This MICCAI paper is the Open Access version, provided by the MICCAI Society. It is identical to the accepted version, except for the format and this watermark; the final published version is available on SpringerLink.

A Secure AR Framework for 3D Medical Data Visualization using Decentralized Biometric Cryptosystem

Shreyansh Sharma[1⋆] and Santanu Chaudhury[2]

[1] Department of Computer Science and Engineering,
NIIT University, Neemrana, Rajasthan, India
shreyanshsharma665@gmail.com
[2] Department of Electrical Engineering,
Indian Institute of Technology Delhi, India
and Vachani School of Advanced Computing, Ashoka University, India
schaudhury@gmail.com

Abstract. Augmented Reality (AR) supports interactive 3D medical visualization but introduces challenges in data security, privacy, and collaborative access. This paper presents a decentralized AR framework that integrates a multimodal biometric cryptosystem, a redactable blockchain, and IPFS-based storage for secure visualization of patient-specific 3D anatomical models. User authentication combines facial and fingerprint biometrics protected by a fuzzy vault scheme with Reed-Solomon (RS) encoding and asymmetric encryption. Smart contracts on a private redactable blockchain provide secure, auditable access control for authorized users. MRI scans are converted into lightweight 3D meshes and visualized through a mobile AR application for collaborative surgical planning. Experimental results show low authentication latency and resilience against common security threats. A user study with 60 medical professionals confirms the framework's security, privacy, usability, and clinical value, demonstrating its effectiveness for secure collaborative 3D medical visualization.

Keywords: 3D Medical data visualization · Augmented Reality · Biometric Cryptosystem · Blockchain · Fuzzy Vault

1 Introduction

The rapid growth of immersive technologies such as Augmented Reality (AR) in healthcare has opened new possibilities for medical visualization, surgical planning, and diagnostic interpretation. These technologies enable spatially contextual, photorealistic 3D overlays of anatomical structures, which aid the medical experts in understanding complex regions such as tumors [1, 2, 3]. Such an ability to visualize medical data remotely using mobile or wearable AR devices

⋆ Corresponding author.

facilitates collaboration among medical experts in real time from different geolocations. However, most of the existing AR-based medical visualization systems lack the security infrastructure needed to handle sensitive patient data. Centralized architectures and password-based access control mechanisms make these systems vulnerable to unauthorized data manipulation, privacy violations, and non-compliance with data protection regulations such as GDPR and HIPAA [4]. In surgical planning workflows involving experts from multi-institutions, clinicians often need collaborative, remote access to patient-specific 3D medical data. Traditional systems lack mechanisms to enforce secure collaborative authentication or traceable access control. Moreover, storing and sharing large volumes of 3D models introduces performance and scalability challenges, especially under privacy constraints.

To address these limitations, we propose a secure and decentralized AR framework for 3D visualization of medical data. For collaborative remote access of the visualization, the proposed framework integrates a Biometric Cryptosystem based on multimodal biometric authentication (face and fingerprint) with a modified fuzzy vault-based cryptographic mechanism for template protection, and a redactable blockchain, which enforces secure collaborative access through smart contracts. Patient-specific 3D models are stored securely on the IPFS, ensuring data immutability, decentralized access, and tamper-resistant retrieval.

2 Related Work

The advancements in AR have enabled 3D visualization for surgical navigation, diagnostics, and training [1, 2, 3], but most applications emphasize usability while neglecting security and privacy. Blockchain-based systems such as MedRec [5] enable decentralized medical record management with traceable access, and Yeh et al. [6] proposed a redactable blockchain to support GDPR compliance. However, these works target textual or structured data, not large interactive 3D datasets, and overlook risks tied to sensitive patient models. For secure access, biometrics have been widely studied [7], yet simple template storage remains vulnerable. The fuzzy vault scheme [8] provides error-tolerant protection of biometric templates, and Sharma et al. [9] extended it into a multimodal decentralized authentication system.

