International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

PRIVACY PRESERVING MEDICAL DATA SHARING WITH BIOMETRIC AUTHENTICATION AND ENCRYPTION

Sameera Parveen.S,Thasumina.M,Padmapriya.S,Dr.M.Chinnadurai M.E,Ph.D
Department of Computer Science and Engineering
E.G.S Pillay Engineering College, Nagapattinam, Tamil Nadu, India

Abstract-

The security of healthcare data is of utmost importance, as conventional password-based authentication is susceptible to attacks, theft, and human errors. To combat these issues, this paper presents a privacy-protecting model that combines biometric authentication based on facial recognition (Grassmann algorithm) with Advanced Encryption Standard (AES) for safe sharing of medical data.The system only provides access to authorized individuals to sensitive documents by applying accurate biometric verification and secure encryption during storage and transmission.

The suggested architecture employs a cloud-based system to ensure controlled and secure data exchange between healthcare organizations. By applying facial recognition rather than passwords and AES encryption, the system is significantly enhanced with respect to preventing unauthorized access and data leakage. Experimental deployment shows that the technique is viable, with an observation that it is possible to maximize data privacy without compromising on usability. Scalability enhancement and integration with current healthcare systems are directions of future research to render it more adoptable.

Keywords: Biometric Authentication,Facial Recognition,Grassmann Algorithm,AES Encryption,Medical Data Security,Privacy-Preserving Framework,Cloud-Based Data Sharing,Healthcare Cybersecurity,Access Control Secure ,Data Transmission

INTRODUCTION

Growing digitization of health systems has exposed medical information to security violations, as conventional password authentication is unable to cope with the sophisticated nature of cyber attacks. Patient information, which is sensitive in nature, needs to be protected through firm mechanisms to avoid it falling into wrong hands and yet shared easily between authorized healthcare providers.These challenges are addressed in this essay by suggesting an integrated system with biometric authentication through facial identification and sophisticated encryption methods to provide a secure and efficient alternative to traditional security systems. The system incorporates the Grassmann algorithm for precise facial recognition and the Advanced Encryption Standard (AES) for secure data storage and transmission. By deploying such technologies in a cloud-based infrastructure, the architecture does away with only unauthenticated users accessing encrypted medical records, greatly minimizing risks of data breaches. This not only ensures better data security but also maintains usability and closes significant loopholes in currently available healthcare data protection frameworks, and is compatible with privacy mandates. The later sections introduce the methodology, implementation, and advantages of this privacy-preserving sharing of medical data framework.

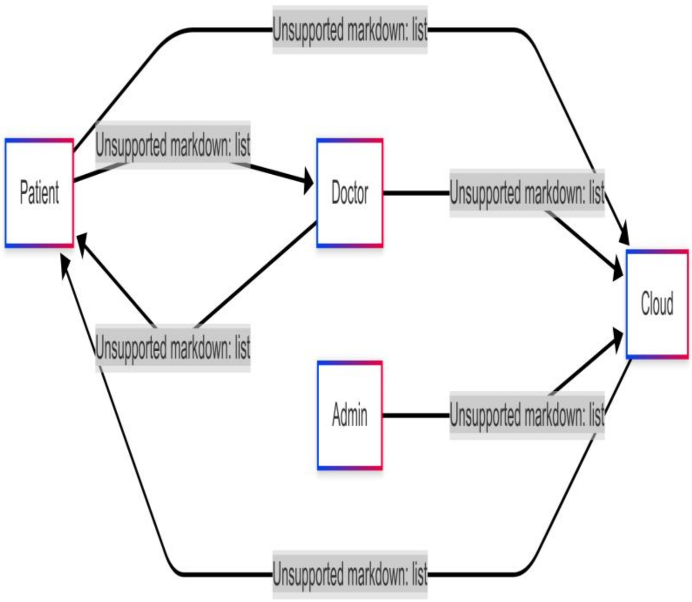
II.LITERATURE REVIEW

The increasing digitalization of healthcare infrastructure has escalated privacy and security concerns regarding personal medical information, and stronger protection beyond password-based means is essential. Studies have confirmed the superiority of biometric authentication and encryption to guard medical records.Miao et al. (2021) have suggested an attribute-based encryption (ABE) scheme for multi-owner environments that supports fine-grained access control and efficient keyword searches, but scalability is an issue. Parallelly, Qiu et al. (2020) investigated privacy-preserving frequent itemset mining with encrypted cloud data and achieved trade-offs in data utility and security but with computationally costly overhead.Chaudhari & Das (2020) suggested searchable encryption with fine-grained access control and enhanced privacy but with enhanced implementation complexity in large-scale systems. The above work points out security vs. usability vs. performance trade-offs in sharing encrypted medical information.

