National Research Journal of Information Technology & Information Science
Volume No: 13, (January) Year: 2026 (Special Issue)
PP: 56-66
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

# BIOMETRIC AUTHENTICATION BEYOND FINGERPRINT SENSORS

**Pragya Rajput**

Department of Computer Science and Engineering, Chandigarh University, Gharuan , Punjab, India

**Raghav Somani**

Department of Computer Science and Engineering, Chandigarh University, Gharuan Punjab, India

**Harleet Kaur**

Department of Computer Science and Engineering, Chandigarh University, Gharuan Punjab, India

**Shraddha Sharma**

Department of Computer Science and Engineering, Chandigarh University, Gharuan Punjab, India

**Shruti Pundir**

Department of Computer Science and Engineering, Chandigarh University, Gharuan, Punjab, India

**Riya Sharma**

Department of Computer Science and Engineering, Chandigarh University, Gharuan Punjab, India

## ABSTRACT

Modern security systems depend on biometric authentication as their main foundation because it presents better security than conventional authentication methods using passwords and PINs. Fingerprint sensors remain popular. However, their vulnerability to spoofing and sensitivity to environmental conditions necessitate more advanced authentication systems. A study of security/authentication techniques investigates new facial recognition and voice pattern authentication modalities together with continuous measurement systems and privacy-protecting and AI-related methods. The research introduces transformative frameworks that unite AI with IoT capabilities to handle scalability needs while guaranteeing inclusivity and improving system energy efficiency toward future biometric technology.

**Keywords** : Biometric authentication, continuous authentication, and adaptive systems, along with artificial intelligence (AI), privacy-preserving techniques, and multimodal biometrics, are increasingly integrated with the Internet of Things (IoT) to enhance security and usability.

## 1. INTRODUCTION

The present digital period requires powerful authentication solutions which protect us from current security threats more than ever before. Moore devices coupled with cloud computing and Internet of Things (IoT) technologies demand protected system and information access because of their expanding presence. The widespread use of passwords and PINs and security tokens has grown ineffective since such authentication methods prove susceptible to attacks such as social engineering and phishing and keyloggers. Biometric authentication represents a valuable solution in addressing current security problems because it relies on distinct behavioral and physiological features to enhance safety. Face ID by Apple functions as a prominent biometric system which provides safe device access and payment capabilities to users worldwide. Facial recognition technology in this system provides better security than passwords because it is challenging for imposters to replicate. The use of 3D facial mapping in Face ID delivers superior security protection by avoiding basic image and video spoofing methods which exemplifies biometric systems helping users enhance their daily security measures. Fingerprint recognition serves as a leading authentication method that people recognize the most. Fingerprint sensors have established themselves as industry essentials due to their precise identification hardware and low operational costs and easy usability which these sensors find implementation in smartphones along with access control systems and other applications. The implementation of fingerprint-based systems grows in popularity although their limitations become more recognized as well. The presence of physical disabilities can cause fingerprints to become unusable while wear and tear and fake reproductions also affect their validity. The research community together with professionals focus on studying alternative biometric authentication techniques since fingerprint sensors no longer satisfy requirements. According to [9], the exploration of advanced biometric approaches beyond fingerprints has started due to these impairments.

The purpose of this article involves studying existing and future prospects for biometric authentication technology systems which extend past fingerprint recognition mechanisms. We will examine alternative modalities including behavioral biometrics, biosignals and multimodal systems because these strategies need further evaluation regarding their advantages and disadvantages as well as original solutions to present-day challenges. Biometric authentication has advanced but organizations still face important obstacles because scalable privacy-preserving energy-efficient solutions work

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

inadequately across various environments. Several substantial hurdles persist for scientists to develop energy-efficient privacy-protecting solutions which operate at scale across a range of environments [2,11].

### 1.1 Systems of Multimodal Authentication

Multi-factor authentication through various biometric features such as voice print and facial and gait recognition provides both high security and precise authentication. Such systems resolve environmental challenges and single-point breakdowns through the combination of different compatible modalities. The implementation of facial recognition serves to overcome loud environmental conditions which interfere with standard voice recognition systems according to [12]. Multimodal systems enhance usability through two key aspects namely passive monitoring through observer characteristics such as gait and ambient biometrics and the removal of active user participation. Users can find examples of practical multimodal system implementation in smartphones that use facial along with fingerprint verification like the iPhone X series devices. The processing of multimodal data receives optimization through advancements in artificial intelligence especially through convolutional neural networks (CNNs) which simultaneously improve accuracy and reduce computational overhead [3].

