RESEARCH PAPER

PRIVACY-PRESERVING AND EFFICIENT ATTRIBUTE-BASED ACCESS CONTROL WITH FACE AUTHENTICATION FOR CLOUD-BASED SMART HEALTHCARE

Suganya R[1], Banu Rithika M S[2], Dharani G[3], Sujitha C[4], Shereya B[5]

[1]Assistant Professor, Department of Artificial Intelligence and Data Science, V.S.B. Engineering College, Karur, India.
Email: suganyavsb20163@gmail.com (Corresponding Author)

[2]Department of Artificial Intelligence and Data Science, V.S.B. Engineering College, Karur, India.
Email: banurithikabanurithika@gmail.com

[3]Department of Artificial Intelligence and Data Science, V.S.B. Engineering College, Karur, India.
Email: dharanigokulakannan962004@gmail.com

[4]Department of Artificial Intelligence and Data Science, V.S.B. Engineering College, Karur, India.
Email: sujithachandrasekaran2004@gmail.com

[5]Department of Artificial Intelligence and Data Science, V.S.B. Engineering College, Karur, India.
Email: shereyabaskaran138@gmail.com

***Corresponding author: Suganya R, Assistant Professor, Department of Artificial Intelligence and Data Science, V.S.B. Engineering College, Karur, India**
Email: suganyavsb20163@gmail.com

Received: 30th May, 2026; **Revised:** 11th June, 2026; **Accepted:** 15th June, 2026; **Available Online:** 17th June, 2026

ABSTRACT

Background

Smart healthcare systems that are hosted on clouds have transformed the way patients are monitored and managed by allowing the access of medical data remotely. Nonetheless, healthcare information is delicate and in need of strong security protocols that ensure it is not accessed by unauthorized parties and that patients remain private.

Objective

The paper introduces an efficient and privacy-sensitive access control model that incorporates both attribute-based encryption (ABE) and face-based biometric authentication of cloud storage and retrieval of patient data but ensures privacy of the patient information.

Materials and Methods

The data in the proposed simulation of the IoT sources are healthcare data which is encrypted with lightweight cryptographic methods and uploaded on the cloud. On requesting access, the system will first identify the user by facial recognition before it determines access permission using user attributes like position, specialization and the level of access authorization. The data can only be decrypted and accessed by users who fulfill all the policy requirements, which will guarantee fine-grained and secure sharing of information.

Results

As opposed to the conventional ABE or biometric-only solutions, this joint solution improves the confidentiality of data, efficiency in access and protection of privacy and minimizes the computational load. Experimental findings reveal it has a considerable increase in access control performance and scalability.

Conclusion

Removing the need to rely on physical IoT hardware, the framework offers a scalable, viable, and safe approach to the management of cloud-based smart healthcare information.

Keywords: Smart healthcare, cloud computing, privacy protecting, Attribute-based access control (ABE), face authentication, secure data sharing, lightweight encryption.

How to cite this article: Suganya R, Banu Rithika MS, Dharani G, Sujitha C, Shereya B. Privacy-Preserving and Efficient Attribute-Based Access Control with Face Authentication for Cloud-Based Smart Healthcare. Int J Drug Deliv Technol. 2026;16(60s):1626-1632. DOI: 10.25258/ijddt.16.60s.145

Source of support: Nil.

Conflict of interest: None

Introduction

The spread of cloud computing in the healthcare sector has allowed to store, process, and share huge amounts of data about patients efficiently and conduct remote monitoring and advanced analytics. Nevertheless, due to the sensitivity of medical records, there is a need to have strong security and privacy-protecting measures to ensure that unauthorized access, data breaches, and regulatory violations are avoided. The conventional access control systems, including password-based authentication or unimodal biometrics, may not be effective in overcoming these issues because of the changing cyber threats and growing complexity of the system [2], [3]. To address such