Biometric authentication has become a secure substitute for passwords, with Zhou & Ren (2018) showcasing its promise through privacy-preserving methods in *PassBio*, though computational requirements are still a drawback.Konan & Wang (2019) further proposed security for wearable medical devices using mutual batch authentication in WBANs but at higher operation costs. All these works, collectively, stress the need for incorporating biometrics with advanced encryption techniques such as AES for end-to-end protection.The framework of the presentation is consistent with these researches, where Grassmann manifold-based facial recognition is blended with AES encryption to counter weaknesses in conventional systems. Future studies must emphasize scalability, compatibility with current healthcare infrastructures, and maximizing computational efficiency to ensure mass adoption.

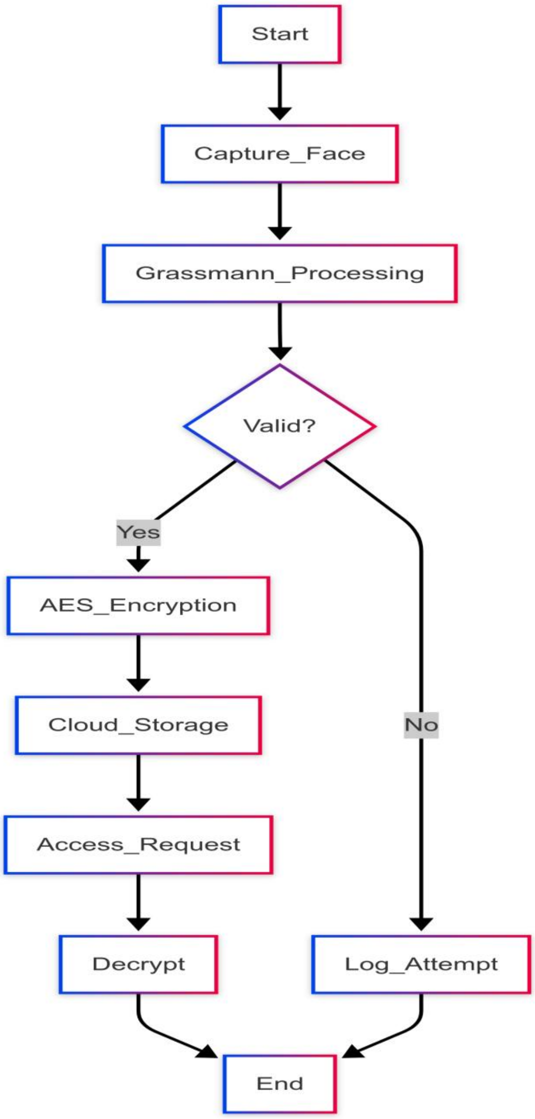
III.PROPOSED DESIGN

The design presented presents a privacy-preserving, secure medical data-sharing platform that combines biometric authentication (via the Grassmann algorithm for face recognition) with AES-256 encryption to provide end-to-end security. The framework includes four primary modules: (1) a biometric verification module that authenticates user identity based on facial feature extraction and normalization, (2) an AES-based encryption/decryption module to secure data storage and transmission, (3) a sharing module in the cloud to grant secure access for authorized healthcare practitioners, and (4) an access control module that regulates authorization and logs transactions for regulatory compliance.By replacing risky password mechanisms with biometric identification and secure encryption, the design defends against unauthorized access threats and supports usability. Emerging development includes multi-modal biometrics (e.g., iris/fingerprint), high-performance AES for big datasets, and blockchain support for unchangeable audit trails, supporting scalability and compliance (e.g., HIPAA/GDPR). The design delivers a single, secure solution for next-generation healthcare data ecosystems.


Unsupported markdown: list
Unsupported markdown: list
Patient
Doctor
Unsupported markdown: list
Cloud
Unsupported markdown: list
Admin
Unsupported markdown: list
Unsupported markdown: list

The developed framework is three-tiered in architecture: (1) User Layer where physicians and patients communicate through biometric-authenticated interface, (2) Processing Layer that processes Grassmann-based face recognition and AES-256 encryption/decryption, and (3) Cloud Storage Layer where encrypted medical records are stored with role-based access control.The data flows only in one direction: biometric authentication unlocks the AES keys to allow only certified users to decrypt records. The architecture combines real-time audit (e.g., access logs) and scaling through modular cloud APIs, complying with HIPAA/GDPR. Future expansion (dotted-line components) is blockchain audit trails and multi-modal biometrics (iris/fingerprint).

