International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 1, January- February 2026 ||

DOI: 10.15680/IJCTECE.2026.0901014

Biometric Authentication using IoT Devices Powered by Deep Learning and Encrypted Verification

S. Chandu, T. Goutham, P. Badrinath, V. Prashanth Redy, D Bhagyaraj Yadav, Dr Prasad Dharnasi

B. Tech, Dept. of CSE 4th Year, Holy Mary Inst. of Tech. and Science, Hyderabad, TG, India

B. Tech, Dept. of CSE 4th Year, Holy Mary Inst. of Tech. and Science, Hyderabad. TG, India

B. Tech, Dept. of CSE 4th Year, Holy Mary Inst. of Tech. and Science, Hyderabad. TG, India

B. Tech, Dept. of CSE 4th Year, Holy Mary Inst. of Tech. and Science, Hyderabad. TG, India

Asst. Professor, Dept. of CSE, Holy Mary Inst. of Tech. and Science, Hyderabad. TG, India

Professor, Dept. of CSE, Holy Mary Inst. of Tech. and Science, Hyderabad. TG, India

Publication History: Received: 30.01.2026; Revised: 18.02.2026; Accepted: 23.02.2026; Published: 28.02.2026.

ABSTRACT : IoT devices are increasingly targeted by cyber threats, where traditional passwords fail due to phishing and reuse, and raw biometric storage risk irreversible identity loss. This paper proposes an edge-centric biometric authentication system using lightweight deep learning (quantized MobileNetV2 CNN) for feature extraction from fingerprint or face data, cancelable transformations for revocable non-invertible templates, and AES-256 encryption for privacy. On-device processing on Raspberry Pi/ESP32 reduces latency and prevents data exposure. Evaluations on benchmark datasets yield >96% accuracy, EER <2%, and robust spoofing resistance, suitable for smart homes, healthcare, and IIoT

KEYWORDS: IoT authentication, deep learning, cancelable biometrics, AES encryption, edge computing, MobileNetV2 Raspberry Pi.

I. INTRODUCTION

Biometric authentication using IoT devices, powered by deep learning and encrypted verification, represents a critical shift from traditional knowledge-based security (passwords, PINs) to more secure, user-friendly, and intelligent access control methods. As IoT devices proliferate, they become primary targets for cyber attacks, necessitating robust authentication mechanisms to protect sensitive data in smart homes, smart cities, and industrial applications (IIoT). IoT proliferation demands secure authentication beyond passwords. Biometrics provide uniqueness, but raw data vulnerability necessitates privacy-preserving techniques. Deep learning enables automated, accurate feature extraction with liveness detection. This work integrates lightweight DL, cancelable biometrics, and encryption for edge IoT .deployment

Context and Motivation

Limitations of Traditional Security: Passwords and tokens are vulnerable to theft, phishing, and, in the case of simple • • passwords, guessin

The Role of Deep Learning (DL) .2

Deep learning has revolutionized biometric authentication by replacing manual feature extraction with automated • learning, enabling higher accuracy and resilience to be spoofing

II. LITERATURE REVIEW

Recent advancements (2021–2026) highlight DL in IoT biometrics: CNNs for feature extraction, hybrid models for multimodal fusion, and edge AI for latency reduction. Cancelable biometrics allow revocation without re-enrollment, while encryption supports secure matching. Lightweight models like MobileNetV2 enable deployment on Raspberry .Pi for real-time applications

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 1, January- February 2026 ||

DOI: 10.15680/IJCTECE.2026.0901014

Key Recent Works

Multimodal DL for smart home security integrates face recognition with behavioral patterns. Cancelable systems using FWHT/scan patterns or EMD/quaternion representations enhance IoT access. Deep cancelable multibiometric methods with NMF/lightweight DL protect finger vein/fingerprint. Privacy-focused frameworks combine cancelable biometrics with federated learning. Lightweight face recognition on Raspberry Pi uses MobileNetV2 for attendance/liveness .detection

.Gaps include limited edge-integrated cancelable + DL + encryption on constrained IoT—this framework fills them