Nevertheless, none of the existing systems have explored a combination of fuzzy vault-based biometric security, decentralized storage, and blockchain-enforced collaborative access into a unified AR-enabled medical visualization framework. In particular, multi-party consensus for remote collaborative authorization before rendering sensitive 3D medical models in AR environments has not been explored in the existing literature. This work addresses this gap by proposing a system that integrates secure multimodal authentication, privacy-preserving data sharing, and photorealistic AR visualization of patient medical data in 3D.

3 Threat Model

Given the highly sensitive nature of medical data and the collaborative nature of surgical planning across distributed environments, the proposed framework for remote 3D medical visualizations must ensure resistance to unauthorized access and malicious attacks. Therefore, the threat model for this framework considers the following potential attack vectors (1) Replay Attack: An attempt to reuse previously captured biometric data for unauthorized access, (2) Brute Force Attack: An attempt to guess or systematically derive cryptographic secrets or biometric vault keys by exploiting template patterns or trying multiple combinations, (3) Template Reversibility: An attempt to reconstruct the original biometric inputs using weakly stored templates in plaintext/ weak hashes, (4) Linkability Across Sessions: Reusing the same biometric encoding across sessions to correlate user identities over time, (5) Tampering of Data or Vault: An attempt to modify 3D model or other stored data, (6) Collaborative Access Breach: A malicious user may gain access to 3D medical data or approve modifications without consensus, undermining both the technical and legal safeguards for sensitive medical data.

4 Proposed Methodology

Fig. 1 illustrates our secure AR-based framework for medical data visualization, which integrates multimodal biometric authentication, fuzzy vault cryptography, decentralized IPFS storage, and a redactable blockchain-based access-control layer. A user within the metaverse environment provides facial and fingerprint biometrics, which are preprocessed and feature-extracted to generate a bio-token. These features are encoded into RS codes, combined with chaff points, and secured using a fuzzy vault scheme with a derived fuzzy key, further encrypted via an asymmetric cryptosystem. The encrypted vault is stored on IPFS, and its content hash is recorded on a redactable blockchain. Patient-specific 3D medical models are likewise stored on IPFS, with their references logged on blockchain. Access is governed by smart contracts and granted only after successful multi-user biometric authentication by all the designated medical experts. The redactable blockchain supports GDPR-aligned access control by enabling controlled modification of access logs while preserving transparency and auditability, thereby supporting decentralized, tamper-resistant visualization of sensitive medical data.

To implement the proposed framework, we first generate lightweight, spatially registered 3D anatomical models from clinical MRI datasets. We utilize the publicly available ReMIND database [10], which includes pre- and intra-operative MRI scans of 123 patients who underwent tumor resection. After excluding low-quality scans and artifacts, 114 datasets remain, each containing preoperative T1-weighted post-contrast and T2-weighted MRI volumes and manual segmentations of the tumor, cerebrum, and ventricles. MRI volumes are imported into 3D Slicer [11] to generate label maps from the provided segmentations. These label maps are converted into high-quality polygonal surface meshes representing

anatomical structures. The meshes are exported in `.OBJ` format, simplified using Instant Meshes to reduce polygon complexity, refined in Blender [12], and exported in `.FBX` format for AR deployment. The optimized models are imported into Unity [13] to build a marker-less Android-based AR application. The system uses device-mounted RGB cameras to enable spatial registration of 3D anatomical structures in the physical environment. Experts can interact with the models through gestures, supporting zoom, rotation, and structural isolation (e.g., selectively visualizing tumors or ventricles). Color-coded segmentation enhances differential interpretation (e.g., red for T2 tumors, green for T1-enhanced regions). To ensure secure and auditable access, each user authentication event and IPFS content hash is recorded on the blockchain. Access to the encrypted vault and 3D models is granted only after all designated medical experts successfully complete biometric authentication within a defined session. Smart contracts retrieve the corresponding IPFS hash to unlock the models. This supports GDPR-aligned access control and preserves long-term auditability without storing raw biometric templates.