ACTIVITY DIAGRAM



IV.REQUIREMENTS

HARDWARE REQUIREMENT

Processor - Intel processor 2.6.0 GHZ
Ram - 4 GB
Hard Disk - 160 GB
Compact Disk - 650 Mb
Keyboard - Standard keyboard
Monitor - 15 inch color monitor

SOFTWARE REQUIREMENT

Operating System – Windows OS
Frontend: Python
Backend: Python 3.8+

IDE - PYCHARM

ADDITIONAL DEPENDENCIES AND CONSTRAINTS

Dependencies

Its major dependencies are Python 3.8+, OpenCV (for Grassmann-based face recognition), PyCryptodome (AES-256 encryption), NumPy/SciPy (affine transformations, Karcher mean computation), and SQLAlchemy (for encrypted db operations). Cloud integration is supported by AWS/Azure SDKs (e.g., boto3), and API endpoints and role-based access are handled by Flask/Django frameworks.Hardware requirements are dual-core CPU (2.6 GHz+), 2GB RAM, and HD camera to support biometric capture, analogous to the specifications outlined in the PPT . The other extensions include the inclusion of blockchain libraries (e.g., PyTezos) to enable audit trail support.

Further Constraints

The proposed system comes with limitations and constraints as follows: Computational Overhead—the Grassmann algorithm and AES-256 encryption may introduce latency in real-time authentication on low-end hardware (2GB RAM/dual-core CPU), Biometric Accuracy—the facial recognition degrades under poor lighting or occlusions and requires ideal conditions for capture; Scalability-the existence of stable Internet supports an almost seamless cloud-based design that does not consider offline access; Regulatory Gaps—the proposed system implies HIPAA and GDPR compliance but leaves undisclosed explicit certification regarding the storage of biometric data; and Interoperability—There are no comments pertaining to the legacy EHR system integration. Future efforts need to balance algorithms for edge devices and overcome these deployment hurdles.

V.METHODOLOGY

CoreTechnique:

Biometric verification (Grassmann algorithm for face recognition) with AES-256 encryption to protect medical information. The procedure starts with face feature extraction and normalization through affine transformation, followed by identity verification on the Grassmann manifold. Authenticated users initiate AES encryption for data storage/transmission, decryption being allowed only after biometric authentication. A cloud-based RBAC system imposes role-specific access (admin/doctor/patient), with audit logs recording transactions. Such end-to-end pipeline assures privacy-preserving sharing of data and avoids password attacks.

DataPreparationandEmbedding:

The data preparation and embedding process involves eight key steps: First, facial images are captured using an HD camera for biometric input. Next, affine transformation normalizes facial coordinates to ensure consistent feature extraction. The processed images are then mapped as points on a Grassmann manifold for mathematical representation. A Karcher mean is computed from these manifold points to create stable biometric templates. These templates are securely bound to AES encryption keys for cryptographic operations.

SecureShareDistribution:

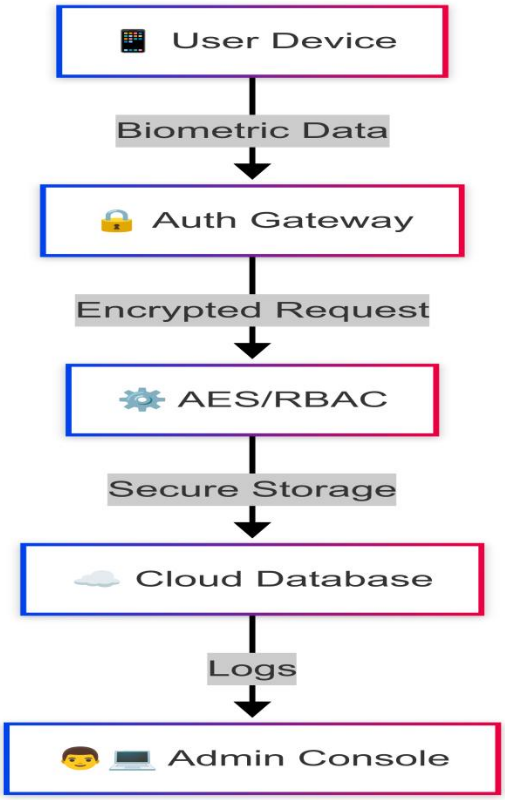
The safe share distribution procedure has eight main steps: Firstly, authenticated users (doctors/patients) request access via biometric verification using the Grassmann algorithm. Once successfully verified, the system retrieves the encrypted medical records from cloud storage. The AES-256 decryption process is invoked only for authenticated users with suitable permissions. Role-based access control (RBAC) is simply sharing information based on the privileges of a user (admin/doctor/patient). All data transfers and access requests are recorded in real-time for audit and compliance. End-to-end encryption is enabled within the system while it is sending the information to avoid interception.