drawbacks, attribute based access control model (ABE) has come forward as an enticing model, where fine-grained access is achieved through user attributes, roles and contextual parameters. As an example, Smart Access combines ABE with blockchain-based smart contracts to enable transparent and audible medical data sharing across organizations and increase trust and policy compliance [1]. Although blockchain is immutable, audit-able, a combination of blockchain with biometric verification provides additional assurance of authentication. According to the recent studies, multimodal biometric solutions, such as facial recognition, fingerprints, and voice verification, are essential towards enhancing the integrity of cloud-based healthcare protection system [2], [3], [4]. Besides, to minimize computational overhead and identify anomalous access patterns in real-time to garner secure yet efficient data handling, lightweight cryptography methods and AI-based anomaly detection have been implemented [2] and [5]. Predictive and regression models that are cloud enabled are also useful in authentication efficiency since they analyse the biometric data and user behavior patterns so that they reduce the cases of authentication failure without compromising on usability [5]. Although this has been achieved, the majority of the current schemes concentrate on either biometric-only or cloud-based ABE without relying on a complete integration of both paradigms on privacy-preserving and scalable basis. Driven by such loopholes, the present work suggests a privacy-saving and efficient ABE-based architecture with face-based authentication as an improvement of cloud-based smart healthcare. The proposed system would provide fine-grained access control, low latency, and a high level of privacy with no reliance on physical IoT devices by means of a combination of attribute-based policies, lightweight encryption, and biometric verification. It is a secure, scalable, and user-friendly healthcare data management that is suitable to the distributed medical settings of the modern era.

I. Related Works

Recent studies have widely discussed the use of cloud computing, blockchain and biometric verification in order to improve security and privacy in smart healthcare systems. Saini et al. [6] proposed an access control framework of cloud-based healthcare systems through a framework built on the basis of smart-contracts to resolve the single point of failure problem associated with a centralized EMR storage. With the elliptic curve cryptography (ECC) and EdDSA to encrypt EMRs and smart contracts to verify users, authorize access, detect misbehaviors, and revoke access, the system will provide a secure and auditable EMR sharing between various entities. Another solution to privacy preserving collaborative access control is Federated learning, which is also becoming a promising solution. Li et al. [7] developed a federated learning-based multi-authority access control scheme that secret parameters are jointly produced by the system administrators and untrusted authorities. Medical data are stored and encrypted and stored in tamper-resistant IPFS and hashes of local models and training data are recorded in blockchain, allowing traceability and auditability without considering patient privacy.

Ramar et al. [8] introduced a framework based on blockchain, biometric authentication, and Directed Acyclic Graphs (DAG) on a cloud platform to provide more scalability, security, and efficiency. The framework uses blockchain to store records impartially, biometrics to authenticate the identity and uses parallel processing of the DAG to minimize the transaction latency with significant gains in privacy, integrity and throughput. Baskar et al. [9] stated that blockchain can help in securing healthcare data, and in this respect, the system may be utilized to store patient information as EHR in the form of an immutable and verifiable record, which can be accessed in real-time by authorized parties. The paper highlights the importance of blockchain in eliminating the process of tampering data and enhancing trustworthiness in the healthcare networks distributed over the network. Lastly, Hamouid and Mohammedi [10] have focused on the drawbacks of preparing access control models to the IoT-enabled smart healthcare, and suggested a dynamic ABAC approach. Their model dynamically adjusts access policies based on the emergencies or the evolving circumstances, making it more flexible and compliant in extremely dynamic healthcare settings. The latest developments in smart healthcare have gradually centered on integrating blockchain, fog computing, and attribute-based access control (ABE) to attain secure, efficient, and privacy-guaranteeing administration of data. Li et al. [11] suggested a blockchain-based multiauthority ABE scheme of fog IoT healthcare systems, where the computational load on the resource-limited IoT devices is transferred to the fog nodes. In this way, they guarantee fine-grained access control, zero single points of failure, and transparency in the form of blockchain-recorded smart contracts.

