

A secure and cloud-based patient management system using attribute-based encryption algorithm

Senthilkumar Kalarani¹, Mahalingam Shobana², Edamakanti Uma Shankari³, Bolly Joshi Praveena⁴, Subramaniam Shanthi⁵, Rathinasabapathy Ramadevi⁶, Rajendar Sandiri⁷

¹Department of Computer Science and Engineering, PSG Institute of Technology and Applied Research, Coimbatore, India

²Department of Computer Science and Engineering, Saveetha Engineering College, Thandalam, India

³Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, India

⁴Department of Computer Science and Engineering, Matrusri Engineering College, Hyderabad, India

⁵Department of Computer Science and Engineering, Kongu Engineering College, Erode, India

⁶Department of Biomedical Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Thandalam, India

⁷Department of Electronics and Communication Engineering, Vardhaman College of Engineering, Hyderabad, India

Article Info

Article history:

Received Mar 16, 2024

Revised Sep 19, 2024

Accepted Oct 1, 2024

Keywords:

Attribute-based encryption

Cloud-based patient management

Data privacy

Regulatory compliance

Scalability

ABSTRACT

Using attribute-based encryption (ABE), cloud-based patient management systems may be made more secure and efficient. The goal is to provide a scalable encryption infrastructure with dynamic attribute handling and context-aware access control for safe data access. Encryption procedures should directly comply with regulatory criteria to secure healthcare data and ensure data privacy and integrity. Secure attribute issuance and revocation are achieved using advanced key management and real-time auditing and monitoring to identify and react to unauthorized access. To help healthcare providers handle data, user-centric security measures including extensive training and adaptive security procedures are used. The encryption system is implemented and maintained using cost-effective cloud and open-source methodologies to ensure seamless integration and operational effectiveness in healthcare contexts. First, secure patient management system dataset results reveal ABE algorithm encryption. The encrypted values are 8F5D6A..., 7C4A3B..., 6E3B2C..., 9D8A7B..., 5E4D3C.... in the second instance, derived from role-based access control of ABE. The patients are 25-60 years old, have medical codes 101-105, 201-205, and 301-305. For roles from different fields, attribute code is 401-406, level code is 501-505.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Senthilkumar Kalarani

Department of Computer Science and Engineering, PSG Institute of Technology and Applied Research
Coimbatore, India

Email: kala.rani1971@gmail.com

1. INTRODUCTION

Cloud computing has transformed healthcare patient data management by improving accessibility, scalability, and efficiency. Cloud computing also raises data security and privacy concerns. Protecting sensitive patient data is crucial [1]. The attribute-based encryption (ABE) algorithm offers a safe and fine-grained cloud access control architecture that addresses these issues. Security and efficiency are the main goals of attribute-based encryption in cloud-based patient management systems. This method protects sensitive patient data while preserving cloud computing's accessibility and scalability [2]. ABE is used to provide a secure environment that supports the complex and dynamic nature of healthcare data management, guaranteeing that only authorized users with the right credentials may access patient data.

The main goal is to create an encryption infrastructure that integrates ABE to safeguard patient data. This requires a system that can change access control restrictions depending on patient characteristics in real time. The goal is to provide an encryption system that manages big patient data volumes and many access requests without sacrificing speed [3]. Another goal is to provide fine-grained permissions depending on patient traits and context. This aim includes complying with health insurance portability and accountability act (HIPAA) and implementing safe cryptographic key issuance, revocation, and management policies.

ABE's capabilities should be used to construct a secure and efficient cloud-based patient management system. This system restricts sensitive patient data to authorized persons with valid credentials to protect data privacy. It aims to integrate with healthcare systems and processes without disrupting operations. Establishing continuous monitoring to identify and react to unauthorized access attempts quickly is also important. To achieve this goal, healthcare providers must receive comprehensive training and tools to manage patient data within the ABE framework, and cost-effective strategies that use cloud resources and open-source solutions to optimize implementation and maintenance costs are essential [4].

ABE deployment of a cloud-based patient management system includes development, installation, and assessment. This comprises system architecture and ABE integration with current infrastructure. Controlling how access control rules are generated, maintained, and dynamically updated depending on patient characteristics is critical. Optimizing encryption and decryption to reduce latency and preserve system responsiveness is another priority. The scope includes embedding compliance measures in the encryption framework to fulfil all applicable healthcare legislation and establishing training programs and support tools to help healthcare professionals adjust to the new system [5].

ABE in a cloud-based patient management system solves security issues by using this encryption technology creatively. This work allows real-time access control policy adjustments, improving system flexibility and responsiveness. Creating an encryption system that handles massive datasets and many access requests is crucial. Fine-grained access restrictions that account patient traits and context increase data security. Integrating regulatory compliance with encryption enables healthcare data protection compliance. Security and efficiency in cryptographic key and patient attribute management lower the danger of unauthorized access. These areas are addressed to improve cloud-based patient management system security, efficiency, and dependability, improving healthcare data management and patient care results. Section 2 introduces the attribute-based encryption algorithm, while section 3 discusses its significance to cloud-based patient management system. Section 4 describes cloud-based patient management system results. Section 5 ends with conclusion.