Effective Transmission and Reconstruction:

The system guarantees efficient transmission and reconstruction via six critical steps: First, medical information is encrypted with AES-256 prior to transmission to ensure confidentiality. Second, encrypted information is transmitted through secure cloud channels with TLS/SSL encryption. Third, only users biometrically authenticated can request decryption via the Grassmann algorithm verification. Fourth, role-based access control checks user permissions prior to starting reconstruction. Fifth, AES decryption rebuilding ensures that original information is reestablished only to certified receivers. Last, the transmission history and access are tracked for security audits and compliance surveillance.

MedicalApplicationSuitability:

The proposed system has significant medical usage potential by fulfilling key health care data security requirements through its combination of biometric authentication (Grassmann-based face recognition) and AES-256 encryption to allow access only to authorized personnel such as doctors, patients, and administrators for viewing sensitive records.Its cloud design provides secure real-time data sharing between medical providers and is privacy regulation compliant.



VI.CONCLUSION

This research presents a privacy-sensitive, secure mechanism for the sharing of medical data through Grassmann-based facial verification for secure biometric authentication and AES-256 encryption for end-to-end encryption of data. Cloud-based technology provides scalable, HIPAA/GDPR-compliant storage and role-based access control limits the access to data for users on a specific role.Through vulnerability removal from passwords and enhanced auditability, the system addresses serious healthcare security issues. New extensions, such as multi-modal biometrics and blockchains for audit trails, have the potential to further augment the framework. The solution offers a secure, effective, and regulative compliant manner of safeguarding sensitive medical files in modern-day healthcare systems.

REFERNCES:

1.Karkhile, A., et al. (2021). Privacy-preserving attribute-based keyword search in shared multi-owner setting.

2.Qiu, S., et al. (2017). Toward practical privacy-preserving frequent itemset mining on encrypted cloud data. IEEE Transactions on Cloud Computing, 8(1), 312-323.

3.Chaudhari, P., & Das, M. L. (2019). Privacy preserving searchable encryption with fine-grained access control. IEEE Transactions on Cloud Computing, 9(2), 753-762.

4.Zhou, K., & Ren, J. (2018). PassBio: Privacy-preserving user-centric biometric authentication. IEEE Transactions on Information Forensics and Security, 13(12), 3050-3063.

5.Konan, M., & Wang, W. (2019). A secure mutual batch authentication scheme for patient data privacy preserving in WBAN. Sensors, 19(7), 1608.

6.Boneh, D., & Franklin, M. (2003). Identity-based encryption from the Weil pairing. SIAM Journal on Computing, 32(3), 586-615.

7.Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In STOC '09 (pp. 169-178). ACM.

Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. In IEEE S&P (pp. 321-334).

Song, D. X., Wagner, D., & Perrig, A. (2000). Practical techniques for searches on encrypted data. In IEEE S&P (pp. 44-55).

8.Bellare, M., Boldyreva, A., & O'Neill, A. (2007). Deterministic and efficiently searchable encryption. In CRYPTO (pp. 535-552).

9.Wang, C., et al. (2010). Secure ranked keyword search over encrypted cloud data. In ICDCS (pp. 253-262).

10.Cash, D., et al. (2014). Highly-scalable searchable symmetric encryption with support for Boolean queries. In CRYPTO (pp. 353-373).

11.Naveed, M., et al. (2015). Inference attacks on property-preserving encrypted databases. In CCS (pp. 644-655).

12.Popa, R. A., et al. (2011). CryptDB: Protecting confidentiality with encrypted query processing. In SOSP (pp. 85-100).

13.Kamara, S., & Lauter, K. (2010). Cryptographic cloud storage. In FC (pp. 136-149).

14.Li, J., et al. (2013). Fuzzy keyword search over encrypted data in cloud computing. In INFOCOM (pp. 441-445).