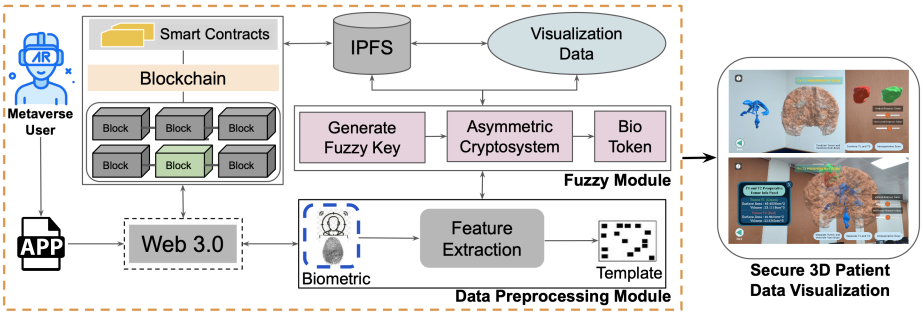


Fig. 1: Overview of the proposed AR medical visualization framework for secure collaborative surgical planning via biometric-based authentication, consensus-based access through blockchain, and IPFS for decentralized data storage.

Enrollment Process: Algorithm 1 describes the enrollment process where features from face and fingerprint biometrics are encoded using RS codes and embedded into a grid structure. A fuzzy vault is then created by encrypting this grid with a key derived from both modalities. The vault is stored on IPFS, and its reference hash is recorded on a private redactable blockchain for secure and decentralized access.

Recognition Process: Algorithm 2 presents the recognition and access control process. The user retrieves the stored fuzzy vault via blockchain and IPFS, then extracts and encodes fresh biometric features. A candidate key is derived and used to decrypt the vault. Matching is performed by comparing distances between decoded grid values and the new RS codes. If the average score meets

Algorithm 1 Enrollment

Input: Face biometric $B1$, Fingerprint biometric $B2$
Output: Fuzzy vault FV, IPFS hash h
Extract features: $F1 \leftarrow \text{CNN}(B1), \quad F2 \leftarrow \text{Minutiae}(B2)$
Generate RS codes: $C1 \leftarrow \text{RS}(F1), \quad C2 \leftarrow \text{RS}(F2)$
Generate random index set $R = \{r_1, r_2, \ldots, r_n\}$ from $[1, 2n]$
Initialize grid G of size $2n \times 3$
for $i = 1$ to n **do**
    $col \leftarrow \text{Random}(\{0, 1, 2\})$
    $G[r_i][col] \leftarrow C1[i]$
end for
Fill remaining grid cells with chaff that each row forms an AP with tolerance δ
Derive fuzzy key $K_f \leftarrow \text{KeyGen}(C1, C2)$
$FV \leftarrow \text{Encrypt}(G, R, K_f)$
Upload FV to IPFS and obtain content hash h
Record h on the private redactable blockchain

the threshold, the user is authenticated. Once all designated experts are verified, the system enables access to the AR-based 3D visualization interface.

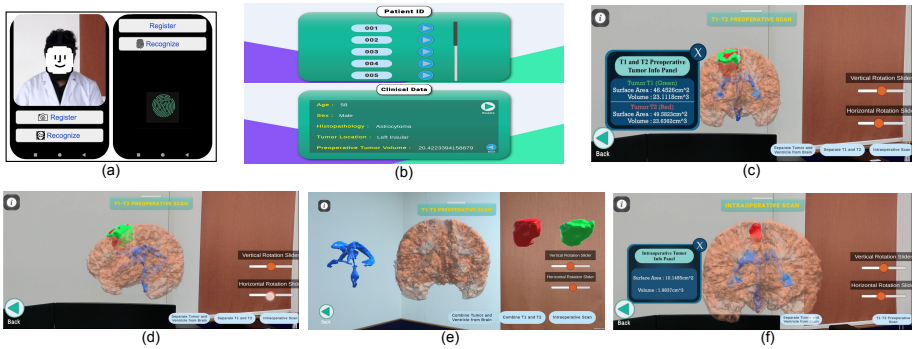


Fig. 2: Developed AR-based interactive application for 3D data visualization using an Android app for brain tumor. Link presents the demonstration video.

