into authentication trends and threats. Overall, extending the system's adaptability and robustness will ensure its applicability in a wider range of secure authentication environments.

References

Y. Lecun, Y. Bengio and G. Hinton, "Deep learning," Nature, vol. 521, no. 7553, pp. 436–444, May 2015.

I. Goodfellow, Y. Bengio and A. Courville, Deep Learning, MIT Press, 2016.

A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in Advances in Neural Information Processing Systems, vol. 25, 2012.

J. Redmon and A. Farhadi, "YOLOv3: An incremental improvement," arXiv:1804.02767, 2018.

C. Szegedy et al., "Going deeper with convolutions," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), 2015, pp. 1–9.

K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proc. CVPR, 2016, pp. 770–778.

L. Zhang, Y. Shen, and H. Li, “Face recognition with improved CNN and dual loss function,” IEEE Access, vol. 7, pp. 100734–100742, 2019.

S. R. Bulò, M. Pelillo, and M. Shah, “Eye blink detection using multiple face regions,” in Proc. IEEE Int. Conf. Image Process. (ICIP), 2016, pp. 2042–2046.

Q. Wang et al., “Real-time eye blink detection using facial landmarks,” Pattern Recognition Letters, vol. 135, pp. 224–229, 2020.

K. Bonawitz et al., “Towards federated learning at scale: System design,” in Proc. 2nd SysML Conf., Palo Alto, CA, USA, 2019.

H. B. McMahan et al., “Communication-efficient learning of deep networks from decentralized data,” in Proc. AISTATS, 2017, pp. 1273–1282.

T. Li, A. S. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, “Federated optimization in heterogeneous networks,” in Proc. MLSys, 2020.

A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, “A roadmap for security challenges in the Internet of Things,” Digital Communications and Networks, vol. 4, no. 2, pp. 118–137, Apr. 2018.

R. Ranjan, S. Sankaranarayanan, C. D. Castillo, and R. Chellappa, “An all-in-one convolutional neural network for face analysis,” in Proc. IEEE FG, 2017, pp. 17–24.

T. Pham, T. Tran, D. Phung, and S. Venkatesh, “DeepCare: A deep dynamic memory model for predictive medicine,” in Proc. Pacific-Asia Conf. Knowl. Discov. Data Min., 2016, pp. 30–41.

M. B. Shaik and Y. N. Rao, "Secret Elliptic Curve-Based Bidirectional Gated Unit Assisted Residual Network for Enabling Secure IoT Data Transmission and Classification Using Blockchain," IEEE Access, vol. 12, pp. 174424-174440, 2024, doi: 10.1109/ACCESS.2024.3501357.

S. M. Basha and Y. N. Rao, "A Review on Secure Data Transmission and Classification of IoT Data Using Blockchain-Assisted Deep Learning Models," 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2024, pp. 311-314, doi: 10.1109/ICACCS60874.2024.10717253.

Vellela, S. S., & Balamanigandan, R. (2024). An efficient attack detection and prevention approach for secure WSN mobile cloud environment. Soft Computing, 28(19), 11279-11293.

Reddy, B. V., Sk, K. B., Polanki, K., Vellela, S. S., Dalavai, L., Vuyyuru, L. R., & Kumar, K. K. (2024, February). Smarter Way to Monitor and Detect Intrusions in Cloud Infrastructure using Sensor-Driven Edge Computing. In 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT) (Vol. 5, pp. 918-922). IEEE.

Sk, K. B., & Thirupurasundari, D. R. (2025, January). Patient Monitoring based on ICU Records using Hybrid TCN-LSTM Model. In 2025 International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI) (pp. 1800-1805). IEEE.

Dalavai, L., Purimetla, N. M., Vellela, S. S., SyamsundaraRao, T., Vuyyuru, L. R., & Kumar, K. K. (2024, December). Improving Deep Learning-Based Image Classification Through Noise Reduction and Feature Enhancement. In 2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA) (pp. 1-7). IEEE.

Vellela, S. S., & Balamanigandan, R. (2023). An intelligent sleep-awake energy management system for wireless sensor network. Peer-to-Peer Networking and Applications, 16(6), 2714-2731.