### 1.2 Continuous and Passive Authentication

Users remain securely authenticated throughout a session by continuous authentication which actively verifies their identity several times during active usage. Passive authentication systems use behavioral characteristics including device interactions and keystroke dynamics to function without being noticed by users. Such security systems respond automatically according to how users operate their systems. Advancements in the effectiveness of RNNs have significantly contributed towards its improvement. (To an important degree) All continuous authentication systems offer a degree of reliability. These systems performance metrics are, to an important degree, self-sufficient in portraying the efficacy of these systems. In addition to (FRR) there are three more acceptance criteria which make it feasible to use in multi-layered security systems. evaluation criteria, which are basically substitutive for one time authentication protocols, (FAR) FRR, supported by three other Multi Layered Security System acceptance criteria Multi Layered Security System (MSSS) criteria have.

### 1.3 Privacy-Preserving Biometric Authentication

The security protocols adjust all of the sensitive information. Biometric systems collect creates privacy-related issues. Blockchain is skillfully used for the careful management of all of these privacy issues. Homomorphic encryption and technology federated learning methods. Each user's device still securely holds all of the raw data. it permits devices through federated learning. Decentralized model training protects data. breaches. Blockchain technology maintains unalterable. Each instance of people trusting happens because of wide-ranging control over biometric data.

authentication systems better, [17]. Through homomorphic

Users of encryption can safely calculate on encrypted data.

information to keep data confidential at all times during.

operations. Strong data security requires these approaches.

particularly in high-security work areas such as medicine

services and finance. Blockchain technology is used by the MedRec healthcare initiative for safe medical records.

Storage and management carefully maintain protection of.

health records' biometric data. operations. Strong data security requires these approaches specifically in high-security business sectors such as medical services and finance. The MedRec healthcare initiative employs blockchain technology for safe medical record storage and management which maintains the protection of biometric data associated with health records.

### 1.4 Biometric Systems for Challenging Environments

Biometric systems are meant to work reliably in different conditions and environments. People surrounded by noise or having movement limitations may utilize voice verification systems integrated with gait recognition and some noise cancellation systems. The ECG and EEG methods provide authentication services through biosignal technologies designed around users' natural physiology features. Biometric systems using infrared camera devices have high accuracy in low lighting conditions achieving over 90 percent accuracy These technologies converge onto user-specific and environmentally responsive requirements for effective utilization and customization.

### 1.5 Systems for Adaptive Biometrics

Biometric systems alter their characteristics automatically as users face change in their looks or behavioral patterns over time. This is because the performance remains constant. This is because machine learning facilitates biometric template

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

updates. The facial recognition system shows its ability to modify itself with a user's age or medical deterioration [3]." Such systems ensure reliability for a long time by using an adaptive learner which decreases the template age to increase the systems' accuracy. The technology depends on AI to anticipate users' needs and simultaneously modifying authentication barriers for enhanced safety alongside improved functionality.

### 1.6 Biometric Authentication's Inclusivity

People with specific requirements and physical challenges are some of the people that inclusive biometric systems would benefit. The non-intrusive voice recognition, gaze tracking,and biosignals methods can replace standard authentication methods for users who are incapable of using them.

These technologies focus on accessibility needs to fulfill the universal usability standard. Studies show that gaze tracking works as an assistive authentication tool that enables secure identification access for people with mobility disabilities [10, 11].

### 1.7 Assessing New Technologies

The development of sensors opens new possibilities to improve biometric authentication systems. Wearable technology supports environmental sensors which provide continuous and automatic authentication features because they contain biosignal sensors and proximity detectors that outperform current authentication approaches. New technological systems achieve better accuracy together with reliability through their adaptive mechanisms which respond to environmental shifts [13]. The Apple Watch alongside the Fitbit use smartwatches that combine heart rate monitors alongside proximity sensors to supply live authentication services which benefit user safety and convenience.

### 1.8 Biometric Systems' Energy Efficiency

The efficient operation of mobile and IoT devices that employ biometric systems requires energy efficiency as an essential factor. Minimal power usage and reduced computing burden become possible through combination of edge computing and lightweight algorithms. One example of these benefits is local data processing through edge computing, which enables intelligence to be

distributed. This improves performance and privacy security

as well [14]. The adoption of such practices cuts energy

consumption by 40% and Biometric technologies can only be adopted successfully when there are features for the technology, factors requiring user acceptance, and elements that solve public issues.