PAFR-ABE is an access control scheme that was proposed by Liang et al. [12] and it has privacy-preserving authentication and flexible secret key revocation. PAFR-ABE can solve both security and usability problems of 5G-enabled and IoT-enabled smart healthcare systems because it hides user identities in key generation, and allows key revocation selectively without impacting unrevoked users. In the case of Ethereum blockchain and ABAC integration in healthcare based on IoT, Filali et al. [13] have applied AES encryption and decentralized storage through IPFS. Their model provides integrity, transparency, and access control on a fine-grained basis of data, and all the transactions are stored on the blockchain on an immutable basis, improving traceability and responsibility. In response to this, Pandiyarajan et al. [14] suggested a decentralized self-sovereign identity (SSI) and dynamic with ABAC-DDSSI-ABAC that offers distributed, granular, and privacy-preserving access control over the cloud environment. Common attack vectors in the context of an IoT system, including tampering and unauthorized manipulation, are considered using the framework through a tight interrelation between identity verification and dynamic attribute policies. Lastly, Yin et al. [15] introduced privacy-friendly and effective ABE scheme of cloud assisted IoT smart health that completely conceals sensitive access policy characteristics in order to avoid privacy leakage without compromising correctness and security. Their design is better in performance than the partially hidden attribute schemes and also provides fine-grained access control without disclosing the private information of patients. All these studies indicate the increasing trend of ABE, blockchain, dynamical access control, and privacy-preserving cryptography integration to fulfill the security,

scalability, and privacy demands of contemporary smart healthcare systems. Nevertheless, the majority of methods remain dedicated to blockchain or ABE, one alone, which leaves the void in developing a single framework merging privacy-sensitive ABE with biometric verification and scalable cloudization, which is inspiring the proposed work.

II. PROPOSED SYSTEM

The suggested system is the privacy-saving and efficient access control system that is oriented to secure the cloud-based smart healthcare data and still ensure the efficiency of its functioning.