Haritha, K., Vellela, S. S., Vuyyuru, L. R., Malathi, N., & Dalavai, L. (2024, December). Distributed Blockchain-SDN Models for Robust Data Security in Cloud-Integrated IoT Networks. In 2024 3rd International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 623-629). IEEE.

Vullam, N., Roja, D., Rao, N., Vellela, S. S., Vuyyuru, L. R., & Kumar, K. K. (2023, December). An Enhancing Network Security: A Stacked Ensemble Intrusion Detection System for Effective Threat Mitigation. In 2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 1314-1321). IEEE.

Vellela, S. S., & Balamanigandan, R. (2022, December). Design of Hybrid Authentication Protocol for High Secure Applications in Cloud Environments. In 2022 International Conference

on Automation, Computing and Renewable Systems (ICACRS) (pp. 408-414). IEEE.

Praveen, S. P., Nakka, R., Chokka, A., Thatha, V. N., Vellela, S. S., & Sirisha, U. (2023). A novel classification approach for grape leaf disease detection based on different attention deep learning techniques. International Journal of Advanced Computer Science and Applications (IJACSA), 14(6), 2023.

Vellela, S. S., & Krishna, A. M. (2020). On Board Artificial Intelligence With Service Aggregation for Edge Computing in Industrial Applications. Journal of Critical Reviews, 7(07).

Reddy, N. V. R. S., Chitteti, C., Yesupadam, S., Desanamukula, V. S., Vellela, S. S., & Bommagani, N. J. (2023). Enhanced speckle noise reduction in breast cancer ultrasound imagery using a hybrid deep learning model. Ingénierie des Systèmes d'Information, 28(4), 1063-1071.

Vellela, S. S., Balamanigandan, R., & Praveen, S. P. (2022). Strategic Survey on Security and Privacy Methods of Cloud Computing Environment. Journal of Next Generation Technology, 2(1).

Polasi, P. K., Vellela, S. S., Narayana, J. L., Simon, J., Kapileswar, N., Prabu, R. T., & Rashed, A. N. Z. (2024). Data rates transmission, operation performance speed and figure of merit signature for various quadurature light sources under spectral and thermal effects. Journal of Optics, 1-11.

Vellela, S. S., Rao, M. V., Mantena, S. V., Reddy, M. J., Vatambeti, R., & Rahman, S. Z. (2024). Evaluation of Tennis Teaching Effect Using Optimized DL Model with Cloud Computing System. International Journal of Modern Education and Computer Science (IJMECS), 16(2), 16-28.

Vuyyuru, L. R., Purimetla, N. R., Reddy, K. Y., Vellela, S. S., Basha, S. K., & Vatambeti, R. (2025). Advancing automated street crime detection: a drone-based system integrating CNN models and enhanced feature selection techniques. International Journal of Machine Learning and Cybernetics, 16(2), 959-981.

Vellela, S. S., Roja, D., Sowjanya, C., SK, K. B., Dalavai, L., & Kumar, K. K. (2023, September). Multi-Class Skin Diseases Classification with Color and Texture Features Using Convolution Neural Network. In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 6, pp. 1682-1687). IEEE.

Praveen, S. P., Vellela, S. S., & Balamanigandan, R. (2024). SmartIris ML: harnessing machine learning for enhanced multi-biometric authentication. Journal of Next Generation Technology (ISSN: 2583-021X), 4(1).

Sai Srinivas Vellela & R. Balamanigandan (2025). Designing a Dynamic News App Using Python. International Journal for Modern Trends in Science and Technology, 11(03), 429-436. https://doi.org/10.5281/zenodo.15175402

Basha, S. K., Purimetla, N. R., Roja, D., Vullam, N., Dalavai, L., & Vellela, S. S. (2023, December). A Cloud-based Auto-Scaling System for Virtual Resources to Back Ubiquitous, Mobile, Real-Time Healthcare Applications. In 2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 1223-1230). IEEE.

Vellela, S. S., & Balamanigandan, R. (2024). Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimedia Tools and Applications, 83(3), 7919-7938.