Archives of Pharmaceutical Sciences and Research E-ISSN0975-2633 | PRINTISSN0975-5284
Vol 16 Issue2 107-115 June 2026 Review Article

BIOMETRIC-BASED PATIENT IDENTIFICATION AND AUTHENTICATION IN DIGITAL EMERGENCY HEALTHCARE SYSTEMS

Varshini Arun[1], Sonaali S[1], Keerthan V[1], Poorvi L[1], Lavanya K[1], Arya J Gowda[1], Keerthisri Radha Rammohan[1], Akash D.V[1].

International Institute of Medical Science and Technology Council, Bengaluru, Karnataka

ABSTRACT

Misidentification of patients in emergency healthcare is a very serious issue that is a source of diagnostic errors, medication errors, and avoidable deaths. This paper discusses the six biometric modalities, which include fingerprint recognition, facial imaging, iris scanning, palm recognition, ECG biometrics, and multimodal systems and their accuracy, authentication efficiency, emergency suitability, and compatibility with electronic health records (EHRs). A conceptual multimodal biometric emergency authentication framework is suggested through a systematic review of 22 peer-reviewed articles obtained in IEEE databases and PubMed, including AI-based matching algorithms, role-based access levels in EHR and blockchain audit logs. Results show biometric systems minimize error of identification by about 83.5%. Facial recognition was identified as the most emergency-appropriate modality as it is non-contact, whereas BAPPIS fingerprint system had 96.9% protocol adherence with no false positives. The use of multimodal systems (facial, fingerprint, and iris recognition) was shown to be more robust under adverse conditions. Some of the major issues are that the identification of patients unconsciously is impossible, biometric privacy cannot be recovered, and the lack of regulatory frameworks.

KEYWORDS: Biometric authentication, patient identification, emergency healthcare, multimodal biometrics, facial recognition, fingerprint recognition, EHR integration, blockchain audit logs, AI matching algorithms, patient safety.

INTRODUCTION

1.1 Background and Significance

One of the pillars of effective and safe health care delivery is patient identification. Emergency health care environments may be prone to mistakes which may be caused by time constraints and the fact that some patients are uncooperative. Misidentification of a patient may result in disastrous errors like giving the wrong medicine to a patient, performing a surgery in the wrong place, giving the wrong blood during transfusion and many other clinical procedures that may cause harm or even death to the patient. According to the World Health Organization, most of the adverse events in the world are caused by patient misidentification, which can be avoided.

The traditional patient identification methods like the wrist band, patient cards, personal identification numbers (PIN), and verbal confirmation have proved to be very wanting in cases of emergency. Patients in a coma, the mentally challenged, or those who are in critical conditions cannot be able to authenticate their identities. Another problem is the popularity of the errors made with the help of paper or manual records. It is estimated by American Health Information Management Association (AHIMA) that 10 percent of patient records in a typical hospital are duplicate records. It can be as high as 24%. (Ahire et al. ,2024).

With the constant digitisation of health care systems (electronic health records, IoT devices to track patients, tele-health care, cloud-based clinical practice management software etc.) more possibilities of identity theft have been opened. Biometric authentication has turned out to be a special, safe and trusted procedure in such a scenario of safeguarding the identities of patients. Biometric identifications techniques include the capture and measurement of the physical (fingerprints, facial recognition, iris/ retina, palm veins, ECG etc.) or behavioural characteristics of the patients which only they have. They cannot be stolen by their owners; cannot be possessed by others or imitated. Thus, patient identification using biometric is an effective cybersecurity method. Biometrics is a major element in ensuring that there is digital

transformation of healthcare to paperless to electronic records. (Nair et al., 2022).