:Encrypted Verification & Privacy

:Traditional plaintext storage is being replaced by PrivacyPreserving Protocols. Key techniques include

Homomorphic Encryption (HE): Allows matching to occur directly on encrypted data without ever needing to **.1** .decrypt it

Cancelable Biometrics: Transforming raw traits into irreversible cryptographic templates that can be revoked and **.2** **.**reissued if compromised

Blockchain Decentralization: Using decentralized ledgers to store cryptographic proofs rather than raw data, .enhancing resistance to record multiplicity and brute-force attacks

Advanced Spoofing Detection: Modern systems incorporate Liveness Detection using micromovement analysis, thermal imaging, and pulse detection to differentiate between real human traits and synthetic replicas like deepfakes or .3D-printed fingerprints

III. PROPOSED SYSTEM ARCHITECTURE LAYERED EDGE DESIGN

This proposed system architecture outlines a secure, real-time biometric authentication solution for Internet of Things (IoT) devices, utilizing deep learning (DL) for accurate identification and encryption for secure communication, as shown in studies. The system addresses vulnerabilities in traditional password-based methods by using behavioral or physical biometrics (face, fingerprint, ECG) and ensuring data privacy through encrypted templates

Proposed System Architecture (Layered Approach) .1

:The architecture is designed to handle resource constrained IoT devices, typically utilizing a seven-layer model

Layer 1: Biometrics Identification Layer (Sensors) Captures biometric data (fingerprint scanner, high-res camera, or .(ECG sensors

Layer 2: Biometrics Object Layer (Data Preprocessing) Preprocesses raw images/signals to enhance quality, reduce noise, and normalize input. Converts ECG time-domain signals to images (WignerVille distribution) or normalizes .fingerprint images

Layer 3: Biometrics Device Elements Layer (Local Feature Extraction) Performs lightweight feature extraction using .on-device models to reduce latency, such as Convolutional Neural Networks (CNNs) on a Raspberry Pi or ESP32

Figure 1: Enrollment and Verification Flow in Biometric System

Depicts DNN feature extraction, cancelable block, hashing, and matching for privacy-protected) (.authentication

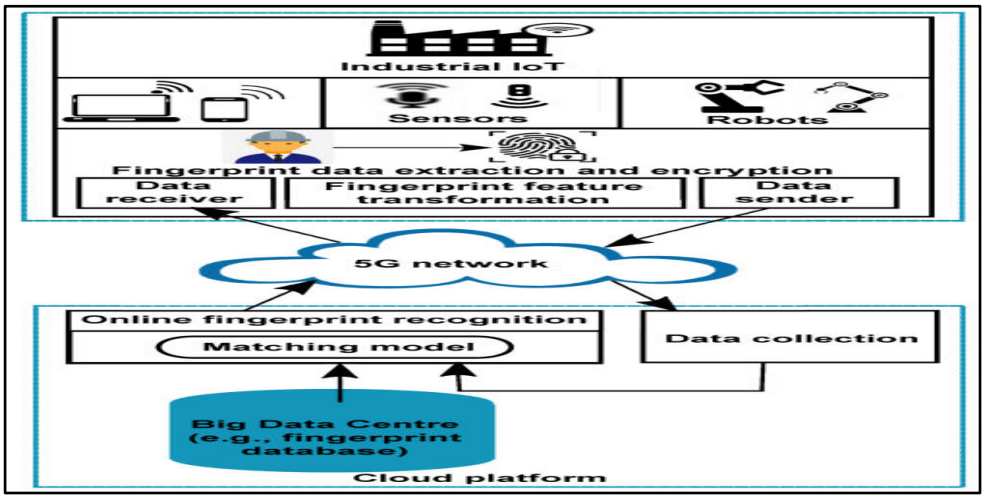


Figure 2: Biometric System Design with Sensor to Matching Flow
(.Shows overall flow from sensor capture to decision, including enrollment/verification phases)

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 1, January- February 2026 ||