15.Sun, W., et al. (2014). Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking. In ASIACCS (pp. 71-82).

16.Yu, S., et al. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. In INFOCOM (pp. 534-542).

17.Li, M., et al. (2015). Authorized private keyword search over encrypted data in cloud computing. In ICDCS (pp. 383-392).

18.Liu, Z., et al. (2016). Efficient verifiable fuzzy keyword search over encrypted data in cloud computing. In IEEE TCC, 4(2), 156-166.

19.Zhang, Y., et al. (2016). Secure attribute-based data sharing for resource-limited users in cloud computing. In IEEE TSC, 9(5), 733-745.

20.Orencik, C., et al. (2014). Multi-keyword search over encrypted data with scoring and search pattern obfuscation. In ESORICS (pp. 95-113).

21.Cao, N., et al. (2014). Privacy-preserving multi-keyword ranked search over encrypted cloud data. In IEEE TPDS, 25(1), 222-233.

22.Wang, B., et al. (2016). Privacy-preserving ranked multi-keyword search for multiple data owners in cloud computing. In IEEE TCC, 4(3), 289-300.

23.Xia, Z., et al. (2017). Secure semantic expansion based search over encrypted cloud data supporting similarity ranking. In IEEE TDSC, 14(4), 400-412.

24.Fu, Z., et al. (2016). Enabling personalized search over encrypted outsourced data with efficiency improvement. In IEEE TPDS, 27(9), 2546-2559.

25.Zhang, W., et al. (2016). Secure and efficient ranked keyword search over encrypted cloud data. In IEEE TDSC, 13(3), 350-362.

26.Li, H., et al. (2017). Privacy-preserving data aggregation for mobile crowdsensing with externality. In IEEE TMC, 16(10), 2764-2776.

27.Yang, Y., et al. (2015). Attribute-based data sharing with hidden policies in cloud computing. In IEEE TKDE, 27(7), 1864-1876.

28.Ruj, S., et al. (2014). Decentralized access control with anonymous authentication of data stored in clouds. In IEEE TPDS, 25(2), 384-394.

29.Hur, J., & Noh, D. K. (2011). Attribute-based access control with efficient revocation in data outsourcing systems. In IEEE TPDS, 22(7), 1214-1221.

30.Lewko, A., & Waters, B. (2011). Decentralizing attribute-based encryption. In EUROCRYPT (pp. 568-588).

31.Chase, M. (2007). Multi-authority attribute-based encryption. In TCC (pp. 515-534).

32.Green, M., et al. (2011). Outsourcing the decryption of ABE ciphertexts. In USENIX Security (pp. 523-538).

33.Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. In EUROCRYPT (pp. 457-473).

34.Goyal, V., et al. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In CCS (pp. 89-98).

35.Waters, B. (2011). Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In PKC (pp. 53-70).

36.Ostrovsky, R., et al. (2007). Attribute-based encryption with non-monotonic access structures. In CCS (pp. 195-203).

37.Okamoto, T., & Takashima, K. (2011). Fully secure functional encryption with general relations from the decisional linear assumption. In CRYPTO (pp. 191-208).

38.Lai, J., et al. (2013). Fully secure key-policy attribute-based encryption with constant-size ciphertexts. In ESORICS (pp. 90-109).

39.Zhang, Y., et al. (2018). Efficient attribute-based encryption with privacy-preserving key generation. In IEEE TIFS, 13(4), 949-962.

40.Liu, Z., et al. (2017). Secure and efficient searchable public key encryption for resource-constrained environments. In IEEE TCC, 5(4), 584-597.

41.Cui, H., et al. (2016). Efficient and expressive keyword search over encrypted data in cloud. In IEEE TDSC, 13(3), 364-375.

42.Wang, C., et al. (2018). Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing. In IEEE TIFS, 14(1), 203-216.

43.Li, J., et al. (2019). Privacy-preserving federated learning for IoT devices. In IEEE IoT-J, 6(5), 9182-9194.

44.Xu, G., et al. (2020). Secure and efficient blockchain-based data sharing for IoT. In IEEE TSC, 13(2), 312-324.

45.Zhang, L., et al. (2021). Lightweight and privacy-preserving authentication for mobile edge computing. In IEEE TIFS, 16, 2346-2359.

46.Chen, X., et al. (2020). Blockchain-based secure data sharing with fine-grained access control in IoT. In IEEE IoT-J, 7(8), 7643-7655.