5 Results and Analysis

In this section, the performance of the proposed framework is validated through extensive experiments and user feedback analysis.

5.1 Experimental Setup

Experiments were conducted on a high-performance workstation and an Android smartphone supporting AR applications. The developed FBX model was inte-

Algorithm 2 Recognition and Visualization Access

Input: Face biometric $B1'$, Fingerprint biometric $B2'$
Output: Genuine or Imposter
$FV \leftarrow$ User sends a request to retrieve fuzzy vaults from IPFS through the blockchain network.
Extract features: $F1' \leftarrow \text{CNN}(B1')$, $F2' \leftarrow \text{Minutiae}(B2')$
Encode features: $C1' \leftarrow \text{RS}(F1')$, $C2' \leftarrow \text{RS}(F2')$
Derive candidate key $K'_f \leftarrow \text{KeyGen}(C1', C2')$
Decrypt: $(G', R') \leftarrow \text{Decrypt}(FV, K'_f)$
if R' is null **then**
    return Imposter
end if
$score \leftarrow 0$
for $i = 1$ to n **do**
    Compute distances d_0, d_1, d_2 between $C1'[i]$ and $G'[r_i][j]$ for $j = 0, 1, 2$
    $score \leftarrow score + \min(d_0, d_1, d_2)$
end for
$avg \leftarrow score/n$
if $avg \leq \theta$ **then**
    return Genuine
else
    return Imposter
end if
if All authorized experts have authenticated successfully **then**
    return Launch AR Visualization Interface
else
    return Wait for other expert authentications
end if

grated into Unity 2021.3 LTS to enable AR-driven visualization and interaction. Within Unity, relevant materials and textures were assigned to the brain model to improve visual clarity and realism. Furthermore, blockchain-based security was implemented through Solidity smart contracts deployed on the Polygon testnet, with biometric data securely managed via IPFS. To support a robust and scalable solution, the system was trained and tested using the ReMIND Brain MRI Database [10] for tumor depiction, along with facial and fingerprint biometric datasets for authentication purposes. A Unity-based user interface was created to offer intuitive control over the 3D model, enabling smooth navigation and real-time interactivity. The optimized meshes contained 20k-35k faces (8-12 MB each) with 3 MB IPFS overhead; the framework supported up to 10 concurrent sessions on the Polygon testnet, with node failover recovery within 2 s.

5.2 3D Visualization through AR

The Android application for AR was built such that each interactive model corresponds to one of three distinct cases: T1 post-contrast pre-operation, T2-weighted pre-operation, and intra-operative scans. As illustrated in Fig. 2, (a)

presents the user interface with a login screen that employs face and fingerprint biometrics of the user (medical experts) for secure identification. Upon successful authentication of all the designated users, they are directed to (b), where a list of patients is displayed by unique IDs, thereby maintaining confidentiality. On the next page, as shown in (b), detailed patient information, namely age, sex, histopathology data, tumor location, and preoperative tumor volume is displayed. In (c), the user utilizes an Android application to access the AR view of the brain along with information of pre-operation scan, and vertical and horizontal rotations functionality. Tumor surface areas are distinctly marked, with T1 regions in green and T2 regions in red. Then, (d) depicts the visualization after horizontal rotation. (e) illustrates the ability to separate and visualize distinct anatomical structures within the AR environment, including the cerebrum, tumor, and brainstem. Finally, (f) illustrates the intra-operative scan of the affected region.