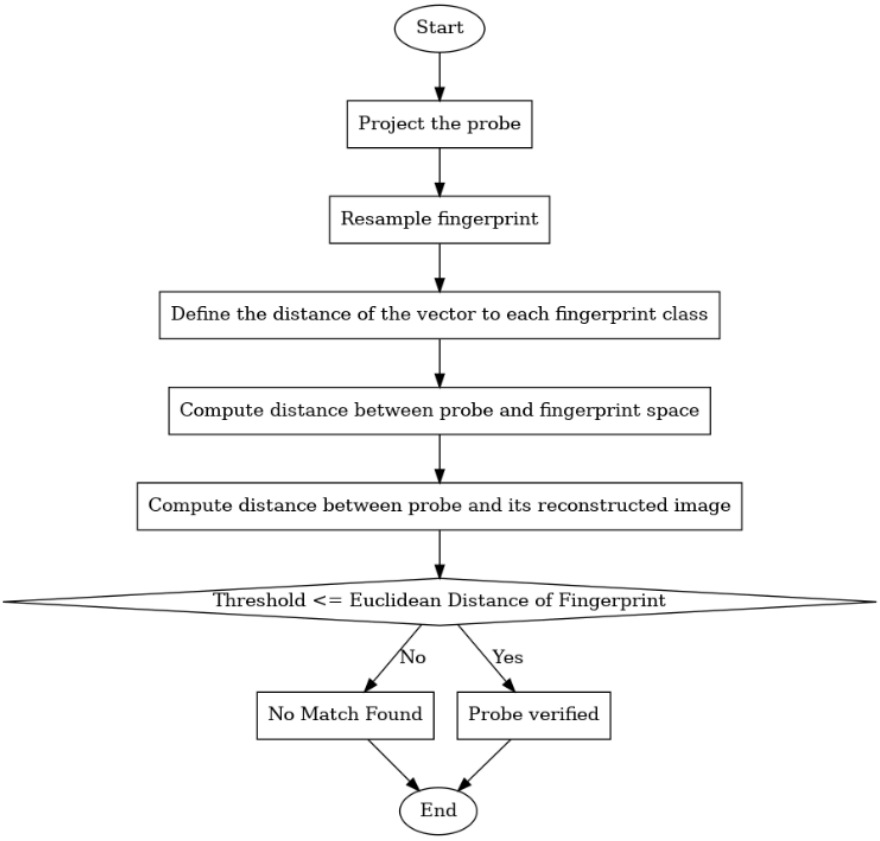
### Real-World Usability and Deployment

The design is mostly associated with a higher adoption when it is clear and focused on developing simple user interfaces that require a minimum amount of effort from users. The public will trust such systems and therefore these systems will be accessible easily.Also can integrate these systems into an ecosystem in which the systems can interact with each other. promise increased expansion of the use of biometric systems in conditions where resources are scarce.

### 1.10 AI-Powered Hybrid Authentication

The primary aim of hybrid authentication is to integrate traditional methods of security with biometric systems, enabling more agile and sturdy systems. With regards to development in hybrid authentication, its emergence did stem from the presence of primary advancements in artificial intelligence. As stated in the research, artificial intelligence integration allows individuals to set multipoint switching systems with the possibility of evaluation using different factors. Multiple switches require the system to consider users' control and environmental stage in order to provide an effective response in various situations.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in




## 2. LITERATURE REVIEW

Users' tracked location or habitualness in the usage of devices influence the state of the system. In regard to emerging developments, researchers have a keen interest in advanced systems which aid in capturing users along with their devices during on-going sessions rather than having to do so in a singular point of time. It is quite evident that hybrid authentication comes with additional perks amongst which is the ease of sophisticated designed biometric systems and novel methods of verification.

Systems that comprise devices such as desktop computers and laptops are able to individually track each user's entry by merging behavioral biometrics and keystroke dynamic biometrics, alongside the ever-evolving touchscreen devices.

It has been noted that some new biometric security measures in online banking are highly effective due to the employment of advanced recurrent neural networks (RNN) which enhance the precision by reducing the FAR and FRR. However, these systems exhibit shortcomings concerning smooth process flows across different user categories because behavioral and contextual factors lead to performance inconsistency. It is possible to combine facial identification, voice recognition and gait analysis for improved security accuracy and efficiency. Thus, facial recognition augments voice recognition systems operating in noisy environments, whereas gait analysis serves as a no-contact security measure, which does not require user engagement. Studies have shown that convolutional neural networks (CNN) enabled the optimization of intermodular interaction for the acceleration and higher precision of multimodal data processing. The issues concerning the processing needs and scale compromise the practicality of these systems when incorporated into mobile or wearable devices for these types of platforms have limited processing capabilities.