2. LITERATURE SURVEY

Healthcare data privacy problems are often addressed using ABE. ABE provides privacy and security with fine-grained access control and integrity protection. ABE features structural efficiency, including faster key generation, computation time, fewer key pairs, and collision resistance [6]. Medical practitioners and patients use medical social networks. It mixes medical information and social interaction to make medical services and health management easier and more personalized. Besides information sharing, medical social networks may increase doctor-patient engagement and give personalized medical advice [7]. A computationally comprehensive hybrid-based health care system architecture based on attribute encryption is offered for scalable, cost-effective patient access to personal, health, and medical data. Updated attribute-based encryption improves access control. Healthcare data protection requires safe, dependable data exchange [8]. Each user receives a private key that matches an access policy, and every encrypted communication is connected to characteristics in key policy attribute-based encryption (KP-ABE). It lets users decode just ciphertext that fits their private key access policy. The ciphertext-policy attribute-based encryption (CP-ABE) technique links a user's private key to characteristics, and each encrypted communication has an access structure depending on specified attributes [9].

Many cloud-based attribute-controlled electronic health record (EHR) systems have been developed; however, most struggle with data expansion and heterogeneous data. These systems store patient data in relational databases or knowledge graphs and flat files with defined structure, which causes issues [10]. Open key encryption algorithm ABE uses a client-side secret key and characteristics to encode the ciphertext. In ABE, numerical characteristics were used in ciphertext to send the message. The public-key will be saved as a string for length calculation after encryption. Decoding included arranging characteristics with the ciphertext and private key [11]. ABE lets users choose to decrypt data based on properties and regulations. ABE generalizes public key encryption for granular data management. With ABE, logs may be encrypted. ABE, a public key cryptography scheme, allows safe data exchange between numerous users [12]. Patient privacy and medical data interchange may be protected using proxy re encryption, ABE, and classic encryption methods. An effective setup and sharing approach with ABE may address the private data sharing problem [13].

Using ciphertext-policy attribute-based encryption, attribute-based multi-keyword search allows fine-grained access control and multi-keyword search. Formal security studies show the recommended method is secure against chosen-keyword attacks [14]. This solution protects CP-ABE's security characteristics, according to extensive testing. Each property is evaluated and assigned a weight before safe cloud sharing. The qualities of this technology make it more efficient and successful than other cloud-based data sharing options [15]. The proposed safe cloud access method uses quantum key distribution (QKD) and attribute-based cryptography (ABC) to increase cloud data security. QKD was used with ABC to protect ABC against quantum computing attacks. ABC controls access and secrecy but is susceptible to quantum attacks since it uses classical cryptography [16]. Medical staff attribute management is crucial for system security and flexibility. The system must provide real-time attribute revocation so medical staff who no longer fulfil access control cannot access the original EHR. Two types of CP-ABE attribute revocation techniques exist: direct and indirect [17].

AC-AC combines dynamic index-based symmetric searchable encryption with ciphertext-policy attribute-based encryption. Based on the MicroSCOPE protocol, the new protocol uses scope values to grant and revoke access permissions for acute care practitioners [18]. Quantum hash-based attribute-based encryption (QHABE) addresses and overcomes past shortcomings. Secret data may be encrypted using cryptographic technologies that provide flexible access control. ABE approaches, including extended attribute-based encryption, protect cloud server data and enable encrypted data searches [19]. A CP-ABE system was suggested to secure, disseminate, and control information. Due to common facilities, misconfigurations exposed all client data in the cloud. Cyberattack-resistant cloud-computing security architecture is difficult [20]. This is addressed by ABE's fine-grained access control mechanisms. Identity-based encryption (IBE) techniques, such as fuzzy identity binary encryption (FIBE), preceded ABE [21].

In recent years, academics have approved attribute-based honey encryption (ABHE) for its capacity to protect against attackers. These decoy cypher messages direct attackers to a different plaintext, giving extra security. Data may be encrypted with characteristics like a person or group that should have access via ABHE. This attribute-based honey encryption approach allows fine-grained cloud data access [22]. Further study is needed on user authentication. To offer optimum telemedicine treatment, patients, healthcare professionals, and administrative personnel need patient data. Only authorized workers should access patient data to protect privacy and security [23]. Users with the right attributes may decode the ciphertext to access the electronic medical records (EMR). Cloud-based EMR systems improve data security and enable genuine users to access data from anywhere, preventing data abuse [24]. Cryptography is a way to alter important information into something useless and then back again using the same key. Examples of multi-method encryption and decryption include symmetric-encryption (SE), asymmetric-encryption (AE), and attribute-based encryption (ABE) [25].