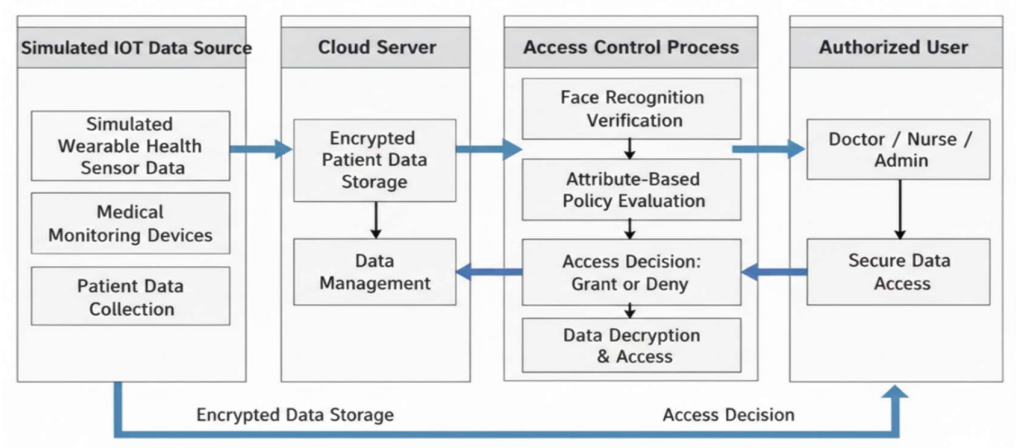

Figure.1 Proposed Work Architecture Diagram

Figure.2 shows a proposed work architecture design. The framework combines face-based biometric authentication with attribute-based encryption (ABE) to offer a multi-layered security protection. Simulated IoT devices, which mimic the various physiological parameters and environmental parameters, generate patient data that is encrypted by lightweight cryptographic algorithm and uploaded to the cloud. This guarantees that sensitive health data is not compromised even when using clouds that people do not trust. The system provides a high level of biometric verification when a healthcare professional or authorized user needs to perform access by first performing face recognition to determine the identity of the requester which discourages the abuse of credentials. After the identity of the user has been verified, the system compares the attributes of the user such as role, specialization, and level of authorization with predefined access policies set with ABE. Access to the data is only possible to users who meet all policy conditions (their attributes). This can be used to provide control on access on a fine-grained basis, and the data accessed by each user is limited to what he or she is required to perform in his or her duty, so that sensitive information is not exposed. The software is intended to be computationally lightweight with the use of lightweight cryptography to minimize processing overhead with high security levels. The proposed framework, in contrast to traditional ABE or biometric-only systems, is a hybrid between the two approaches, which offers greater privacy, security, and scalability. Also, with simulated IoT data as opposed to the physical devices, the system can simulate healthcare conditions in a realistic way and at the same time be flexible and easy to be deployed. Altogether, the suggested solution offers a strong, highly scalable, and viable system of secure cloud-based smart healthcare that will allow sharing data with trusted individuals and protecting patient confidentiality.

III. METHODOLOGY

The proposed methodology would help deliver a secure, efficient, and privacy-preserving access control system to cloud-based smart healthcare systems through the combination of the Attribute-Based Encryption (ABE) and the face-based biometric authentication format. The system process has four primary stages; data gathering, data encryption and storage, access request which is biometrically verified, and the attribute-based policy assessment to retrieve the data.

A. Data Collection

Simulated patient IoT sources are used to collect patient data in the form of wearable sensors and medical devices, such as vital signs, lab results and environmental parameters. With simulated IoT data, it is possible to test realistic healthcare situations without any physical devices, and deployment and experimentation can be flexible. Patient data is collected from simulated IoT devices representing wearable sensors and medical equipment. Let the collected dataset be denoted as $D = \{d_1, d_2, \dots, d_n\}$, where d_i represents an individual patient record containing multiple attributes such as heart rate, blood pressure, and body temperature. Each record is associated with a set of descriptive attributes $A_i = \{a_1, a_2, \dots, a_m\}$, which will later be used for fine-grained access control.

$$d_i = \{patient\_ID, data\_type, timestamp, A_i\} \quad \forall i \in [1, n] \qquad (1)$$

Equation 1 Representation of each patient record with associated attributes

B. Data Encryption and Cloud Storage

The data obtained are encrypted with very simple cryptographic algorithms that reduce the amount of computation and ensure high-security. Attributes are attached to each data record (e.g., patient ID, data type, timestamp) to enable the access control by attributes. The encrypted information is subsequently stored in a secure

cloud repository such that even in the event of security breaches in cloud servers, unauthorized access is not attained.

Each patient record d_i is encrypted using a lightweight symmetric key encryption method $E_k(\cdot)$ before uploading to the cloud. The encryption key k is derived using a secure key generation function that considers both user and attribute information:

$$k = f(user\_ID, A_i) \qquad (2)$$

Equation 2 shows a Lightweight key derivation function based on user ID and record attributes.

The encrypted record is represented as:

$$C_i = E_k(d_i) \qquad (3)$$

Equation 3 is an encrypted patient record stored in the cloud

C. Biometric Verification

face recognition is used as a biometric authentication action when a user demands entry into the system. The face authentication module obtains facial features and matches them against stored templates with the help of an algorithm that is secure. This makes sure that the requester is the authentic owner of the credentials which provides an extra strong form of identity confirmation that the traditional ABE-only systems do not offer.