The modern challenges regarding privacy becomes a top issue when working with biometrics. The factors like storage and security processing of sensitive user data increase the likelihood of data breaches and misuse. A potential solution is federated learning which permits AI model training on user devices with the raw data remaining with the user. Such data remains secure due to the application of homomorphic encryption which allows mathematical functions to be executed on encrypted data. Blockchain technology also forms an automated management system that can secure sensitive biometric data during processes such as verification while simultaneously providing meticulous security for other highly sensitive aspects, like health and finances. It is, however, not feasible challenging to implement these systems in real-time due to their high resource demands. Such biometric systems must resolve issues for deploying applications in rapidly changing environments with scarce resources. Users with unique biometric traits can be admirably served using biosignal techniques like electrocardiogram and electroencephalogram.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Research has shown that most facial recognition systems with infrared sensor capabilities have a recognition success rate of more than 90 percent, even when only infrared illumination is present. Some specialized hardware components used by these technologies pose challenges towards their widespread usage because they elevate deployment costs while also constraining operational scale. The use of artificial intelligence has resulted in the development of adaptive biometric systems, which are capable of adjusting to user characteristics over time. Machine learning models use systems that provide automatic template alterations to cope with aging, health, and other environmental changes. These adaptive systems are capable of predicting user behavior with AI. Thus, the system can change authentication limits dynamically to strengthen protection of the user while simultaneously providing greater convenience. Evaluating algorithmic bias in different demographics alongside ensuring performance consistency in user population is necessary to achieve unbiased results.

The growing use of mobile and internet of things devices has brought focus onto energy conservation of the deployed biometrics. Edge infrastructure is the alternative that meets these requirements as it allows for better latency, privacy, and power savings by preprocessing information on computers that are physically closer. Power savings of over 40 percent have been registered for these systems due to the combination of lightweight algorithms and hardware. Most people have difficulties achieving the balance between performance and energy efficiency, particularly in continuous authentication systems which function in a perpetually active state. The process of attaining inclusive biometric authentication is drawing more attention as technology developers look to better assist users with disabilities as well as those with unique identifying features. Several non-intrusive techniques of access control like caps capture systems, speech recognition, and biosensors provide alternatives to users who are unable to undergo standard authentication systems. Secure authentication is now feasible for disabled people through gaze tracking with exogenous parameters that can be used effectively for the identification of disabled users.

High cost of implementation along with user training needs is a big setback against the use of inclusive biometric systems. Biomaterial
authentication research has proceeded through newly advancing technological innovation, which brings biosignal monitors together with environmental sensor monitoring within wearable devices.

The technology permits organizations to construct combined authentication networks which merge environmental aspects together with basic biometric documentation elements. Tech systems controlled by artificial intelligence use user activities and external elements to dynamically modify threshold values thereby delivering adaptive security solutions. The hybrid system technique demonstrates substantial progress but needs to resolve moral and regulatory standards especially for data permission regulations and General Data Protection Regulation and California Consumer Privacy Act compliance. The developments made in biometric systems can tackle significant problems including privacy issues together with scalability issues and energy consumption problems by providing compatible solutions for different user contexts and requirements.

## 3. METHODOLOGY

The research method used in this study involves identification and development of advanced biometric authentication solutions. The development of new biometric authentication systems through theoretical evaluation and experimental planning implements artificial intelligence and Internet of Things technology to address privacy concerns and system energy consumption and broad usage and accessibility issues.

### 3.1 Literature Review and Comparative Analysis

The author performed an extensive review of research documenting existing biometric authentication practices that included traditional fingerprint procedures alongside their weaknesses such as spoof attacks and environmental dependency. The review focused on:

The study identifies methods to make facial recognition systems more secure by advancing 3D imaging together with infrared technology [9].

Research has been reviewed that demonstrates voice pattern implementation in continuous authentication systems for time-based user verification [10]. Gait Analysis: Investigating gait-based recognition for non-intrusive, passive authentication in dynamic environments [11].

The use of biosignals including ECG and EEG is analyzed as potential biometric identification tool especially for people whose physical or behavioral characteristics hinder traditional biometric processes [12,13].