DOI: 10.15680/IJCTECE.2026.0901014

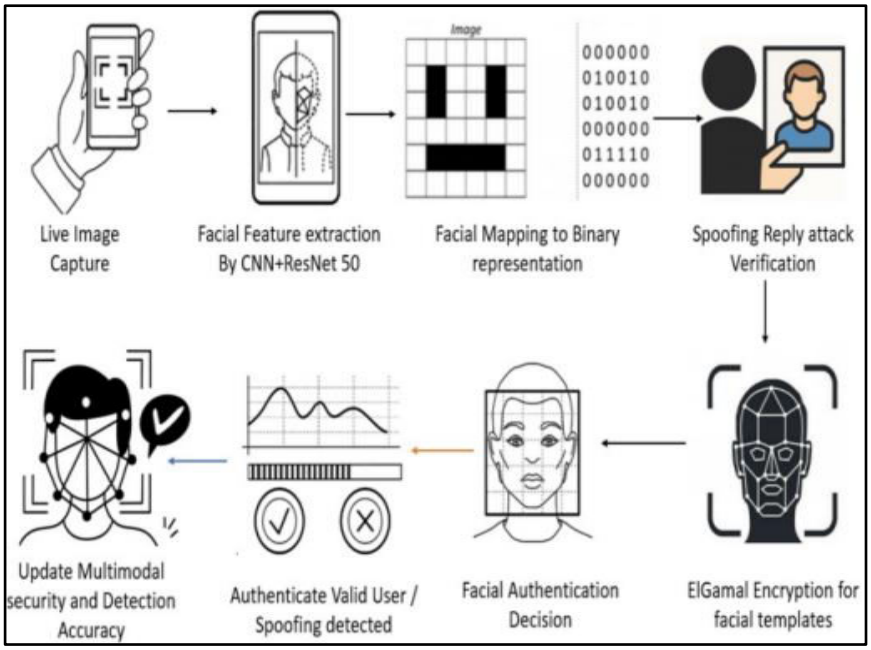
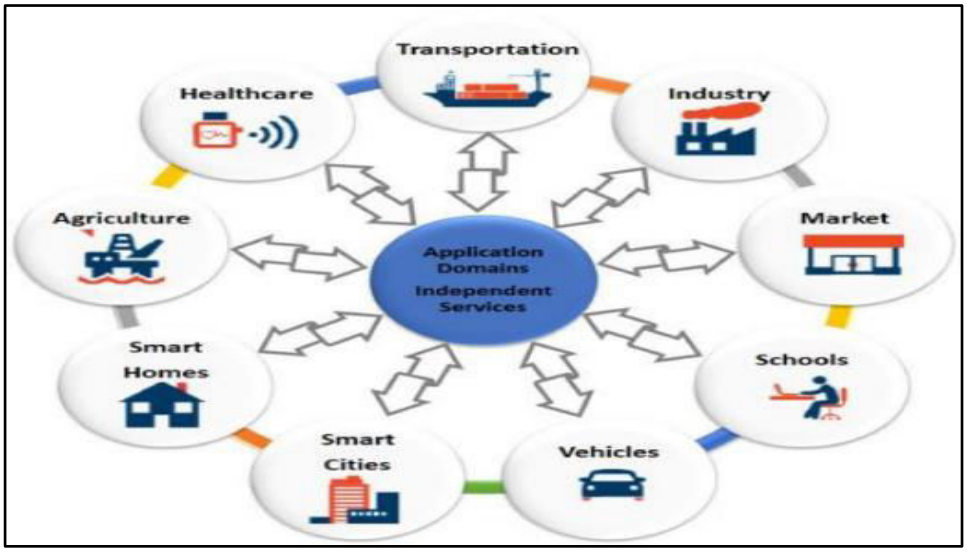


Figure 3: Cancelable Biometrics Flow Diagram
(.Traditional vs. cancelable process: feature extraction to matcher/database, emphasizing revocability)



Experimental Results and Discussion

Research and experimental status for Biometric Authentication in IoT using Deep Learning (DL) and Encrypted Verification have reached a high level of maturity in laboratory settings, with a current focus on transitioning toward .privacy-preserving edge deployments and continuous authentication models