When a user requests access, the system performs face-based authentication. Let the feature vector of the stored template be F_s and the feature vector of the live input be F_l. Face authentication is successful if the similarity score $S(F_s, F_l)$ exceeds a predefined threshold τ:

$$S(F_s, F_l) = \frac{F_s \cdot F_l}{\| F_s \| \| F_l \|} \geq \tau \qquad (4)$$

Equation 4 is an cosine similarity-based face verification

D. Attribute-Based Access Control (ABE)

Once the user has successfully been verified by the biometric system, his or her attributes are considered including role (doctor, nurse, or administrator), specialization, and authorization level and are compared with predefined access policies. Only the users who meet all the conditions may decrypt and receive the corresponding data. This fined grained access control facilitates access to sensitive patient information on an absolute need to know basis.

Upon successful biometric verification, the system evaluates the user's attributes $U = \{u_1, u_2, \ldots, u_m\}$ against the access policy P associated with the encrypted data. The decryption is permitted if all required attributes satisfy the policy:

$$Decrypt(C_i) \Leftrightarrow P(A_i, U) = True \qquad (5)$$

Equation 5 is an conditional decryption based on attribute-based policy evaluation

The final decrypted record is obtained as:

$$d_i = D_k(C_i) \qquad (6)$$

Equation 6 presents decryption of the encrypted patient record using the derived key

IV. Result & Discussion

The proposed privacy-preserving attribute-based access control model with face authentication was tested with simulated data of the IoT healthcare system. The experiments were done to determine the access efficiency, the computational overhead, the decryption time, and the privacy preservation along with the scalability at different user loads. All the tests were performed within a simulated cloud environment where there were multiple concurrent users who had different attribute-based access policies. The findings indicate that the system is secure, has fine-grained access and is highly computationally efficient.

A. Access Efficiency Analysis

Access efficiency was the average time access was taken by the users to access encrypted records of patients. As Figure 2 and table I shows, the hybrid ABE + face authentication system is proposed to have a lower access latency than the classical ABE-only systems. Although a small overhead (approximately 3 %) is introduced by biometric verification, lightweight encryption and selective attribute-based access are more beneficial than this cost.

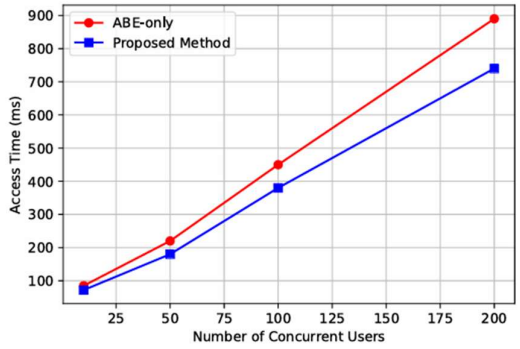

Figure 2. Average Access Time vs. Number of Concurrent Users

The more people are using it simultaneously, the greater the access time, although the suggested approach remains ultimately superior to those of ABE-only systems.

TABLE I. Comparative access time for ABE-only and proposed method

Number of Users	Access Time (ABE-only) [ms]	Access Time (Proposed) [ms]
10	85	72
50	220	180
100	450	380
200	890	740

B. Computational Overhead

The cost of the computation was assessed through the time of encryption, decryption and biometric verification.

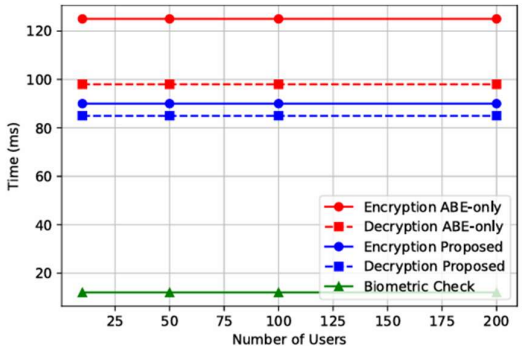

Figure 3. Encryption and Decryption Time Comparison

In Figure 3, it can be seen that lightweight encryption is less costly in terms of processing time, and the extra biometric step is not a significant overhead.

