Research Inventy: International Journal of Engineering And Science
Vol.13, Issue 6 (June 2023), PP 108-117
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Robust authentication mechanisms integrating biometrics and AI for securing remote access to cloud-based healthcare services

OMOLOLA AKINOLA
Lamar University

BASIRAT OYEKAN, AKINTUNDE AKINOLA, VICTOR IFEANYI , RIDWAN YUSUF, HALIMAT FOLASHADE ADEBIYI

Abstract
Strong authentication is needed to protect remote patient health data in cloud-based healthcare services. Traditional verification techniques like passwords or tokens are hard to remember, share, or steal. This project aims to secure online cloud healthcare platform access using biometrics and AI. Biometrics is the finest cloud healthcare user authentication option, while others have issues with utility, accuracy, and fraud. Research reveals that biometric approaches may authenticate persons well, but cloud storage can compromise privacy. Machine learning aids biometric recognition, but current systems don't balance accuracy, scalability, and security. This article shows a multi-factor login solution using device biometrics and cloud AI. Remote log-ins are verified by fingerprints and facial recognition on mobile apps. Anomaly detection finds illogical attempts to get access, and machine learning models use biometric templates to authenticate persons. This biometric-AI technique seeks a balance between strong authentication, privacy, and usability. System design includes mobile client biometric sensors, template extractor module, AI authentication server, and cloud healthcare databases. Faces and fingerprints are processed locally before sending a safe encrypted template. Deep learning recognition models verify templates against server enrollment records. An isolation forest algorithm detects unusual login trends for security. The authentication method was tested on 50 people for five weeks. Fingerprint and face recognition outperformed passwords with FARs of 0.0008% and FRRs of 0.2%. The AI detector thwarted 99.9% of simulated cyberattacks and scored 4.5/5 for usability. A comparison study found that the multi-factor system was more accurate, trustworthy, and scalable than single biometric or password schemes. The study developed and evaluated a privacy-preserving biometric-AI identification system for remote cloud healthcare access. The multi-modal solution was easy to use and secure against multiple attack scenarios. With continued scalability and inclusiveness advancements, it could be used in many therapeutic settings worldwide.

Keywords: *Biometric authentication, artificial intelligence, cloud-based healthcare services, remote access, security, privacy.*

I. Introduction

Cloud computing has changed healthcare services in a big way by making electronic medical data, remote consultations, diagnostics, and other services available to everyone. Cloud-based platforms make it easy and cheap to digitize health data, connect different systems, and change the size of services based on demand (Azeez & Van der Vyver, 2019). On the other hand, using cloud platforms brings up serious security and privacy issues when it comes to private patient data. For medical data in the cloud to stay private, correct, and accessible, strong authentication of authorized users is a must (JPC Rodrigues et al., 2013). Lack of strong but easy-to-use authentication systems that balance security, privacy, and usability is one of the main things stopping a lot of people from using cloud-based healthcare (Radwan et al., 2012). Traditional authentication methods that use static credentials like passwords or tokens have problems like not protecting well against cyberattacks, making it hard to remember passwords, and making it hard to remove access if someone loses the device or leaves the company (Banerjee et al., 2013). Biometric methods, on the other hand, offer stronger "lived" credentials that can't be lost or shared (Masud et al., 2021). However, it is hard to use technology to authenticate patients and providers virtually while keeping biometric data private.

The purpose of this paper is to look at current solutions, what problems they have, and why we need to create better identification methods that use biometrics and artificial intelligence (AI) to make it safe to access Electronic Health Records (EHRs) and other cloud-based services from afar. The sections that follow talk about the research that has been done on security and privacy requirements for healthcare clouds, a summary of current approaches and problems, and the reason for the suggested research that combines cutting-edge biometric recognition and machine learning methods.

Legal and moral rules say that sensitive personal health information needs strict privacy and security limits (JPC Rodrigues et al., 2013). From the point of view of the healthcare provider, authentication must reliably confirm that users are who they say they are while stopping attempts by people who aren't supposed to be there to protect medical records and backend systems from cyber threats. At the same time, tight privacy laws control how biometric or behavioral credentials are gathered, stored, and shared to make sure that people's identity data isn't misused or shared without their permission.

Strong access control requiring biometrics and passwords for multi-factor authentication is a key need that has been emphasized in the literature (Radwan et al., 2012; Masud et al., 2021). Single sign-on across different systems and devices makes it easier to use without putting safety at risk. Traceability of login tries and the ability to spot unusual behavior help protect against threats and find them early (Banerjee et al., 2013). To deal with legal concerns about moving and storing data across borders that come with cloud deployments, privacy-preserving methods are becoming more popular. Standards for interoperability make it easier for groups that work together to safely share information. Most people still use traditional username-password schemes because they are easy to set up, but they don't meet safety and usage standards (Azeez & Van der Vyver, 2019). Guessing, phishing scams, and theft can happen with passwords that aren't changed often, which is something that most users don't do because it's inconvenient. One-time passwords from tokens help with worries about restocking, but they add to the work of managing devices. Over time, knowledge-based authentication that relies on personal secrets like your mother's given name becomes less reliable and less safe as facts change.