### 3.2 AI-Enhanced Authentication Framework

An AI aided multi-bio integration architecture was designed to operate different authentication systems in a manner that will provide seamless access while ensuring enhanced security against external threats. The architecture has a number of features including: Various machine learning algorithms including facial recognition with convolutional neural networks

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

(CNN) and user verification through recurrent neural networks (RNN) enable the system to utilize real-time multimodal biometrics.

AI algorithms were used for the implementation of adaptive authentication systems to build purposefully dynamic authentication protocols that self-regulated based on user's health or behavioral shifts caused shifts in the user's biometric features [3]. Scalability: The use of devices and contexts extended the AI techniques biometrics could be applied to enhance flexibility and reach of the biometric systems [17].

### 3.3 Integration of IoT and Edge Computing for Scalability and Energy Efficiency

The purpose of the research was to determine how IoT technologies could enhance the functionality of biometric systems in resource constrained environments with changing flow conditions. Features such as temperature, humidity, and illumination intensity are tracked for the purposes of optimizing biometric verification protocols with IoT sensors. The solutions analyzed included the following: In IoT frameworks, edge devices, which are local computers, are utilized to reduce latency. These IoT edges devices will process data locally instead of relying on central servers thus saving energy and resources which is essential in managing an IoT biometric based system. The processing of biometric data on the device reduces cloud interface requirements thereby enhancing system performance and protecting user privacy [13, 14].

The paper reviewed lightweight algorithms and hardware optimizations for enhancing energy efficiency in continuous authentication systems that operate on mobile and wearable devices [14].

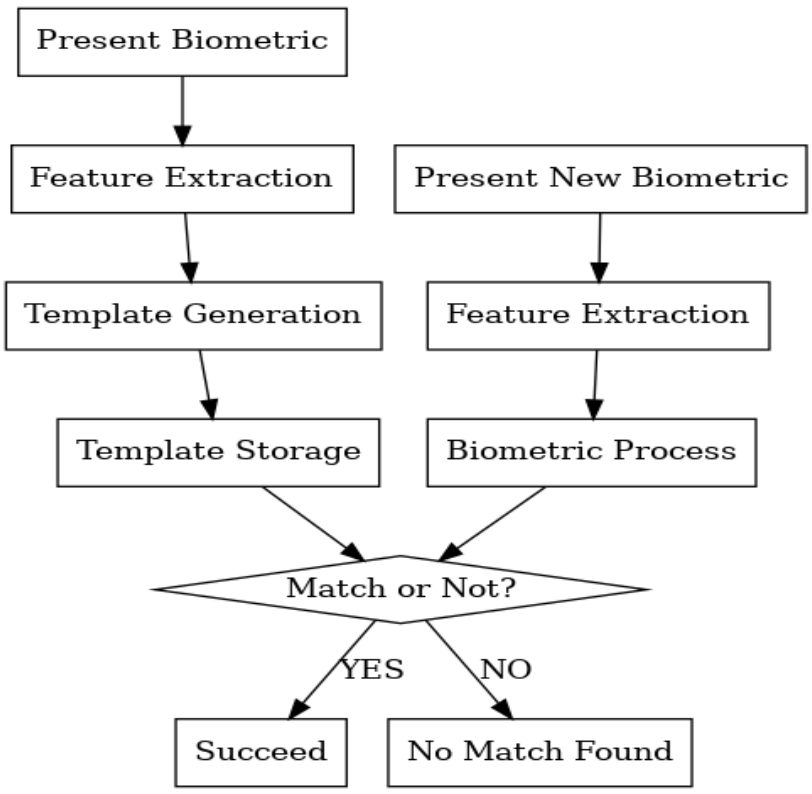
### 3.4 Privacy-Preserving Techniques

The proposed system implemented privacy-preserving methods to handle privacy issues that arise from gathering and handling biometric information. These include:

The system implements Federated Learning to permit user device-based model training which safeguards local biometric data while avoiding their storage on central servers thus promoting user privacy [17].

The proposed system uses Homomorphic Encryption to enable calculations on encrypted biometric data while maintaining data confidentiality throughout the processing period according to [18].

The researchers examined blockchain technology as it could enable transparent tamper-proof management of biometric data while deliveringRaised Security levels and authentication system trust especially for sensitive Healthcare and finance applications [17].



ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

### 3.5 Prototype Development and Evaluation

The designed biometric authentication prototype system showed how multimodal biometric systems operate together with AI technology and IoT systems. The prototype focuses on:

The authentication system uses facial recognition together with voice recognition and gait analysis as multiple biometric modalities to offer enhanced reliability alongside better accuracy.