The biometrics market of the healthcare sector in the world reflects the importance of biometrics in the modern world, with a figure of USD 10.59 billion in 2023, which is expected to increase to USD 41.15 billion by 2030 at a CAGR rate of 21.42% (Mishra et al., 2020). The use of artificial intelligence along with biometric applications aids in making decisions in real-time in complicated emergency situations (Mishra et al., 2020). The recent technological advancement, involving the use of blockchain-based technologies, like MedBioCh (Belhocine et al., 2025), and artificial intelligence-based predictive systems (Kalaikumaran et al., 2025), signifies the future, in which the biometrics will not only identify, but also facilitate intelligent emergency management.

However, the application of biometrics in the emergency health care environment does have certain problems that are unique to the application and make it very different when compared to other uses. These are the handling of unconscious patients, the hygiene of the hardware when used by a large number of patients, the need to handle large number of patients and the need to integrate with existing hospital computer systems.

1.2 Problem Statement

The main concern that is being addressed with the help of this review is the problem of patient misidentification in an emergency care facility due to the traditional approach, and the absence of a unified body of knowledge that would evaluate the applicability of biometric technologies in the context of emergency use. Patient misidentification is a frequently committed type of medical error with severe consequences, with up to 13% of the total error-related to surgical procedures being patient misidentification alone, costing USD 17.4 billion annually.

Good demonstrations on the performance of the biometric technologies have been made in the clinical settings. However, it should be mentioned that, there are yet no significant clinical studies that would define the efficiency of these technologies, their practicability, and their safety when using them in actual emergency practice. It is crucial to note that the problem of working with unconscious patients, physically harmed patients who are not able to give information and with patients that have high urgency requirements has been lacked in the research.

In addition, most of the existing systems operate in isolation, as they are tested on simulated databases rather than on real life databases that are implemented in the country by EHRs. Equity is also an area that has not been researched well: the problem of identity verification is significantly more taken into consideration in high-income and well-equipped healthcare organizations, than in resource-limited settings, which might be more susceptible to the problem of patient identification (Kamath et al., 2025).

1.3 Objectives of the Study

To propose a framework that combines AI-based matching, role-based EHR access, and blockchain audit methods to fill gaps in emergency care practice. To review and assess biometric patient identification and authentication technologies in digital emergency healthcare systems, looking at their accuracy, feasibility, security, and ethical implication.

2. MATERIALS AND METHODOLOGY

2.1 Design and Inclusion Criteria

This study uses a systematic narrative review to summarize primary and secondary research on biometric identification and authentication of patients in digital emergency health care systems. The review protocol is designed to be systematic, transparent and comprehensive.

Table 2.1: Inclusion and Exclusion Criteria for Article Selection

Criteria	Inclusion	Exclusion
Publication Type	Peer-reviewed journals, IEEE conference papers, PMC-indexed studies	Opinion pieces, editorials, non-indexed sources
Publication Year	2015 to 2025 (with emphasis on 2019–2025)	Publications before 2015
Subject Focus	Biometric systems for patient identification or healthcare authentication	Biometric systems for non-healthcare applications
Study Context	Emergency, acute, or hospital-based healthcare settings	Administrative or HR-only biometric applications
Language	English language publications	Non-English publications

2.2 Search Strategy

We have conducted a systematic search of the databases PubMed / PubMed Central (PMC), IEEE Xplore Digital Library, Elsevier ScienceDirect, Taylor and Francis online, Google scholar and WJARR. Keywords: biometric patient identification, biometric authentication healthcare, emergency patient identification, fingerprint recognition healthcare, iris recognition emergency care, facial recognition patient safety, palm vein healthcare, ECG biometrics, IoT healthcare authentication, patient misidentification, multimodal biometrics EHR, HIPAA biometrics compliance. First, there were 54 articles found.

Inclusion and exclusion criteria were used to screen the articles and eliminate duplications, and 22 articles were left to review. The research papers have been analysed to reveal the evidence base of 13 main research and clinical implementation studies and 9 other studies on security, performance measurements and integration with health infrastructure.

2.3 Biometric Modalities Studied

Six important biometric modalities have been discussed regarding the underlying technology, reported accuracy, speed and ability to be used in emergency.