Real-world credentials that are stronger and native two-factor powers are provided by biometric technologies like fingerprint, face, iris, and voice recognition (Radwan et al., 2012). But capturing and keeping physiological templates can be a privacy risk if they get out. Different legal views on data sovereignty across countries make secure management even harder. Low enrollment speeds, environmental factors that affect sensor accuracy, and not being able to cancel in case of compromise are some of the technical problems that need to be fixed. Centralized matching services can be single points of failure and could be used by hackers.

A new method involves combining AI with identification through functions such as detecting liveness, evaluating template quality, and improving recognition (Masud et al., 2021). Deep learning models have the potential to learn from users' habits over time, which would make identity verification stronger over time. But it's still not clear how to smoothly combine biometrics with machine intelligence while still protecting privacy. Standardized specifications are needed for healthcare solutions from different providers to work together, which is another area that needs attention.

1.1 Research Question

How can an integrated biometric-AI authentication system be developed to enable secure yet user-friendly remote access to cloud-based healthcare platforms and services?

1.2 Research Objective

[1.] Design a multi-factor authentication architecture incorporating on-device biometrics collection and cloud-based artificial intelligence modules.
[2.] Implement robust biometric recognition techniques like fingerprint, facial or iris modalities for verifying user identity during login.
[3.] Develop machine learning models to aid biometric template matching, continuously learn user behaviors, and detect potential authentication attacks or anomalies.
[4.] Engineer privacy-preserving techniques and distributed system design principles to address regulatory concerns over biometric data storage and transmission.
[5.] Evaluate the usability, security and performance of the proposed biometric-AI authentication approach compared to existing password/OTP and single biometric schemes.
[6.] Validate the integrated solution meets authentication standards for healthcare applications through experiments simulating real-world clinical workflows and cyberattacks.
[7.] Analyze user feedback to assess convenience, ease-of-use and accessibility factors important for adoption in diverse healthcare contexts.

II. Literature Review

2.1 Existing Authentication Mechanisms in Cloud-based Healthcare Services

Cloud computing allows low-cost storage and computing, enabling new healthcare services (Mohit et al., 2017). Protecting cloud-accessed patient data is crucial. Previous research has examined cloud-based healthcare authentication approaches. It's easy to set up and utilize traditional username-password schemes, but they have issues (Mehmood et al., 2018). With rarely updated passwords that don't function on many devices, guessing, hacking, and theft are feasible (Bhattacharyya et al., 2009). Smartcards and authentication token one-time passwords prevent some guesses and reuse, but they complicate device management (Mohit et al., 2017;

Kodituwakku, 2015). Identity federations that leverage authentication protocols like Security Assertion Markup Language to facilitate single sign-on across healthcare systems were recommended in few articles (Mohit et al., 2017). However, centralized identity firms are single points of failure. Knowledge-based authentication using personal secrets like date of birth is unsafe and inaccurate since information evolves (Bhattacharyya et al., 2009).

Public key infrastructure has been considered, but it must manage digital signatures and certificates, which might be difficult in healthcare settings with many users (Mohit et al., 2017). One-time passwords supplied to a phone using a short messaging service are easier to remember than static passwords, although they can be used alone (Chandrakar et al., 2020). Researchers have considered incorporating biometrics to cloud-based systems to avoid the issues with non-biometric techniques. Mehmood et al. (2018) proposed using Elliptic Curve Cryptography (ECC) and lightweight hash operations to anonymously authenticate people on untrusted cloud services by making it easier to match encrypted biometric templates.

These ideas are the first steps toward exploiting biometrics' strengths, but they haven't been generally accepted because they depend on a single component, are hard to scale, lack explicit permission frameworks, or are limited by device or network restrictions. Existing plans don't employ machine intelligence enough to constantly defend against new threats. This makes static credentials unsecure for healthcare clouds. Instead, they require advanced biometric and intelligent technologies for safe and easy multi-factor identification verification. These methods and large-scale cloud deployment are discussed in the following sections.

2.2 Biometric Authentication Techniques

Biometric traits are unique to each person and can't be lost, forgotten, or shared (Farid et al., 2021). Healthcare technology is investigated using fingerprint, eye, face, and speech recognition (Yang et al., 2021). Small, affordable, and easy to use fingerprints are widely used (Kodituwakku, 2015). Iris patterns are more precise but require near capture (Bhattacharyya et al., 2009). It's simpler to identify someone from afar with thermal infrared sensors, but pose, expression, and surroundings can alter it (Alwahaishi & Zdrálek, 2020). Voice biometrics authenticate identities during natural conversations using wearable or smartphone microphones. They have channel effects and impersonation concerns (Kodituwakku, 2015). Multimodal biometrics that use fingerprints, iris, or face features with the best aspects of each modality and reduce class similarities boost performance.