5.3 User Study and Feedback Analysis

A structured evaluation involving 60 medical professionals, including neurosurgeons, radiologists, and surgical assistants, was conducted to assess the usability, security, and clinical relevance of the proposed mobile AR biometric authentication framework. Participants included 38 neurosurgeons, 14 radiologists, and 8 surgical assistants from three tertiary hospitals and two private clinics. After interacting with the developed AR-based system for secure 3D brain MRI visualization, participants completed a comprehensive survey covering security perception, usability, clinical utility, authentication speed, privacy, system reliability, learning curve, and blockchain trust. As shown in Fig. 3, the feedback

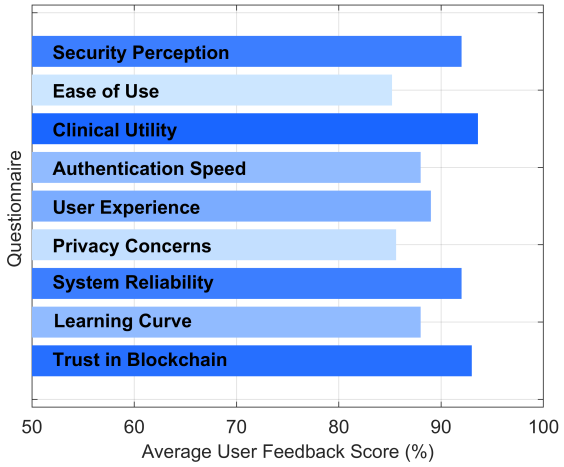


Fig. 3: User Study and Feedback from Medical Professionals.

was strongly positive. Security perception and trust in blockchain scored above 90%, reflecting strong confidence in safeguarding sensitive patient data via decentralized storage. System reliability was similarly rated highly, reinforcing the robustness of the biometric mechanism under clinical conditions. Clinical utility achieved a rating of 91%, with participants appreciating the role of real-time AR visualization in improving surgical planning and intraoperative navigation. Ease of use averaged 87%, with most professionals finding the authentication process intuitive, although a few required minimal onboarding, as indicated by the learning curve score of 81%. Privacy assurance was rated 88%. Authentication speed, measured between 480 ms to 530 ms, was considered acceptable for routine workflows, with minor suggestions to further reduce latency for emergency cases. This latency decomposed into 120 ms biometric processing, 150-180 ms smart-contract execution on the Polygon testnet, 90-120 ms IPFS retrieval (warm local), and 80-110 ms AR rendering, measured over 20 repeated trials per representative case (mean ± SD). Under emulated adverse networks (2 Mbps, 5% loss), latency rose to 710 ± 65 ms vs. 495 ± 28 ms baseline; cold IPFS fetches averaged 1.8 s vs. 0.12 s warm, with Polygon testnet finality at 1-2 s.

6 Security Analysis

The proposed framework mitigates the threats identified in Section 3.

Replay Attack: Session-specific fuzzy vaults are generated using fresh biometric samples and feature encodings. Consequently, replayed credentials cannot reconstruct a valid vault: [$F_k^{\text{current}} \neq F_k^{\text{replay}}$.]

Brute Force Attack: Biometric features are encoded using Reed–Solomon codes and protected with chaff points. The probability of recovering the genuine polynomial by exhaustive search is [$P = \binom{n+k}{n}^{-1}$,] where n and k denote the numbers of genuine and chaff points, respectively. For sufficiently large k, P becomes negligible.

Template Reversibility: Raw biometric templates are never stored. The RS encoding and fuzzy vault construction provide a non-invertible representation, preventing recovery of original facial or fingerprint features.

Linkability Across Sessions: To prevent user tracking across authentication sessions, feature vectors are combined with session-specific entropy: [$h_i^{\text{session}} = \mathsf{Hash}(f_i \parallel \eta)$.] This produces unlinkable encodings for the same user across different sessions.

Tampering of Data: Vaults and 3D model references are stored on IPFS, while their hashes are recorded on the blockchain. Any modification results in [$\mathsf{Hash} * \text{retrieved} \neq \mathsf{Hash} * \text{on-chain}$,] thereby detecting unauthorized changes.