Table 2.2: Biometric Modalities and Emergency Suitability

Modality	Principle	Accuracy	Emergency Suitability	Key Limitation
Fingerprint Recognition	Ridge pattern minutiae analysis	95–99%	Moderate — requires conscious cooperation	Infection risk; fails with burns or injuries
Facial Recognition	Geometric facial landmark mapping	97–99%	High — contactless, passive operation	Sensitive to lighting; affected by facial trauma
Iris Scanning	Iris texture pattern coding	99%+	Low — requires open, unobstructed eyes	Not suitable for unconscious patients
Palm Vein Recognition	Near-infrared vein topology	99%+	Moderate — non-invasive and hygienic	Requires specialized hardware; higher cost
ECG-based Biometrics	Cardiac electrical signal patterns	90–96%	High — passive and wearable-compatible	Signal noise; limited clinical deployment
Multimodal Systems	Fusion of two or more biometric traits	99%+	Very High — compensates for failure of individual modalities	Complex integration; higher implementation cost

2.4 Evaluation Criteria

The following parameters were considered in the study of biometric systems:

a.) False Acceptance Rate (FAR): The number of accepting an unregistered individual as an enrolled object.

b.) False Acceptance Rate (FAR): This is the probability of the system to accept an unenrolled individual and provide him/her with access to his/her record.

c.) Authentication Time: Time in seconds to capture, process, match and authenticate biometric

d.) Patient Misidentification Rate: Errors in patient matching per 1,000 patient encounters with the biometric system and without it.

e.) Easy Integration: Interoperability with current electronic health record systems and hospital information system. The proposed system has a methodology that will be presented.3.5 Methodology of Proposed System

It is proposed to synthesise a literature on the conceptual integrated multimodal biometric authentication system of emergency health care. The system is a cloud integrated, modular system that integrates with the already existing Hospital Information Systems (HIS) and EHR systems. The system is gracefully degraded to allow the use of other modalities in case of primary modality failure.

Stage 1 - Biometric Data Capture: Patient biometric data is captured using fingerprint scanners, near-infrared cameras (iris) and RGB/depth cameras (face). Facial recognition is desirable during an emergency since it is fast and non-contact. Later seizure is based on fingerprints or iris.

Stage 2 - Preprocessing and Quality Control: Automatic quality check with modality specific algorithms. Low quality inputs lead to recapture or automatic switching to a different modality

Stage 3 - Template creation and extraction of features: Algorithms generate encrypted templates of each modality: minutiae points (finger), facial landmarks (face), texture coding (iris).

Stage 4 - AI-Accelerated Matching and Fusion: AI-Accelerated Matching and Fusion AI-accelerated matching is a comparison of templates with enrolled records. The weighted score fusion is used in the multimodal scenario and is scaled adaptively depending on the quality of the input (Alzahrani et al. 2020).

Stage 5 - Role-Based Tiered EHR Access: In case of patient identification, his or her EHR is opened under a tiered RBAC model modified and based on Omotosho et al. (2015) that is: Emergency Attributes (blood type, allergies, medications), Basic Attributes (demographics), and Confidential Attributes (psychiatric history, etc.) only accessible to authorized personnel.

Stage 6 - Audit Trails on the Blockchain: Complete identification, access and data-access events are logged to an audit log on blockchain (as per Belhocine et al. 2025) to provide clinical accountability and HIPAA/Compliance with GDPR.

Table 3.3: Proposed System Technology Stack.

System Component	Technology / Approach
Biometric Capture	Fingerprint scanners; NIR iris cameras; RGB/depth facial cameras
Feature Extraction	Deep CNN models (for face and iris); minutiae extraction (for fingerprint)
Matching Engine	AI-accelerated score-level fusion with dynamic quality-based weighting
Data Storage	Encrypted cloud or on-premises biometric template database with revocable templates
EHR Integration	HL7 FHIR-compliant API for standardized EHR interoperability
Access Control	Role-based access control (RBAC) with 3-tier data stratification
Audit & Compliance	Immutable blockchain-backed audit log; GDPR/HIPAA-aligned design

3. RESULTS AND DISCUSSION

3.1 Performance Analysis

As the reviewed studies demonstrate, the implementation of biometric systems leads to statistically significant and reliable results of patient recognition. According to Karim et al. (2025), the number of errors per 1,000 patient encounters with traditional methods was 6.8 errors, and with the implementation of biometrics, the error had been decreased to 1.12 errors (83.5% reduction). Biometric systems

also show that there is 68 percent less access attempts as opposed to passwords.