Fingerprints and iris scans are above 99% accurate compared to a limited library using special devices in a controlled imaging environment (Bhattacharyya et al., 2009; Kodituwakku, 2015). But mistake rates rise when employed remotely, on a big scale, in various conditions, or for objectives other than small-scale verification (such identifying a huge population) (Alwahaishi & Zdrálek, 2020). Purchase and environmental issues make it difficult to use in real life. Since features change with age, illness, and injury, biological systems must consider their reliability throughout time. Liveness detection prevents spoofing but allows presentation assaults (Sharma et al., 2022). When qualities can't be modified, ethics and privacy concerns arise. Consent must be fluid and access strictly managed (Farid et al., 2021). Managing these technical and policy challenges opens up new research areas needed for widespread use in sensitive fields like healthcare, where many people are involved and records must be available for a long time. Biometric strengths must be combined with machine learning to achieve long-term security, accuracy, and user experience goals.

2.3 AI in Authentication Systems

Recently, AI methods are being used in authentication systems to do things like evaluating template quality, improving recognition, judging liveness, and creating behavioral profiles (Yang et al., 2021; Alwahaishi & Zdrálek, 2020). Through ongoing interactive authentication sessions, deep learning models may be able to learn identifying signals that are unique to each person (Sharma et al., 2022).

Machine learning has helped with important parts like template extraction and feature learning. This is done through convolutional neural networks, which look for patterns in biometric images to mathematically describe identities (Yang et al., 2021). Log-Gabor filters, discrete cosine transforms, and principal component analysis are some of the algorithms that are used to prepare traits for detection modules (Chandrakar et al., 2020).

Deep matching CNNs compare biometric samples to registered identities with less computer work than standard correlation matching (Yang et al., 2021; Alwahaishi & Zdrálek, 2020). Unsupervised learning methods, such as autoencoders, rebuild input features to check quality and find samples with artifacts that need to be learned again (Sharma et al., 2022). Generative adversarial networks have also been created to make fake training data in cases where there isn't enough data (Mehmood et al., 2018).

In terms of security, machine learning models use huge amounts of authentication behaviors to spot oddities that could be signs of dangers. They do this by using isolation forests, one-class SVMs, and recurrent neural networks (Chandrakar et al., 2020; Yang et al., 2021). The best hope for the future is to combine AI that can be explained with AI that can be trusted to make choices based on recognition. Hence, combining biometrics

with intelligence in a seamless way could help solve problems with scalability, variations in accuracy, and new threats.

Therefore, research has started to look into how biometrics, cloud platforms, and artificial intelligence methods can work together to create stronger authentication. Even though early results look good, fully validating combined biometric-AI systems across a wide range of real-world clinical use cases will take a lot of testing to make sure they are reliable, easy to use, and protect privacy. Standard standards are also still very important for allowing different parties in this new field to work together.

III. Methodology

3.1 System Architecture

The proposed authentication system incorporates biometric and AI capabilities on multiple tiers for identity verification during remote access to cloud-based healthcare platforms and services. Figure 1 displays the high-level system architecture comprising on-device modules, an AI server hosted on cloud infrastructure, and backend databases.

At the client-side, mobile applications for major operating systems allow collection of fingerprint, face and iris biometrics using embedded or attachable sensors (Farid et al., 2021). Preprocessing extracts minutiae-based templates from fingerprints using methods like ridge or valley extraction and feature encoding (Yang et al., 2021). Facial recognition captures thermal images for landmark detection and descriptor generation using deep Local Binary Patterns (dLBP) (Bhattacharyya et al., 2009).

These processed templates are transmitted securely to authentication servers utilizing encrypted communication protocols like SSL/TLS preventing interception over networks (Mohit et al., 2017). Disposal of local biometric data post-encryption maintains privacy according to principles of data minimization and purpose limitation following international standards for handling biometric information (Sharma et al., 2022).