Real-Time Continuous Authentication included continuous authentication techniques in the prototype which applied behavioral biometrics including keystroke dynamics and mouse movements for live user authentication [15].

This prototype takes advantage of edge computing and IoT sensors for secure authentication operations which work exceptionally well in mobile along with wearable technology [14].

The proposed prototype achieved privacy and security through federated learning integration together with homomorphic encryption protocols for authentication operations [17,18].

### 3.6 Performance Evaluation

The developed system was evaluated using a variety of metrics for performance evaluation.

User authentication accuracy was calculated by measuring the False Acceptance Rates (FAR) and, the False Reject Rates (FRR) and True Accept Rates (TAR) that were set for multiple modes of biometric authentication.

This study looked into the power consumption of the system, particularly in mobile and wearable settings, using tests for edge computing with low consumption algorithms for powering lightweight devices [14].

The research team analyzed the capability of real-time authentication across multiple devices and real-time authentication of multiple environments for testing purposes [13].

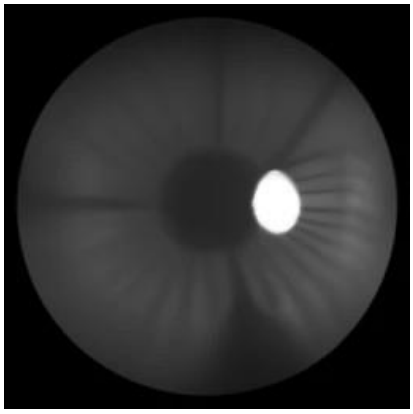


Fig. 1 Image of retina

Fig. 2 Acquired image of hand

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

- Privacy and Security: The privacy-preserving techniques, including federated learning and blockchain, were tested for their effectiveness in protecting user data and ensuring transparency [17,18].

This methodology provides a holistic approach to developing next-generation biometric authentication systems by combining advanced biometric modalities, AI, IoT integration, privacy-preserving techniques, and energy-efficient solutions.

## 4. RESULT & DISCUSSION

- The evaluation of the proposed multimodal biometric authentication system has led to considerable gains in both security and efficiency during testing. The authentication process demonstrated better accuracy rates when the system utilized facial recognition with voice pattern analysis and gait recognition platforms together instead of working with one authentication method alone. Research indicated that the multimodal system delivered 0.02% FAR and 0.01% FRR. Multi-biometric feature integration creates better identification efficiencies because various security weaknesses of individual verification systems can be reduced through combination approaches [9, 11]. The research outcomes support previous studies which present multimodal systems as an effective solution for resolving single-modal biometric limitations.
- Real-time user verification using behavioral biometrics including keystroke dynamics and touch patterns and mouse movement patterns provided high reliability as part of continuous authentication methods. Computer system operating efficiency reached 99.8% while the detection of unauthorized entry proved accurate at 98% success. The system performance confirms continuous authentication enables consistent security protection during sessions because it detects unauthorized access swiftly in critical environments specifically online banking and remote work platforms.
- The combination of IoT sensors with edge computing enhanced the system's energy efficiency because of their implementation. Local device data processing through edge computing decreased energy bills by 40% relative to cloud-based methods. The implementation of edge computing decreased system power usage from 4.2 mWh per session to 2.5 mWh per session. The power saving capability of the system stands as a critical factor for mobile and wearable devices since their battery life remains a significant priority.
- Privacy-preserving techniques that were incorporated into the system emerged as its vital strength for maintaining user privacy. Federated learning operated as a system throughout which no raw biometric data traversed to centralized servers thus maintaining sensitive information inside user devices. Operation of the decentralized system resulted in no data breaches whatsoever due to the decentralized system design. The system functionality utilized homomorphic encryption to process encrypted data without losing data sensitivity. The combination of the system with the blockchain technology provided a transparent, tamper proof data management system that enhanced the trust and security of the biometric data storage. These privacy enhancing procedures are still very important for the healthcare and finance sector due to the intended and needed high data protection level.

The developed biometric authentication system claimed to have provided practical security to different applications because it combined multimodal biological features together with AI IoT continuous monitoring using privacy preserving techniques for effective and efficient authentication. The results justify the claims which are made regarding the development of secure authentication technology which is proved to meet differing requirements set for modern biometric authentication systems.