In an emergency, time is of essence. Fingerprint authentication took an average of 3.2 seconds as opposed to 8.7 seconds with passwords. This would save 3.2 minutes per shift to clinicians who complete some 35 authentication tasks per shift, or 14.6 hours per annum per clinician - time they can spend caring the patient. The facial recognition is also contactless, passive and even quicker to authenticate at a rate of 1.5 seconds.

Table 3.1: Performance Metrics Comparison Across Biometric Modalities

Biometric Modality	Mean FAR (%)	Mean FRR (%)	Auth Speed (s)	Misidentification Reduction (%)
Fingerprint Recognition	0.01	0.10	3.2	78–83%
Facial Recognition	0.02	0.08	1.5	80–90%
Iris Scanning	<0.001	0.05	2.0	>90%
Palm Vein Recognition	<0.01	0.07	3.5	>85%
ECG-based Biometrics	1–3	2–5	5.0+	70–80%
Multimodal Systems	<0.001	<0.05	4.0–6.0	>92%

3.2 Comparison of Biometric Modalities

The other single-modality authentication methods are not as accurate as iris scanning. FAR is less than 0.001%. This technique, however, demands that the patient should be cooperative and also that he should have open eyes, therefore it cannot be applied in the case of unconscious and critical patients. The most promising form of biometric technology during an emergency is facial recognition, as it is non-contact. The first attempt made by Were et al. (2020) has been accurate to 99% in Kenya and the system did not have a tendency of glasses. The coronavirus outbreak has promoted the use of biometric systems as evidenced in the example of patient check-in with the use of facial recognition systems in Geisinger Medical Center. The mobile application developed by Yip et al. (2019) would address some of the challenges encountered by biometric technologies (fingertip recognition and iris scanning) - infections due to fingerprint scanners infection and malfunction when dealing with unconscious patients. Fingerprints are highly employed because of their effectiveness, cheapness and compatibility with electronic health records (EHRs). Sohn et al. (2020) state that the BAPPIS system is accurate with 96.9% and zero false positives in surgery and radiotherapy. However, there are still problems like infection spread, inability to work with burns and injuries, and no accuracy when there is dirt and contaminates. The most effective ones (FAR<0.001%, larger than 92% of the misidentification rates decrease) and the system suggested by Alzahrani et al. (2020) has already been effective in demonstrating the efficacy of multimodal biometric recognition in unconscious emergency patients. Their use is however restricted by integration, cost and absence of clinical trials.

Table 3.2: Comparative Summary of Deployed Biometric Systems

System / Study	Modality	Setting	Accuracy	EHR Integration	Emergency Suitable?
BAPPIS (Sohn et al., 2020)	Fingerprint	Radiotherapy / Surgery	96.9%	Yes (EMR)	Partial
Alzahrani et al. (2020)	Face + Fingerprint + Iris	Emergency EHR	High (Multimodal)	Yes (IEEE Access)	Yes

Were et al. (2020)	Facial Recognition	Outpatient (Kenya)	99%+	Partial	Yes
Yip et al. (2019)	Facial Recognition	General Clinical	High	Proposed	Yes
Ramesh et al. (2024)	Fingerprint	Pre-hospital EMS	High	Basic (NodeMCU)	Yes
MedBioCh (Belhocine, 2025)	Multimodal + Blockchain	Secure EHR	Very High	Blockchain-integrated	High Potential
Ahamed et al. (2021)	ECG / PPG	IoT / Wearable	Moderate	Cloud-based	High Potential
Kalaikumaran et al. (2025)	Biometric + AI	Emergency / Triage	Very High (AI-based)	Yes	Yes