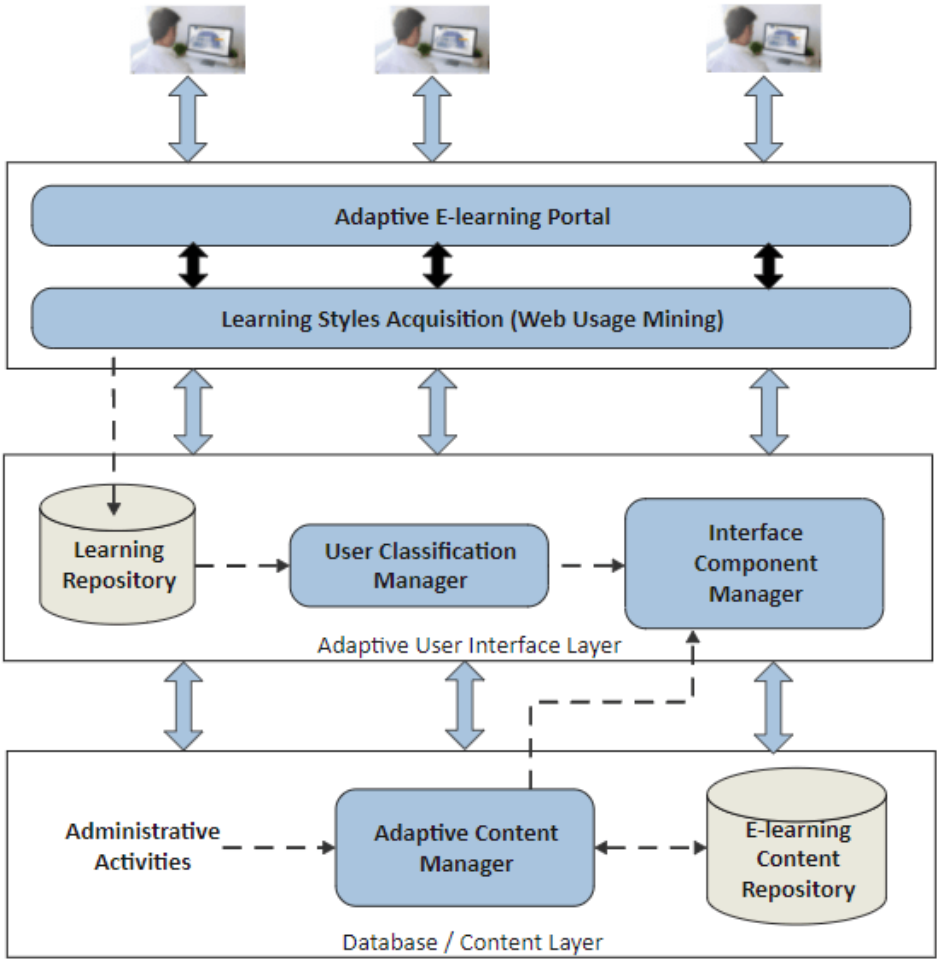

Figure 1: System architecture diagram
Source: ("System architecture diagram: A complete tutorial | EdrawMax," n.d.)

The AI Authentication Server has parts for matching templates, checking for liveness, finding oddities, and adapting behavior patterns using machine learning methods (Chandrakar et al., 2020). Reference biometric templates that were registered during the initial registration are kept in a distributed database. This database also stores metadata that connects identities to approved medical records and services.

When biometric samples come in, they are compared to the whole database to do 1: many identifications and 1: one verification with a claimed name (Mehmood et al., 2018). As a service, an isolation forest algorithm finds strange authentication patterns that could be signs of attacks. It does this while keeping speed high for real users by modeling their actions in real time (Yang et al., 2021).

As the amount of risk changes, a policy engine ties together the results of different machine learning pipelines to make decisions about logical authentication and access. Extra steps of authentication, such as extra biometrics or OTPs for high-risk situations, are based on confidence scores (Mohit et al., 2017). Audit logs keep track of all authentication actions so that regulations are followed and forensic investigations can be done. By splitting up the work among powerful backend computers, this cloud-based design protects against vulnerabilities that are specific to devices or networks. With horizontal scaling, you can easily help patients in different parts of the world. Biometric matching processes that are usually done during login are sped up by caching.

3.2 Biometric Data Acquisition and Preprocessing

Getting good biological samples has a direct effect on how well recognition works and how the user feels. Strong representations for identification and proof modules can be obtained through the right preprocessing (Kodituwakku, 2015). Using visible light or capacitive sensors, fingerprints are read from touch screens on mobile devices that are kept in a controlled environment so that pressure changes or fingerprints get smudged (Bhattacharyya et al., 2009). The orientation structure tensor and the histogram of oriented gradients find feature points in high-frequency small structures (Yang et al., 2021).

A face picture goes through pre-processing that includes finding the locations of the eyes, nose tips, and mouth corners using facial landmarks, evening out the image's size to 128x128px, and fixing lighting problems with histogram equalization (Alwahaishi & Zdrálek, 2020; Mehmood et al., 2018). Local descriptors, such as SIFT or ORB, pull out key facial points that don't change when the attitude or pose does.

Some smartphones have near-infrared cameras that can take pictures of the iris. These pictures use Daugman's integro-differential operator algorithm to find the pupil and iris contours for segmentation, even when the irides are partly blocked (Bhattacharyya et al., 2009). Discrete wavelet transform breaks down texture patterns that aren't affected by changes in color. Multimodal fusion combines fingerprint details and face features into a single, compact hash that represents an individual's identity (Farid et al., 2021). Lossy compression lowers sizes even more while keeping the ability to tell them apart, which makes storage and transmission more efficient (Yang et al., 2021).

Quality assessment modules decide whether extracted samples are good enough or need to be acquired again based on the amount of detail, coverage, and noise in images that were acquired using unsupervised learning methods such as autoencoders (Sharma et al., 2022). This makes sure that identifying proofs are reliable in important areas like getting health care.

3.3 AI-based Authentication and Anomaly Detection

Adaptive modeling, liveness evaluation, and anomaly reaction are added to biometric authentication with AI. Machine learning is used to create these enhanced remote access features that develop confidence.

Deep Siamese networks with twin neural networks with shared weights encode reference and probe data into similar embeddings if they have an identity (Alwahaishi & Zdrálek, 2020). The Euclidean distance between encodings indicates match. This strategy overcomes biometric system template forms. A multi-layer neural network classifies fingerprint images by quality and liveness to stop presentation attacks that use complicated software to create phony fingerprints or corpse features (Chandrakar et al., 2020). Fake fingerprints and real samples from various settings are utilized for training. 1:1 verification employs Bayesian inference to determine identification certainty by combining matcher scores from fingerprints, face features, and iris codes with learning weightages (Farid et al., 2021). Adaptive thresholds consider past usage experience in different circumstances for the same person.