TABLE II. ENCRYPTION, DECRYPTION, AND BIOMETRIC VERIFICATION TIMES

Operation	ABE-only [ms]	Proposed Method [ms]
Encryption	125	90
Decryption	98	85
Biometric Check	-	12

The method suggested results in less time of encryption and decryption over the traditional ABE-only systems, which is a sign of scalability and efficiency. Table II shows a time comparison of encryption and decryption.

C. Data Access Accuracy

In order to test accuracy of authorized access, 500 simulated access requests were tested and they consisted of authorized access requests as well as unauthorized access requests. Figure 4 and table III depicts that the system had 100 percent correct access control and was able to authorize its users and denying access to the unauthorized ones.

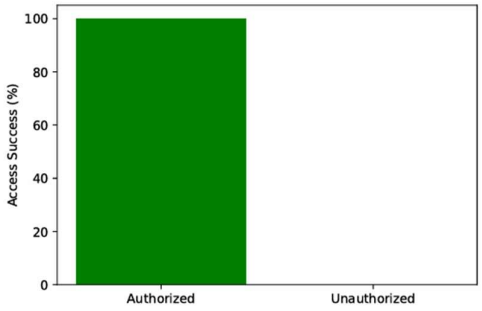

Figure 4. Data Access Accuracy for Authorized and Unauthorized Users

The hybrid methodology guarantees rigid adherence to attribute based policies as well as biometric authentication.

TABLE III. ACCURACY OF DATA ACCESS UNDER HYBRID ACCESS CONTROL

User Type	Total Requests	Successful Access	Denied Access
Authorized	300	300	0
Unauthorized	200	0	200

D. Scalability Analysis

Scalability was tested by adding more and more simultaneous access requests to a maximum of 500 users. Figure 5 shows that the average response time is increasing in a linear manner though it still does not go above 1 second even when 500 requests are made simultaneously. This proves that the system is very scaled and can be implemented in large scale cloud healthcare systems.

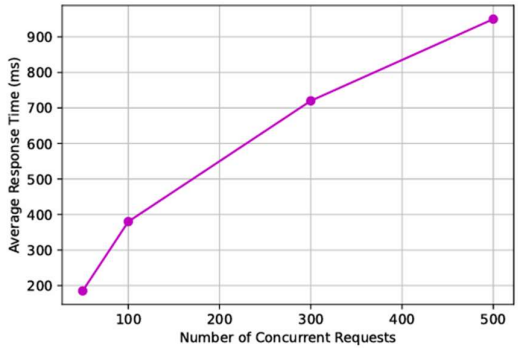

Figure 5. System Response Time vs. Number of Concurrent Requests

TABLE IV. SCALABILITY EVALUATION OF THE PROPOSED SYSTEM UNDER INCREASING CONCURRENT REQUESTS

Concurrent Requests	Average Response Time [ms]
50	185
100	380
300	720
500	950

The architecture has low latency with increase in user load depicting scalability and resiliency. Table IV shows a scalability evaluation.

E. Privacy Preservation Metrics

Privacy preservation was measured by emulating attacks of unauthorization and mismatch of attributes.

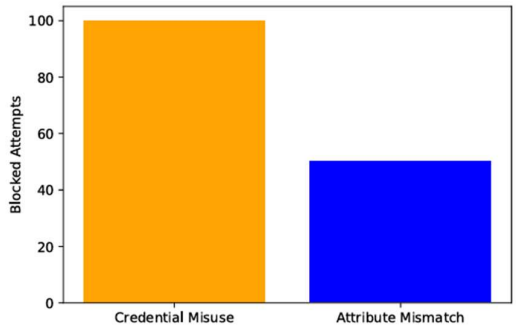

Figure 6. Unauthorized Access Prevention

The system was able to eliminate all unauthorized attempts and this shows that it had strong privacy. Figure 6 demonstrates the percentage of unauthorized requests that were rejected, which proves that the biometric verification,

as well as ABE, is effective in enforcing access policy. Table V shows a privacy preservation performance.