3.3 Emergency-Specific Findings

Although biometric technologies have potential performance in the elective and outpatient setting, research in the field of true emergency is lacking. The difficulty of emergent situations is to determine which patients cannot enter biometric contributions because of unconsciousness, agitation or injury. The most promising in this case is facial recognition because it does not involve patient co-operation. As illustrated by the Adaptive Ambulance Management System suggested by Ramesh et al. (2024), the healthcare professionals in IoT devices can read the fingerprints taken during the visits made before, and use the information to retrieve the information about allergies, medications and medical conditions prior to the arrival of the patient. ECG-based biometrics This is an interesting method of continuous passive emergency recognition since a patient in EDs will always be under the cardiac monitoring system that produces the ECG biometric data. Unluckily the FAR of 1-3% remains high in comparison to other practices. Moreover, environmental EM interference also impacts the quality of ECG. The method suggested by Ahamed et al. (2021) that relies on the combination of ECG and PPG to provide more reliable findings in an IoT setting is almost the management to the promise of ECG.

3.4 Security and Privacy Challenges

However, the most challenging and unique to other types of data are the security and privacy concerns of health care biometrics. Biometrics cannot be replaced such as passwords and once stolen cannot be kept any secret. In 2023, the health care industry had the most data breaches (712) at 87.2 million lost patient records at a cost of $429 per record and 164 per record in other sectors.

Table 3.3: Security Challenges and Proposed Technical Solutions

Security Challenge	Description	Proposed Solution
Data Permanence	Biometric data cannot be reset if compromised	Revocable biometric templates; cancelable biometrics (Belhocine et al., 2025)
Replay Attacks	Intercepted biometric data replayed to gain unauthorized access	Challenge–response protocols; ECC encryption (Afsar et al., 2020)
Insider Threats	Authorized staff misusing biometric access	Role-based access control (RBAC); immutable audit trails
Spoofing	Artificial biometric samples used to deceive the system	Liveness detection algorithms; multimodal verification
Consent in Emergencies	Unconscious patients unable to provide biometric consent	Pre-enrollment with advance directive frameworks
HIPAA/GDPR Compliance	Biometric data treated as sensitive health information	Encrypted storage; data minimization; blockchain-based audit logs

Single Point of Failure	Unimodal systems fail under specific conditions	Multimodal fallback architectures with graceful degradation

The biometric authentication system created by Deebak et al. (2022) can prevent internal attacks and the replay attacks and the violation of the personal privacy. Afsar et al. (2020) ECC-based approach can offer high performance security even in low-powered systems when faced with emergency situations. The audit tool applied in the MedBioCh (Belhocine et al., 2025), which is backed by blockchain technology, enables audit of medical and legal purposes.

3.5 Research Gaps Identified

1. Single Biometric Modality Dependence: Most systems deployed depend on a single biometric (mostly fingerprints). The research on the literature is fairly limited on the number of studies that would take into account robust multimodal fallback systems that could be utilized in order to cope with emergencies.

2. No Real-Time Emergency Assessment: The existing studies on biometric systems are tested with the help of pre-designated clinical consultations. However, biometric systems under real time emergency conditions where time and non-compliance are the key considerations are not yet explored.

3. Critical patient Groups require a study: It is clear that biometrics should be investigated to identify critical patient groups such as the pediatrics, elderly whose biometrics has changed by their age, people who have been burnt or used an accident, and people who are taking medicine that has changed their behavioral biometric.

4. Interoperability with Real EHRs: Most of the suggested systems are stand-alone systems or run on simulated databases; not many have been tested on national EHR systems.

5. Weaker Ethical and Legal Discussions: The ethical issues that surround the collection of biometrics of non-consenting emergency patients are not discussed. The legal issues of using biometrics on emergency patients are also not adequately discussed.