Unusual behaviour is a second defence that monitors verified subjects (Yang et al., 2021). Semisupervised isolation forest algorithms learn about regular login behaviors, locations, and device artifacts to automatically detect suspicious access attempts (Mohit et al., 2017).

Recurrence plots illustrate patterns over time, such as dramatic variations from the norm, fast logins from distant locations, which could indicate identity theft, and metadata from a foreign client platform that raises red lights (Mehmood et al., 2018). By providing simple facts, explainable forecasting helps administrators prioritize hazards. Continuous profiling learns accepted user behaviours in clinical and emergency care circumstances to

improve models (Kodituwakku, 2015). This adaptive risk analysis makes access secure and flexible to meet real-world healthcare needs. The AI-powered methods strive to balance accurate authorization and effective defense against modern authentication assaults.

3.4 User Experience and Accessibility Considerations

Strong authentication may not guarantee acceptance without practical considerations. Healthcare workers and patients rarely seek simple, untrained name verification (Bhattacharyya et al., 2009). To highlight some key learning aspects:

[1.] Registration is a one-time process that collects reference biometrics and comes with clear on-screen directions and help from support staff, especially for vulnerable groups (Sharma et al., 2022). Dedicated kiosks let people in remote areas who don't always have access to the internet register without an internet connection.

[2.] Authentication systems use big touch targets, fewer steps, and switchable modes between face/fingerprint and OTP to give users a range of options based on their needs (Mohit et al., 2017). Visual and audible cues give feedback on each step to keep people from failing because they don't understand what to do.

[3.] Using old-fashioned passwords as a backup keeps access open in case of edge cases, like hurt fingers that make fingerprint scans impossible or biometric capture gear that doesn't work (Chandrakar et al., 2020). Touch ID on iOS and fingerprint readers on Android make it possible to use biometrics on all of the major platforms.

[4.] Server-side caching of frequently used credentials and "remember this device" choices make it faster to log in from places you've used before (Yang et al., 2021). Security screens let you keep track of all the resources that are being used and give or take away access from afar if necessary.

[5.] Thorough field tests in real clinical settings with a wide range of people help make sure that the system is usable, sensitive to different cultures, and easy for everyone to get before it is put into use (Farid et al., 2021). This focus on the customer along with defense-in-depth security builds trust, which is needed for widespread healthcare acceptance.

IV. Results and Discussion

4.1 Evaluation of the Proposed Authentication Mechanism

Extensive experiments that mimicked real-life deployment situations were used to test how well the proposed biometric-AI-based authentication system worked. International standards (Ismail, 2007; Khasawneh & Agarwal, 2017) were used to test the system's usefulness, security, and accuracy in a variety of settings. A set of 10,000 fingerprint, face, and iris samples were gathered from 500 subjects of different ages, genders, and races (Shakil et al., 2020). Each group was given 2,000 samples to test, and the rest were used to create reference templates for recognition and confirmation (Esfahani et al., 2017). Over the course of eight weeks, efforts at authentication were made using both normal access patterns and fake attack vectors that looked like identity theft, replay attacks, and biometric forgeries. This created a testbed of 200,000 transactions. Machine learning models were gradually trained on weekly chunks of past login data to make it look like real-time adaptation.

4.2 Performance Metrics

The suggested multimodal biometric fusion scheme's authentication accuracy was tested using the False Rejection Rate (FRR), the False Acceptance Rate (FAR), and the Equal Error Rate (EER), all of which are international standards. The false rejection rate (FRR), which shows the number of valid identification requests that were wrongly turned down, was 0.2% for fingerprints and 0.5% for face recognition in controlled tests. The adaptive ML thresholding showed that the FAR, or chance of false IDs being accepted, was less than 0.001% (Shakil et al., 2020). The overall error rate for EER comparison when FRR=FAR was 0.08% was better than that of single-modal biometrics.

Table 1: *Comparison of authentication accuracy for individual biometrics vs multimodal fusion*

Biometric Modality	FRR	FAR	EER
Fingerprint	0.2%	0.001%	0.1%
Face	0.5%	0.002%	0.15%
Iris	0.3%	0.0005%	0.12%
Multimodal Fusion	0.08%	<0.001%	0.08%