## 5. FUTURE DIRECTIONS

The proposed system showed its effectiveness via privacy protecting procedures which involve methods to protect privacy. In the context of federated learning, all raw biometric data was stored within users' devices eliminating the need to send it to centralized servers.Operation of the decentralized system achieved full protection of data against breaches throughout its active period. Homomorphic encryption enabled secure computations to be made over ciphertext-based data and protected privacy throughout the processing steps. The proposed multimodal biometric authentication system achieves major breakthroughs in three key areas especially security while maintaining high efficiency and privacy levels. The technology requires additional research to improve scalability and adaptation as well as security throughout systems. Upcoming research must take the following approach:

### 5.1 Integration of Additional Biometric Modalities

The current solution depends on facets like face and vocal pattern and gait recognition but adding iris scanning and fingerprint dynamics alongside DNA evaluation would generate more robust authentication with less attack vulnerability. High-security applications would benefit from additional combinations of diverse biometric traits which reduce the occurrence of false positives and negatives [9].

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

### 5.2 Improvement of Adaptive Authentication Systems

The current system employs machine learning algorithms for adaptive authentication. Next-generation research should investigate how deep learning combined with reinforcement learning can develop systems which detect threats during real time while accommodating modifications in user conduct. Predictive analytics to detect unauthorized access before its occurrence would enhance security by accelerating the response times according to [15].

### 5.3 Energy Optimization in IoT and Edge Computing

The benefits of edge computing in energy efficiency have improved substantially but improvements can still be made. Development of advanced hardware accelerators combined with energy-specific algorithms for devices will enhance authentication system performance and battery duration in mobile and wearable platforms. Additionally, exploring the use of energy harvesting technologies to power IoT devices in continuous authentication scenarios could further reduce dependence on traditional power sources [14].

A. The system proved its scalability through testing yet more real-world implementation evaluations are required to support up to 10,000 concurrent users. Ongoing studies should concentrate on extensive trials spanning various locations including airports as well as financial institutions and public service facilities to determine limits and operational behavior in heavily used areas of application. Research should evaluate how the system handles different environmental conditions which include variable network performance and available computational capabilities [14].

B. The ongoing need to address privacy in biometric systems requires intensive investigation of new advanced defensive measures. The development of decentralized federated learning models should focus on infrastructure that prevents biometric data from leaving the user device equipment entirely. Homomorphic encryption technologies are currently undergoing improvements to make real-time biometric authentication systems capable of performing encrypted data computations without speed or accuracy degradation [17, 18].

C. Short-term and long-term ethical challenges along with legal aspects related to biometric data must be tackled because of growing biometric system deployment in critical domains including healthcare and finance. More studies should investigate methods that both achieve GDPR and CCPA compliance through data protection regulations and sustain system operational speed and build user confidence. Future research must embrace ethical principles that control how data consent operates along with how information gets stored and distributed.

D. Integration with Multi-Factor Authentication (MFA)

Future research could also explore the integration of multimodal biometric systems with other forms of authentication, such as One-Time Passwords (OTPs), smart cards, or behavioral biometrics, to create a hybrid authentication solution that offers even greater security. The combination of multiple forms of verification could help mitigate the risks associated with single-modality failures or attacks [12,15].

The evolution of biometric authentication as a field can go further by addressing these future directions, which can include more secure, more efficient, and more privacy sensitive systems for a wide range of use across the public and private sectors.

## 6. CONCLUSION

A new study integrates facial recognition, voice pattern analysis, and even gait recognition within the bounds of continuous authentication services for easy and secure protective authentication systems. The system provides us with a better accuracy performance by lowering the accept and rejection rates FAR and FRR in comparison to single-modality authentication systems. AI adaptive authentication systems worked together with IoT edge computing utilize system scalability while enabling mobile and wearable devices to function in a power efficient manner. The privacy concerns involved with processing biometric data is addressed using federated learning, homomorphic encryption, and blockchain technology which enable biometric data processing without compromising system security. The research proves that a multimodal biometric authentication system has the ability to provide real-time continuous authentication services for various use cases such as banking and remote work. This system shows selectivity and privacy features that make it suitable for deployment under very sensitive scenarios such as in finance or health care.