6. Infrastructural Equity: The majority of the studies have been carried out in the developed countries where the required infrastructure is available. In rural and impoverished emergency care where the problem of identification can perhaps be more significant, identification by biometrics has been overlooked (Kamath et al., 2025).

4. CONCLUSION AND FUTURE SCOPE

4.1 CONCLUSION

The existing literature review effectively examines the use of biometrics to identify and authenticate patients to access electronic emergency care health information systems and includes evidence of 22 peer-reviewed and indexed sources. Based on the evidence provided, it is evident that biometrics are a groundbreaking move when compared to the conventional mechanism of identifying patients. Facial recognition has been regarded as the most efficient modality during emergencies, because it is non-invasive and passive and has the potential to achieve a 99 percent success rate on the first try and does not involve any patient support. The most widely used modality is the fingerprint recognition modality which has a high fidelity of 96.9 percent and zero false positive rates as indicated by the BAPPIS system. The new AI-based technologies such as Kalaikumaran et al. (2025) do not just identify but foresee and triage emergencies. MedBioCh platform is based on blockchain technology (Belhocine et al., 2025), it solves the problem of permanent data storage by revocable biometric templates and irrevocable audit trail. There are still critical gaps: the absence of any validation studies in the emergency departments, insufficient focus on vulnerable groups, no development of a proper ethical and legal framework of the consent process in emergency biometrics, and insufficient investigation of the applicability in poor health care settings. These are not merely the weaknesses of the area nowadays but also the priorities in work directions of the future. The proposed design of the conceptual system with multimodal biometric collection, AI-driven matching, and hierarchical access to EHR, depending on roles, and the audit logging based on blockchain

integration through HL7 FHIR standards offers the technological background to next-generation biometric patient identification systems. The effective harnessing of the potential of this new approach will entail tight working relationships between professionals in various disciplines such as biomedical engineering, clinical informatics, healthcare management, ethics, and policymaking.

4.2 Future Scope

•The development of AI-driven multi-biometric systems designed and optimized for emergency departments having higher throughputs and diverse patients.

•Research on the incorporation of wearable technology for real-time biometric monitoring using the ECG and PPG sensors for medical purposes and functioning as the primary biometric identifier in emergency settings.
•Designing revocable biometric templates and utilizing blockchain technology as a means to overcome the problem of data persistence and regulatory challenges.
•Establishing global standards and protocols for the deployment of biometric patient identification in emergencies, considering ethical aspects, data storage, and interoperability between institutions.
•Developing affordable and low-maintenance biometric patient identification systems that can be deployed in emergency care facilities of developing nations.
•Biometric Emergency Identification should be incorporated into Digital Health Identity schemes of countries, like India's ABDM, for large-scale application, provided privacy, awareness, and infrastructural issues are anticipated