Collaborative Access Breach: Smart contracts enforce consensus-based authorization, granting access only when all designated experts are successfully authenticated: [$\forall u_i \in U, \quad \mathsf{Auth}(u_i) = \text{True}$,] where $U = u_1, u_2, \ldots, u_m$ represents the set of authorized medical experts.

7 Conclusion

This work proposes a secure AR framework for collaborative 3D medical data visualization by combining multimodal biometric authentication, fuzzy vault cryptography, IPFS, and a redactable blockchain. The framework enables authenticated access, secure storage, and controlled sharing of patient-specific 3D models in an AR environment. The prototype was implemented on mobile devices and evaluated through security analysis and a user study with medical professionals. The results indicate that the framework supports secure collaboration while preserving data privacy and access accountability. Future work will evaluate the framework with additional imaging modalities and larger clinical studies.

Disclosure of Interests. The authors have no competing interests to declare.

Bibliography

[1] Vincenzo Ferrari, Gudrun Klinker, and Fabrizio Cutolo. Augmented reality in healthcare. *Journal of healthcare engineering*, 2019:9321535, 2019.

[2] Abel J Lungu, Wout Swinkels, Luc Claesen, Puxun Tu, Jan Egger, and Xiaojun Chen. A review on the applications of virtual reality, augmented reality and mixed reality in surgical simulation: an extension to different kinds of surgery. *Expert review of medical devices*, 18(1):47–62, 2021.

[3] Shu-Chen Liao, Shih-Chieh Shao, Shi-Ying Gao, and Edward Chia-Cheng Lai. Augmented reality visualization for ultrasound-guided interventions: a pilot randomized crossover trial to assess trainee performance and cognitive load. *BMC Medical Education*, 24(1):1058, 2024.

[4] P. Voigt and A. Von dem Bussche. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer International Publishing, 2017.

[5] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. Medrec: Using blockchain for medical data access and permission management. In *2016 2nd international conference on open and big data (OBD)*, pages 25–30. IEEE, 2016.

[6] Lo-Yao Yeh, Wan-Hsin Hsu, and Chih-Ya Shen. Gdpr-compliant personal health record sharing mechanism with redactable blockchain and revocable ipfs. *IEEE Transactions on Dependable and Secure Computing*, 2023.

[7] Anil Jain, Lin Hong, and Sharath Pankanti. Biometric identification. *Communications of the ACM*, 43(2):90–98, 2000.

[8] A. Juels and M. Sudan. A fuzzy vault scheme. *Proceedings of IEEE Symposium on Security and Privacy*, 2002.

[9] Shreyansh Sharma, Anil Saini, and Santanu Chaudhury. Multimodal biometric user authentication using improved decentralized fuzzy vault scheme based on blockchain network. *Journal of Information Security and Applications*, 82:103740, 2024.

[10] Parikshit Juvekar, Reuben Dorent, Fryderyk Kögl, Erickson Torio, Colton Barr, Laura Rigolo, Colin Galvin, Nick Jowkar, Anees Kazi, Nazim Haouchine, et al. Remind: The brain resection multimodal imaging database. *Scientific Data*, 11(1):494, 2024.

[11] Andriy Fedorov, Reinhard Beichel, Jayashree Kalpathy-Cramer, Julien Finet, Jean-Christophe Fillion-Robin, Sonia Pujol, Christian Bauer, Dominique Jennings, Fiona Fennessy, Milan Sonka, John Buatti, Stephen Aylward, James V. Miller, Steve Pieper, and Ron Kikinis. 3d slicer as an image computing platform for the quantitative imaging network. *Magnetic Resonance Imaging*, 30(9):1323–1341, 2012. Quantitative Imaging in Cancer.

[12] Blender Online Community. *Blender - a 3D modelling and rendering package*. Blender Foundation, Stichting Blender Foundation, Amsterdam, 2018.

[13] John K Haas. A history of the unity game engine. 2014.