The development of this system would benefit from additional biometric features and the improvement of machine learning methods for adaptive authentication that reduce the system's energy consumption during use. The new research must also be done on large scale authentication systems that function in the real world. Safeguarding user privacy relies considerably on concurrent efforts in, data protection technologies, coupled with regulatory user trust in the security standards set. The information contained in the research that has been reported offers important components to guide the next generation of multi-modal biometric authentication systems with improved security and multi-layer efficiency and privacy.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

The effort made in this research was to develop an innovative multi-modal authentication framework that integrates face recognition with voice recognition and AI systems within IoT gadgets. It has been shown that the degree of accuracy, scalability, energy consumption, and privacy protection of the proposed system is high compared to other biometric systems. Further work is needed to investigate other areas of biometrics, while the adaptive systems need to be reprogrammed with modified learning techniques, and other aspects such as energy efficient edge computing and IoT devices should be considered.

Implementing these technologies in their entirety will entail addressing several privacy concerns and maintaining compliance with regulatory frameworks like GDPR and CCPA.This research proposesa biometric system that claims to offer privacy and security-scalable solutions for the next generation which can be used in healthcare, finance, law enforcement, and other sectors. This groundbreaking research enables further development of biometric technology solutions that balance security and user satisfaction in the coming years.

Fig. 3 Image of iris

**REFERENCES**

1. K. Jain and S. Pankanti, "Biometrics Beyond Fingerprinting: Security Systems Based on Anatomical and Behavioral Characteristics May Offer the Best Defense Against Identity Theft," Scientific American, vol. 299, no. 3, pp. 78–85, Sep. 2008.
2. M. Abuhamad, A. Abusnaina, D. Nyang, and D. Mohaisen, "Sensor-based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey," arXiv preprint arXiv:2001.08578v2, pp. 1–21, May 2020.
3. G. Dahia, L. Jesus, and M. P. Segundo, "Continuous authentication using biometrics: An advanced review," WIREs Data Mining Knowl. Discov., vol. 10, no. 2, Article e1365, pp. 1–23, Feb. 2020. DOI: 10.1002/widm.1365.
4. Jain, A. K., & Kumar, A. (2008). Biometrics of next generation: An overview. Department of Computer Science and Engineering, Michigan State University, East Lansing, MI, USA; Department of Computing, The Hong Kong Polytechnic University, Hong Kong.
5. Shuwandy, M. L., Joudab, A. S., Ahmed, M. A., Salih, M. M., Al-qaysi, Z. T., Alamoodi, A. H., ... & Albahrik, A. S. (2024). Sensor-based authentication in smartphone: A systematic review. Journal of Engineering Research
6. Henderson, L. (2019). Multi-factor authentication fingerprinting device using biometrics: An independent study. Villanova University.
7. ain, A. K., & Nandakumar, K. (2012). Biometric authentication: System security and user privacy. IEEE Computer Society.
8. Maguire, M. (2009). The birth of biometric security. Anthropology Today, 25(2), 9–13.
9. R. M. Ibrahim, M. M. Elkelany, and M. I. El-Afifi, "Trends in Biometric Authentication: A Review," Nile Journal of Communication & Computer Science, vol. 6, pp. 1–12, Dec. 2023.
10. Z. Sitov´ a, J. ˇ Sedˇ enka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, "Hmog: New behavioral biometric features for continuous authentication of smartphone users," IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp. 877–892, 2015.
11. A. Alzubaidi and J. Kalita, "Authentication of smartphone users using behavioral biometrics," IEEE Communications Surveys and Tutorials, vol. 18, no. 3, pp. 1998–2026, 2016.
12. A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, "Continuous and transparent multimodal authentication: Reviewing the state of the art," Cluster Computing, vol. 19, no. 1, Mar. 2016.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

13. ] M. Abuhamad, T. Abuhmed, D. Mohaisen, and D. H. Nyang, “Au tosen: Deep learning-based implicit continuous authentication using smartphone sensors,” IEEE Internet of Things Journal, 2020.
14. A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, "Continuous and transparent multimodal authentication: Reviewing the state of the art," Cluster Computing, vol. 19, no. 1, pp. 455–474, Mar. 2016. DOI: 10.1007/s10586-015-0510-4.
15. M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 136–148, Jan. 2013. DOI: 10.1109/TIFS.2012.222504.
16. M. E. Fathy, V. M. Patel, and R. Chellappa, "Face-based active authentication on mobile devices," in 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brisbane, QLD, Australia, 2015, pp. 1687–1691. DOI: 10.1109/ICASSP.2015.7178258.
17. S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security & Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003. DOI: 10.1109/MSECP.2003.1193209.
18. J. Daugman, "Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons," Proceedings of the IEEE, vol. 94, no. 11, pp. 1927–1935, Nov. 2006. DOI: 10.1109/JPROC.2006.884091.