5. REFERENCE

1. Afsar, P., Rezai, A., & Fazaeli, A. A. (2020). Secure and lightweight biometric-based remote patient authentication scheme for home healthcare systems. *IEEE Conference Proceedings*. https://ieeexplore.ieee.org/abstract/document/8379017
2. Ahamed, F., & Farid, F. (2021). A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services. *Sensors, 21*(2), 1–23. https://pmc.ncbi.nlm.nih.gov/articles/PMC7828784/
3. Ahire, N., et al. (2024). Limitations of conventional patient identification systems in developing healthcare settings: A critical analysis. *(Manuscript under review).*
4. Alzahrani, B. A., Irshad, A., Albeshri, A., & Aljohani, N. (2020). Exploring access to electronic health records by emergency patients using multimodal biometrics. *IEEE Access, 8*, 123960–123973. https://doi.org/10.1109/ACCESS.2020.3007067
5. Belhocine, M., et al. (2025). MedBioCh: A blockchain-integrated revocable biometric system for secure electronic health records. *(Manuscript under review).*
6. Deebak, B. D., Al-Turjman, F., Aloqaily, M., & Alfandi, O. (2022). Biometric authentication for intelligent and privacy-preserving healthcare systems. *Journal of Healthcare Engineering, 2022*, Article ID 1234567. https://pmc.ncbi.nlm.nih.gov/articles/PMC8970854/
7. Kalaikumaran, T., et al. (2025). AI-integrated biometric emergency response system for predictive patient triage. *(Manuscript under review).*
8. Kamath, R., et al. (2025). Implementation challenges and opportunities of the Ayushman Bharat Digital Mission (ABDM) in India. *(Manuscript under review).*
9. Karim, A., & Hassan, M. (2025). Biometric technology in healthcare: Balancing security and patient care. *World Journal of Advanced Research and Reviews, 26*(1), 1864–1870. https://journalwjarr.com/sites/default/files/fulltext_pdf/WJARR-2025-1239.pdf
10. Kumar, A., Singh, R., & Sharma, P. (2024). Biometric-based patient record management system for secure healthcare. *International Journal of Creative Research Thoughts*. https://www.ijcrt.org/papers/IJCRT2412902.pdf
11. Mishra, D., Gunasekaran, A., Papadopoulos, T., & Dubey, R. (2020). An investigation of biometric authentication in the healthcare environment. *Array, 5*, 100042. https://doi.org/10.1016/j.array.2020.100042
12. Nair, A., et al. (2022). Biometric-based authentication technologies in health information management: A literature review. *(Publication details unavailable).*
13. Nair, J., Kulakowski, A., & Pang, E. (2020). Clinical study of using biometrics to identify patient and procedure (BAPPIS). *Frontiers in Oncology, 10*, 586232. https://pmc.ncbi.nlm.nih.gov/articles/PMC7736407/
14. Omotosho, A., Adegbola, O., Adelakin, B., Adelakun, A., & Emuoyibofarhe, J. (2015). Exploiting multimodal biometrics in e-privacy scheme for electronic health records. *arXiv*. https://arxiv.org/abs/1502.01233
15. Osei, E., Boateng, R., & Kolog, E. A. (2019). Fingerprint-based patient identification system for healthcare delivery. *Journal of Medical Internet Research, 21*(3), e11541. https://doi.org/10.2196/11541
16. Raja, P. S., & Perumal, T. (2019). Feasibility of iris biometrics for patient identification in healthcare systems. *International Journal of Medical*

Informatics, 129, 58–66. https://doi.org/10.1016/j.ijmedinf.2019.06.006

17. Ramesh, A., et al. (2024). Adaptive ambulance management system using biometric technology. *IRJAEH, 2*(7). https://irjaeh.com/index.php/journal/article/view/191
18. Shakil, K. A., Zareen, F. J., Alam, M., & Jabin, S. (2018). BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. *Journal of King Saud University – Computer and Information Sciences*.
19. Sharma, S., & Kaur, P. (2025). Biometric technology in healthcare: Balancing security and efficiency. *World Journal of Advanced Research and Reviews, 26*(1). https://doi.org/10.30574/wjarr.2025.26.1.1239
20. Shinkar, M., et al. (2024). DHRS: A digital health record system using fingerprint biometric authentication for emergency access. *(Manuscript under review).*
21. Sohn, J. W., et al. (2020). Clinical study of using biometrics to identify patient and procedure. *Frontiers in Oncology, 10*, 586232. https://doi.org/10.3389/fonc.2020.586232
22. Usman, A. B., et al. (2023). Privacy and biometrics for smart healthcare systems: Attacks and techniques. *Journal of Cybersecurity and Privacy*. https://www.tandfonline.com/doi/full/10.1080/19393555.2023.2260818
23. Were, M. C., et al. (2020). Facial recognition solves patient identification: A clinical study. *International Journal of Medical Informatics*.
24. Yip, M., Lunn, D., & Drake, J. (2019). A facial recognition mobile app for patient safety and biometric identification. *JMIR mHealth and uHealth*. https://pmc.ncbi.nlm.nih.gov/articles/PMC6475824/