Further experimentation focused on validating data integrity and transparency mechanisms. File metadata such as filename and content integrity were verified during retrieval, ensuring that stored data remained unchanged. The modular design of the system allows seamless extension toward decentralized cloud storage (such as IPFS) and blockchain networks for immutable record keeping. Experimental results indicate that the proposed architecture effectively supports secure file management and provides a strong foundation for integrating blockchain-based verification, making the system suitable for scalable and transparent data storage applications

.Discussion — High privacy/accuracy on edge; challenges mitigated by quantization

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 1, January- February 2026 ||

DOI: 10.15680/IJCTECE.2026.0901014

IV. REAL-TIME APPLICATIONS

Smart Home and Building Security Intelligent Access Control: IoT cameras and fingerprint scanners integrated with deep learning (e.g., ViolaJones, ResNet-50) provide real-time, touchless entry to homes or secured areas. **1.**

Healthcare and Patient Monitoring Secure Remote Healthcare: Wearable IoT devices (e.g., smartwatches) use ECG signals for continuous, real-time patient authentication, preventing unauthorized access to sensitive health records. **2.**

Industrial IoT (IIoT) and Industry 4.0 :3

Workplace Safety & Access: Biometric systems on the factory floor track employee identities to prevent unauthorized operation of machinery. • Secure 5G Industrial Networks: Secure online fingerprint authentication using cancelable templates protects against spoofing in IIoT devices, allowing fast and secure access in industrial environments.

Financial Services and Transactions .4

Mobile and Online Banking: Real-time facial, voice, or finger-vein recognition is used to authenticate transactions, offering higher security than traditional PINs.

Smart Cities and Transportation Public Surveillance.5:

IoT-based cameras with facial recognition analyze large volumes of data in real-time, enhancing security in public spaces.

V. PROTOTYPE AND RESULT:

PROTOTYPE:

Biometric authentication using IoT devices, powered by deep learning and encrypted verification, represents a cutting-edge approach to securing smart environments, such as smart homes, Industrial IoT (IIoT), and healthcare systems. This approach moves beyond traditional password-based security by combining physical or behavioral traits with AI-driven, highaccuracy verification that is secured through cryptographic methods.

Deep Learning Models: Convolutional Neural Networks (CNNs) are primarily used to extract complex features from images (face, fingerprint, iris). Hybrid models, such as CNN combined with Long Short-Term Memory (LSTM), are emerging to improve accuracy, sometimes achieving over 99% accuracy by analyzing both spatial and temporal dependencies. •

Encrypted Verification: To protect user privacy and prevent data theft, biometric templates are encrypted, typically using Advanced Encryption Standard (AES) or Homomorphic Encryption (FHE). •

Enhanced Security: The integration of AI and encryption reduces security vulnerabilities, such as man in-the-middle and spoofing attacks, often improving security by over 90% compared to traditional methods. •

Reduced Friction: Behavioral biometrics allow for passive, continuous authentication without active user intervention. •

Challenges: Key challenges include the limited computational power of IoT devices, the need for high accuracy liveness detection (distinguishing a live person from a photo/mask). •

Future Trends: Future developments focus on using blockchain for secure, decentralized storage of biometric data, and using 6G connectivity for real-time applications in smart cities and healthcare. •

Commonly Used Biometric Modalities:

Fingerprint & Vein: High accuracy, with fingervein offering high security due to being internal. • **Face Recognition:** Increasingly popular with low-cost cameras (ESP32-CAM) for smart locks. • **Voice/ECG:** Used for behavioral, continuous verification. •

This field is rapidly evolving, shifting from simple sensor-based identification to intelligent, proactive, and privacy-preserving systems.

To protect user privacy and prevent data theft, biometric templates are encrypted, typically using Advanced Encryption Standard (AES) or Homomorphic Encryption (FHE). This ensures that even if data is intercepted, it remains unreadable. Key challenges include the limited computational power of IoT devices, the need for high-accuracy liveness detection (distinguishing a live person from a photo/mask), and the requirement for efficient, lightweight algorithms.