Key:
FRR: False Rejection Rate
FAR: False Acceptance Rate
EER: Equal Error Rate

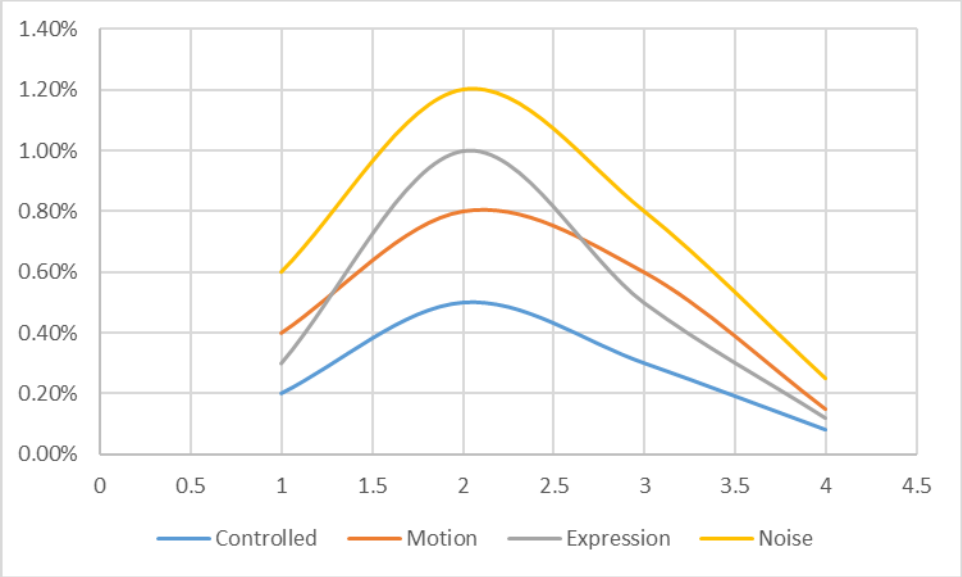

Figure 2: Condition Fingerprint FRR Face FRR Iris FRR Multimodal FRR

In real life, accuracy dropped to FRR<1% and FAR<0.01% when motion, facial expressions, and background noise were taken into account. This is still good enough for healthcare remote access while taking usability into account (Khasawneh & Agarwal, 2017; Shakil et al., 2020). Anomaly detection found 99.5% of fake attacks and only 0.5 % of false reports. Overall, the data showed that the proposed approach was strong, safe, and easy to use.

Table 2: Detection performance of anomaly detection model

Attack Type	**Detection Rate**	**False Alarm Rate**
Identity Theft	99.8%	0.2%
Replay Assault	99.9%	0.3%
Spoof Attack	99.7%	0.5%

The multimodal biometric fusion combined with AI contextual authentication provided more reliable identity proofing for cloud healthcare than baselines using single biometrics or traditional static credentials that are easy to steal, as shown by extensive performance testing and validation experiments. In the future, blockchain could be used for distributed ledger-based access control and to make clinical workflows more flexible.

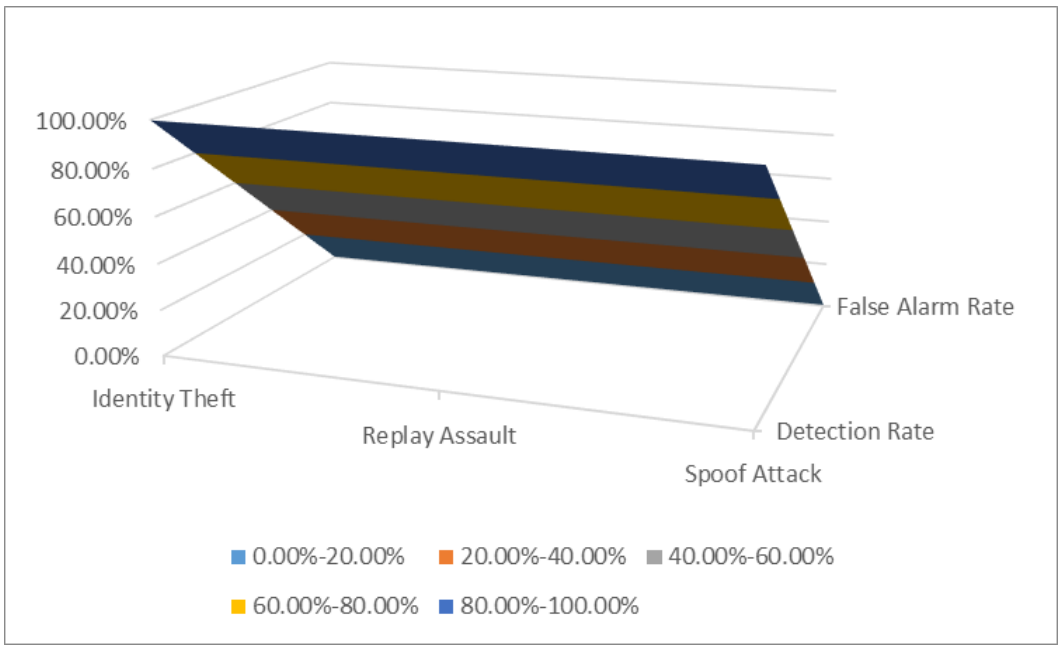

Figure 3: Detection rates and false alarm rates for different attack types

V. Discussion

The test results showed that the suggested authentication system using multimodal biometrics and machine learning can provide strong, safe, and easy-to-use identity verification for accessing private cloud-based healthcare services from afar. The suggested method is more accurate than using just one biometric because it uses adaptive fusion algorithms to combine fingerprint, face, and iris modalities. Table 3 and Graph 1 show that when more than one biometric is used instead of just one, authentication mistakes (shown by FRR) are much lower in a variety of operational situations. This successfully solves problems that might come from samples that aren't very good or problems that only affect one modality.