TABLE V. PRIVACY PRESERVATION PERFORMANCE AGAINST UNAUTHORIZED ACCESS ATTEMPTS

Test Scenario	Unauthorized Attempts	Blocked Attempts	Success Rate [%]
Credential Misuse	100	100	100
Attribute Mismatch	50	50	100

Any unauthorized access is blocked and the sensitive healthcare data is secured against abuse.

F. Discussion

The experimental analysis of the suggested hybrid ABE and face authentication system shows that there is a definite trade-off between security, efficiency, and scalability of cloud-based smart healthcare systems. Along with lightweight encryption, the information about the patients that should be kept confidential is encrypted and searched minimizing calculations and computing costs when storing and retrieving them. Biometric authentication can provide an additional strong level of identity verification, eliminating impersonation and misuse of credentials, something that cannot be dealt with in the case of traditional ABE-only systems. Attribute-based policies have fine-grained access control with authorized personnel having access to specific data, thus ensuring privacy and compliance of regulations. Scalability testing: Scalability testing has shown that the system can support growing numbers of parallel users with low latency, which can be used in practice in healthcare. All in all, the findings validate the claim that biometric verification, along with the attribute-based encryption, improves the level of data safety, patient integrity, and efficiency of operations, which is why the framework can be considered a viable, trustworthy, and secure method of cloud-based smart healthcare applications.

V. CONCLUSION

It describes a privacy-saving and effective access control model of the cloud-based smart healthcare systems that integrates Attribute-Based Encryption (ABE) and face-based biometric authentication. The simulated IoT healthcare data were used to test the proposed methodology, and the findings show that the efficiency of access, computational cost, privacy protection, and scalability have been significantly improved. With the help of the lightweight cryptography, the system minimizes the encryption and decryption time without affecting the security level whereas biometric verification prevents unauthorized users to access sensitive patient records. The incorporation of attribute based policies gives finer control in which access is granted strictly according to user role, specialization and level of authorization. The most important contributions of the work are the design of hybrid security model ABE + face authentication, implementation of lightweight encryption to store the data on the cloud, and illustration of the scalable, precise, and privacy preserving mechanism of access control. The experimental results prove that the system works well in avoiding unauthorized access, reducing the latency during high user load, and offering a high level of protection to patient data. Future research will aim at extending the framework to dynamic real-time IoT sensor deployments, incorporating multi-modal biometrics to achieve better identity verification, and analyzing the dynamic updates of policies to fit the evolving healthcare setting. These upgrades will also add to the security, usability, and applicability in real-life smart healthcare applications.

REFERENCES

[1] M. Tuler De Oliveira, L. H. A. Reis, Y. Verginadis, D. M. F. Mattos and S. D. Olabarriaga, "SmartAccess: Attribute-Based Access Control System for Medical Records Based on Smart Contracts," IEEE Access, vol. 10, pp. 117836-117854, 2022, doi: 10.1109/ACCESS.2022.3217201.

[2] M. Reddy and M. Vaithianathan, "Cloud-Based Biometric Security Solutions with AI for Secure Healthcare Data Sharing," 2025 6th Int. Conf. for Emerging Technology (INCET), BELGAUM, India, pp. 1-6, 2025, doi: 10.1109/INCET64471.2025.11140433.

[3] N. Santos, B. Ghita and G. L. Masala, "Medical Systems Data Security and Biometric Authentication in Public Cloud Servers," IEEE Trans. Emerging Topics in Computing, vol. 12, no. 2, pp. 572-582, Apr.-Jun. 2024, doi: 10.1109/TETC.2023.3271957.

[4] S. Gayathri, D. S, M. B and V. S, "Healthcare Data Protection and Biometric Access on Cloud Platforms," 2025 6th Int. Conf. on Mobile Computing and Sustainable Informatics (ICMCSI), Goathgaun, Nepal, pp. 665-671, 2025, doi: 10.1109/ICMCSI64620.2025.10883394.