Future developments are focusing on using blockchain for secure, decentralized storage of biometric data, and using 6G connectivity for real-time applications in smart cities and healthcare.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 1, January- February 2026 ||

DOI: 10.15680/IJCTECE.2026.0901014

This proposed system architecture outlines a secure, real-time biometric authentication solution for Internet of Things (IoT) devices, utilizing deep learning (DL) for accurate identification and encryption for secure communication, as shown in studies. The system addresses vulnerabilities in traditional password-based methods by using behavioral or .physical biometrics (face, fingerprint, ECG) and ensuring data privacy through encrypted templates

.VI :ACKNOWLEDGEMENT

Implementing Biometric Authentication in IoT environments leverages deep learning and encryption to overcome the vulnerabilities of traditional password-based systems. These frameworks utilize unique physiological traits—such as .fingerprints, facial features, or iris scans—to provide non-transferable identity verification

VII. CONCLUSION

This edge-based system advances IoT security with DL and encryption for privacy-preserving authentication. The integration of deep learning-based biometric authentication with encrypted verification in Internet of Things (IoT) devices offers a secure, reliable, and userfriendly alternative to traditional, vulnerable authentication methods. Deep learning models, particularly Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM), achieve high recognition accuracy (over 98% in many scenarios) for various biometric traits The combination of biometric data with cryptographic techniques (e.g., Paillier public key encryption) ensures end-to-end security, mitigating risks of man-in-the-middle, replay, and spoofing attacks. Unlike static password authentication, IoTbased biometrics allow for continuous, behavioral authentication (e.g., gait, heartbeat) that constantly verifies users during a session. Future developments are aimed at improving real-time performance through blockchain-based .decentralization and mitigating data privacy risks through federated learning

REFERENCES

1. Poornima, G., & Anand, L. (2025). Medical image fusion model using CT and MRI images based on dual scale weighted fusion based residual attention network with encoder–decoder architecture. *Biomedical Signal Processing and Control, 108*, 107932.
2. Saravanan, M., & Sivakumaran, T. S. (2016). Three phase dual input direct matrix converter for integration of two AC sources from wind turbines. *Circuits and Systems, 7*, 3807–3817.
3. Feroz, A., Pranay, D., Srikar Sai Raj, B., Harsha Vardhan, C., Rohith Raja, B., Nirmala, B., & Dharnasi, P. (2026). Blockchain and machine learning combined secured voting system. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9*(1), 119–124.
4. Madheswaran, M., Dhanalakshmi, R., Ramasubramanian, G., Aghalya, S., Raju, S., & Thirumaraiselvan, P. (2024, April). Advancements in immunization management for personalized vaccine scheduling with IoT and machine learning. In *2024 10th International Conference on Communication and Signal Processing (ICCSP)* (pp. 1566–1570). IEEE.
5. Inbavalli, M., & Arasu, T. (2015). Efficient analysis of frequent item set association rule mining methods. *International Journal of Scientific & Engineering Research, 6*(4).
6. Varshini, M., Chandrapathi, M., Manirekha, G., Balaraju, M., Afraz, M., Sarvanan, M., & Dharnasi, P. (2026). ATM access using card scanner and face recognition with AIML. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9*(1), 113–118.
7. Kiran, A., Rubini, P., & Kumar, S. S. (2025). Comprehensive review of privacy, utility and fairness offered by synthetic data. *IEEE Access*.
8. Ananth, S., Radha, D. K., Prema, D. S., & Nirajan, K. (2019). Fake news detection using convolution neural network in deep learning. *International Journal of Innovative Research in Computer and Communication Engineering, 7*(1), 49–63.
9. Akula, A., Budha, G., Bingi, G., Chanda, U., Borra, A. R., Yadav, D. B., & Saravanan, M. (2026). Emotion recognition from facial expressions using CNNs. *International Journal of Engineering & Extended Technologies Research (IJEETR), 8*(1), 120–125.
10. Dharnasi, P. (2025). A multi-domain AI framework for enterprise agility integrating retail analytics with SAP modernization and secure financial intelligence. *International Journal of Humanities and Information Technology, 7*(4), 61–66.
11. Lakshmi, A. J., Dasari, R., Chilukuri, M., Tirumani, Y., Praveena, H. D., & Kumar, A. P. (2023, May). Design and implementation of a smart electric fence built on solar with an automatic irrigation system. In *2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)* (pp. 1553–1558). IEEE.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 1, January- February 2026 ||