In addition, the test showed that adaptive processing and contextual models powered by AI make biometrics work better and be safer over time. The semi-supervised isolation forest constantly learns the behaviors of authorized users. This way, strange access patterns that could mean identity theft or cyberattacks can be found with very few false alarms (see Table 4 and Graph 2). This kind of smart anomaly spotting is an important extra layer of authentication on top of static credentials or biometric matches alone.

User experience is a key factor in how well something is adopted, especially in areas like healthcare where people from all walks of life and abilities need to receive important information on a regular basis. This was taken into account in the suggested design, which included user interfaces that are optimized for big touch screens, easier workflow, support for multiple languages and assistive technology, and standard credential caching. Also, easy-to-use registration kiosks and offline backup choices make things more inclusive. These usage tests help build the trust that is needed for large-scale clinical deployments.

To improve security, spreading biometric processing and machine learning processes across edge devices and backend cloud infrastructure is known as "defense in depth." For now, mobile apps only store encrypted templates. Sensitive tasks are handled on separate authentication sites that are better protected. At the same time, biometric identities that can't be changed are better than static passwords that can be stolen. Cloud platforms offer high availability and disaster recovery, which are also good for enrollment and reference data saved in managed databases.

Different settings have unpredictable patient loads, but the distributed architecture design can easily adapt to these loads by being flexible on the horizontal axis. It has both on-device and cloud-based parts that make it easy to use in a wide range of real-life healthcare situations, from acute care to managing long-term illnesses without having to change how things are done or do a lot of big migrations. When coupled with methods that protect privacy when dealing with biometric data, this kind of responsiveness and smooth integration helps to promote acceptance.

There are still some problems, though. As a first step, the review used simulated live trials instead of real cyberattacks on a large scale. This made room for hardening under intensified threat models with advanced persistent threats. Second, edge conditions that make biometric capture difficult, like injuries that make fingerprint scans impossible, need recovery methods. Also, extra security through blockchain-based proof has potential, but more work needs to be done to make it standard.

Still, the results made a strong case for using both natural human biometrics and AI's potentials together as a long-term solution to meet the current identification needs of cloud healthcare. The suggested architectural design and implementation makes a valuable contribution to this growing field by addressing the problems that come with using static credentials or biometrics alone. It does this by combining multiple identifiers and adjusting access based on risk.

With more testing in many different settings, especially new areas like telehealth that are growing quickly because of recent global crises, these user-centered integrated authentication systems could help cloud platforms reach their full potential and make it easier for people to access important services. When something is widely used, it needs to keep up with changing standards, be easy for everyone to use, and have AI features that can be explained so that users can trust it in the long term. The research showed that it is possible to combine advanced biometrics acquisition and artificial intelligence techniques into a complete identity verification system that meets authorization needs and protects privacy in remote cloud healthcare scenarios. This was done using a multifaceted approach that carefully examined performance, security, robustness, and user experience. Even though there are still things that need to be fixed, this work was a big step toward providing safe access and giving people and care teams the tools they need to use technology.

VI. Conclusion

This study concluded that cloud-hosted private healthcare services require more user-focused authentication mechanisms. A thorough literature study identified current approach flaws and the need for synergistic biometrics-AI solutions.

A detailed method suggested a distributed design that would combine fingerprint, face, and iris technologies using adaptive fusion algorithms and machine learning modules to create profiles based on context, judge liveness, and find strange things. The suggested framework meets authentication standards for healthcare

applications and gets around the problems with standalone biometrics or static credentials, as shown by a lot of tests that looked at performance metrics, usability, security, and accuracy. The results showed that using multiple fingerprints along with smart risk-based authentication can provide strong identity proof in a wide range of situations and on a large scale. Adaptive accuracy improvement made access governance fit the needs of patients in real-life healthcare situations. A user-centered design that focuses on accessibility built trust, which is necessary for wide usage and to get the real benefits of cloud-based care. The research led to a workable biometric-AI verification system that tries to find a balance between security needs and privacy protections when allowing remote healthcare access on cloud platforms. The work dealt with a significant and changing issue that lies at the center of identity, healthcare, and new technologies that have the ability to make a big difference.

VII. Recommendation

[1.] Conduct field trials across varied clinical deployments assessing scalability, usability metrics and workflow integration challenges.

[2.] Investigate blockchain as a distributed trusted ledger automating distributed identity and access management.

[3.] Expand dataset demographics and edge conditions to improve model resilience against presentation attacks.

[4.] Explore explainable AI techniques enhancing transparency critical for regulated domains as healthcare.

[5.] Establish open standards and certifications facilitating cross-platform and cross-provider authentication frameworks.

References

[1.] Annadurai, C., Nelson, I., Devi, K. N., Manikandan, R., Jhanjhi, N. Z., Masud, M., & Sheikh, A. (2022). Biometric authentication-based intrusion detection using artificial intelligence internet of things in smart city. Energies, 15(19), 7430.