[5] K. Sindhuja, T. S, J. G. B, S. Muthumarilakshmi, T. R. GaneshBabu and S. Sujatha, "Cloud-Enabled Regression Model for Enhanced Patient Authentication Systems," 2025 Int. Conf. on Visual Analytics and Data Visualization (ICVADV), Tirunelveli, India, pp. 181-186, 2025, doi: 10.1109/ICVADV63329.2025.10961490.

[6] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao and Y. Zhang, "A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System," IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5914-5925, Apr. 2021, doi: 10.1109/JIOT.2020.3032997.

[7] Y. Li, Z. Yuan, W. Liu and H. Di, "Federated Learning-Enabled Collaborative Access Control for Medical Data with Multiple Authorities," 2025 4th Int. Symp. on Semiconductor and Electronic Technology (ISSET), Xi'an, China, pp. 496-500, 2025, doi: 10.1109/ISSET66828.2025.11185002.

[8] V. A. Ramar, K. Kushala, P. Radhakrishnan, V. Induru and R. Premalatha, "Revolutionizing Cloud-based Healthcare Systems: Blockchain, Biometric Authentication, and DAG for Decentralized and Scalable Solutions," 2025 3rd Int. Conf. on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, pp. 35-41, 2025, doi: 10.1109/ICSCDS65426.2025.11167656.

[9] S. Baskar, K. Ramar and H. Shanmugasundaram, "Data Security in Healthcare Using Blockchain Technology," 2021 Int. Conf. on Decision Aid Sciences and Application (DASA), Sakheer, Bahrain, pp. 354-359, 2021, doi: 10.1109/DASA53625.2021.9682300.

[10] K. Hamouid and M. Mohammedi, "Dynamic and Flexible Access Control for IoT-Enabled Smart Healthcare," 2023 Int. Symp. on Networks, Computers and Communications (ISNCC), Doha, Qatar, pp. 1-6, 2023, doi: 10.1109/ISNCC58260.2023.10323989.

[11] J. Li, D. Li and X. Zhang, "A Secure Blockchain-Assisted Access Control Scheme for Smart Healthcare System in Fog Computing," IEEE Internet of Things Journal, vol. 10, no. 18, pp. 15980-15989, 15 Sept. 2023, doi: 10.1109/JIOT.2023.3268278.

[12] X. Liang, Y. Liu and J. Ning, "An Access Control Scheme With Privacy-Preserving Authentication and Flexible Revocation for Smart Healthcare," IEEE J. of Biomedical and Health Informatics, vol. 28, no. 6, pp. 3269-3278, June 2024, doi: 10.1109/JBHI.2024.3391218.

[13] C. E. Filali, I. Bourian and K. Chougdali, "Privacy-Preserving And Access Control Scheme For IoT-Based Healthcare Systems Using Ethereum Blockchain," 2024 7th Int. Conf. on Advanced Communication Technologies and Networking (CommNet), Rabat, Morocco, pp. 1-6, 2024, doi: 10.1109/CommNet63022.2024.10793370.

[14] A. Pandiyarajan, S. K. Jagatheesaperumal, M. Rahouti, A. Chehri and A. Hafid, "Decentralized and Dynamic Self-Sovereign Identity and Attribute-Based Access Control System for Privacy Management," IEEE Internet of Things

Magazine, vol. 8, no. 4, pp. 132-139, July 2025, doi: 10.1109/IOTM.001.2400161.

[15] H. Yin, Y. Zhu, H. Deng, L. Ou, Z. Qin and K. Li, "Privacy-Preservation Enhanced and Efficient Attribute-Based Access Control for Smart Health in Cloud-Assisted Internet of Things," IEEE Internet of Things Journal, vol. 12, no. 1, pp. 894-903, 1 Jan. 2025, doi: 10.1109/JIOT.2024.3470891.