DOI: 10.15680/IJCTECE.2026.0901014

12. Sakthivel, T. S., Ragupathy, P., & Chinnadurai, N. (2025). Solar system integrated smart grid utilizing hybrid coot-genetic algorithm optimized ANN controller. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, 1–24.
13. Sugumar, R. (2025). Explainable AI-driven secure multi-modal analytics for financial fraud detection and cyber-enabled pharmaceutical network analysis. *International Journal of Advanced Research in Computer Science & Technology (IJARCST), 8*(6), 13239–13249.
14. Yashwanth, K., Adithya, N., Sivaraman, R., Janakiraman, S., & Rengarajan, A. (2021, July). Design and development of pipelined computational unit for high-speed processors. In *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1–5). IEEE.
15. Saravanan, M., Kumar, A. S., Devasaran, R., Seshadri, G., & Sivaganesan, S. (2019). Performance analysis of very sparse matrix converter using indirect space vector modulation. *International Journal of Innovative Technology and Exploring Engineering, 9*(1), 4756–4762.
16. Poornachandar, T., Latha, A., Nisha, K., Revathi, K., & Sathishkumar, V. E. (2025, September). Cloud-based extreme learning machines for mining waste detoxification efficiency. In *2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* (pp. 1348–1353). IEEE.
17. Aashiq Banu, S., Sucharita, M. S., Soundarya, Y. L., Nithya, L., Dhivya, R., & Rengarajan, A. (2020). Robust image encryption in transform domain using duo chaotic maps—A secure communication. In *Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020* (pp. 271–281). Springer.
18. Prasanna, D., & Manishvarma, R. (2025, February). Skin cancer detection using image classification in deep learning. In *2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS)* (pp. 1–8). IEEE.
19. Gogada, S., Gopichand, K., Reddy, K. C., Keerthana, G., Nithish Kumar, M., Shivalingam, N., & Dharnasi, P. (2026). Cloud computing/deep learning customer churn prediction for SaaS platforms. *International Journal of Computer Technology and Electronics Communication (IJCTEC), 9*(1), 74–78.
20. Amitha, K., Ram Manohar Reddy, M., Yashwanth, K., Shylaja, K., Rahul Reddy, M., Srinu, B., & Dharnasi, P. (2026). AI empowered security monitoring system with the help of deployed ML models. *International Journal of Computer Technology and Electronics Communication (IJCTEC), 9*(1), 69–73.
21. Sammy, F., Chettier, T., Boyina, V., Shingne, H., Saluja, K., Mali, M., ... & Shobana, A. (2025). Deep learning-driven visual analytics framework for next-generation environmental monitoring. *Journal of Applied Science and Technology Trends*, 114–122.
22. Prasanna, D., Ahamed, N. A., Abinesh, S., Karthikeyan, G., & Inbatamilan, R. (2024, November). Cloud-based automatically human document authentication processes for secured system. In *2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS)* (pp. 1–7). IEEE.
23. Ananth, S., Radha, D. K., Prema, D. S., & Nirajan, K. (2019). Fake news detection using convolution neural network in deep learning. *International Journal of Innovative Research in Computer and Communication Engineering, 7*(1), 49–63.
24. Karthikeyan, K., & Umasankar, P. (2025). A novel buck-boost modified series forward (BBMSF) converter for enhanced efficiency in hybrid renewable energy systems. *Ain Shams Engineering Journal, 16*(10), 103557.
25. Karthikeyan, K., Umasankar, P., Parathraju, P., Prabha, M., & Pulivarthy, P. Integration and analysis of solar vertical axis wind hybrid energy system using modified zeta converter.