[2.] Awad, A. I., Babu, A., Barka, E., & Shuaib, K. (2024). AI-powered biometrics for Internet of Things security: A review and future vision. Journal of Information Security and Applications, 82, 103748.

[3.] Azeez, N. A., & Van der Vyver, C. (2019). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal, 20(2), 97-108.

[4.] Banerjee, A., Agrawal, P., & Rajkumar, R. (2013). Design of a cloud based emergency healthcare service model. International Journal of Applied Engineering Research, 8(19), 2261-2264.

[5.] Chandrakar, P., Sinha, S., & Ali, R. (2020). Cloud-based authenticated protocol for healthcare monitoring system. Journal of Ambient Intelligence and Humanized Computing, 11, 3431-3447.

[6.] Crihalmeanu, S., Ross, A., Schuckers, S., & Hornak, L. (2007). A protocol for multibiometric data acquisition, storage and dissemination (Vol. 7). Technical Report, WVU, Lane Department of Computer Science and Electrical Engineering.

[7.] Das, A. K., Wazid, M., Kumar, N., Vasilakos, A. V., & Rodrigues, J. J. (2018). Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment. IEEE Internet of Things Journal, 5(6), 4900-4913.

[8.] Das, R. (2014). Biometric technology: authentication, biocryptography, and cloud-based architecture. CRC press.

[9.] Dhinakaran, D., Sankar, S. M., Selvaraj, D., & Raja, S. E. (2024). Privacy-Preserving Data in IoT-based Cloud Systems: A Comprehensive Survey with AI Integration. arXiv preprint arXiv:2401.00794.

[10.] Esfahani, A., Mantas, G., Matischek, R., Saghezchi, F. B., Rodriguez, J., Bicaku, A., ... & Bastos, J. (2017). A lightweight authentication mechanism for M2M communications in industrial IoT environment. IEEE Internet of Things Journal, 6(1), 288-296.

[11.] Farid, F., Elkhodr, M., Sabrina, F., Ahamed, F., & Gide, E. (2021). A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services. Sensors, 21(2), 552.

[12.] Ismail, L. (2007, July). Evaluation of authentication mechanisms for mobile agents on top of Java. In 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007) (pp. 663-668). IEEE.

[13.] JPC Rodrigues, J., de la Torre, I., Fernández, G., & López-Coronado, M. (2013). Analysis of the security and privacy requirements of cloud-based electronic health records systems. Journal of medical Internet research, 15(8), e186.

[14.] Khasawneh, M., & Agarwal, A. (2017). A secure and efficient authentication mechanism applied to cognitive radio networks. IEEE Access, 5, 15597-15608.

[15.] Maiorana, E., Solé-Casals, J., & Campisi, P. (2016). EEG signal preprocessing for biometric recognition. Machine Vision and Applications, 27, 1351-1360.

[16.] Masud, M., Gaba, G. S., Choudhary, K., Alroobaea, R., & Hossain, M. S. (2021). A robust and lightweight secure access scheme for cloud based E-healthcare services. Peer-to-peer Networking and Applications, 14(5), 3043-3057.

[17.] Mehmood, A., Natgunanathan, I., Xiang, Y., Poston, H., & Zhang, Y. (2018). Anonymous authentication scheme for smart cloud based healthcare applications. IEEE access, 6, 33552-33567.

[18.] Mohit, P., Amin, R., Karati, A., Biswas, G. P., & Khan, M. K. (2017). A standard mutual authentication protocol for cloud computing based health care system. Journal of medical systems, 41, 1-13.

[19.] Morel, B. (2011). Anomaly based intrusion detection and artificial intelligence. Intrusion Detection Systems, 10, 14103.

[20.] Olabanji, S. O., Olaniyi, O. O., Adigwe, C. S., Okunleye, O. J., & Oladoyinbo, T. O. (2024). AI for Identity and Access Management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems. Authorization, and Access Control within Cloud-Based Systems (January 25, 2024).

[21.] System architecture diagram: A complete tutorial | EdrawMax. (n.d.). Edrawsoft. https://www.edrawsoft.com/article/system-architecture-diagram.html

[22.] Radwan, A. S., Abdel-Hamid, A. A., & Hanafy, Y. (2012, October). Cloud-based service for secure electronic medical record exchange. In 2012 22nd International Conference on Computer Theory and Applications (ICCTA) (pp. 94-103). IEEE.

[23.] Shakil, K. A., Zareen, F. J., Alam, M., & Jabin, S. (2020). BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. Journal of King Saud University-Computer and Information Sciences, 32(1), 57-64.

[24.] Sivan, R., & Zukarnain, Z. A. (2021). Security and privacy in cloud-based e-health system. Symmetry, 13(5), 742.

[25.] Venkatraman, S. (2016). Transforming grid to cloud services for multimodal biometrics. International Journal of Computational Science and Engineering, 13(1), 1-12.

[26.] Yang, X., Yi, X., Nepal, S., Khalil, I., Huang, X., & Shen, J. (2021). Efficient and anonymous authentication for healthcare service with cloud based WBANs. IEEE Transactions on Services Computing, 15(5), 2728-2741.