EHR data may be safely shared in the public cloud using revocable-storage hierarchical attribute-based encryption (RS-HABE) and permission architecture. The suggested method solves user revocation, keystroke delegation, and ciphertext update security issues. Guo *et al.* [26] developed the RS-HABE technique to provide advance and reverse security of encoded EHR data and let clients to build unique private keys for their children. Patient-directed attribute-based access and encryption provide selective disclosure of required data fields. Interoperability and secrecy may be accomplished using privacy-enhancing technology. Access controls may limit data access to authorized users using role-based, attribute-based, and multi-factor authentication [27]. The input training set properties are used to statistically classify personal health records (PHRs). The authorized set of characteristics relates to rows and columns by sharing the created matrix key locally via cypher text appended by cloud service providers. Simple Bayesian networks require conditional independence among class characteristics, which is unworkable. Bayesian categorization loses information when domain partitioning is sharp. In health care, fuzzy logic fuzzifiers health characteristics to solve this problem. Since healthcare data is huge data, speed should be considered [28]. Strong access controls regulate healthcare file access. Access is usually controlled by roles, permissions, and attributes using role-based access control (RBAC) and attribute-based access control (ABAC). These techniques restrict data access and manipulation to authorized users [29]. Two private and mutual authentication procedures prioritize privacy with a three-message attribute-based encryption key exchange mechanism and a one-round protocol for simplicity and speed [30].

3. METHOD

3.1. Secure dental records with attribute-based encryption for cloud patient management

When it comes to safe cloud-based electronic dental records and sophisticated encryption, ABE methods are crucial for simplified patient administration. Modern digital healthcare requires new ways to protect patient data. The dentistry industry discusses integrating ABE algorithms into electronic record systems to improve patient data protection and administration. This framework uses ABE to provide

attribute-based access control for granular and dynamic data security. ABE and secure cloud technologies improve data accessibility and confidentiality for authorized users. We explore the potential of ABE algorithms to improve electronic dental record security and create a robust and efficient patient management ecosystem in the digital era. Many forms of ABE encryption schemes are shown in Figure 1.

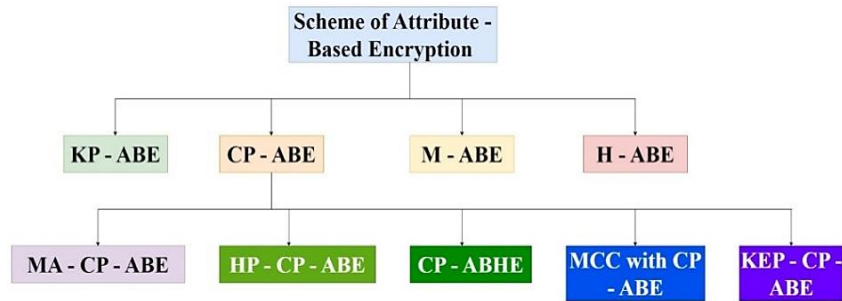


Figure 1. Different types of ABE schemes

3.2. Secure cloud-based electronic dental records with attribute-based encryption algorithms for streamlined patient management

Patient privacy is crucial in electronic dental records (EDRs). This article discusses how ABE algorithms secure cloud-based EDR systems. ABE's advanced encryption method permits access to sensitive patient data depending on predetermined criteria, providing nuanced data security. Dental healthcare providers may utilize ABE algorithms to set fine-grained access limits based on user roles and patient information. This improves data privacy and facilitates patient administration, expanding dental practice efficiency. The essay highlights how ABE algorithms in cloud-based EDR systems protect patient data and provide a secure digital healthcare environment. Data generators have greater control with CP-ABE systems since access permission is chosen during data encryption. Figure 2 show KP-ABE. These algorithms are used by any KP-ABE scheme: 1. Setup (Sec) (MK, P). This method produces a random master key MK and public parameters P, initializes the scheme with Sec strength, and returns them.

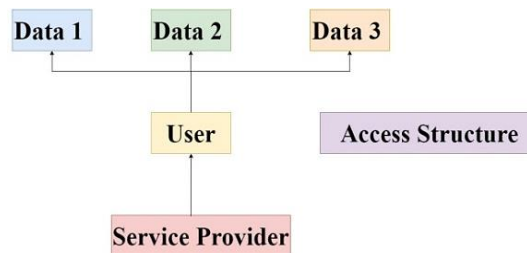


Figure 2. Scheme diagram of KP-ABE

3.3. Innovative attribute-based encryption algorithms improve cloud-based electronic dental record security

The growing digitalization of healthcare data, especially EDRs, requires strong security measures to secure sensitive patient data. Cloud-based dental record security and confidentiality are discussed in this article. This study tackles dental patient management's changing environment utilizing ABE techniques. Access management and confidentiality are simplified by ABE algorithms for dynamic healthcare processes. ABE in EDRs improves data security and streamlines user access control, enabling healthcare provider cooperation. Beyond safe data storage, cloud-based ABE makes dental operations more adaptive and scalable for patient data management. This research examines how ABE algorithms may modify safe electronic dental record frameworks. Data generators have greater control with CP-ABE systems, since access permission is selected during data encryption. Both CP-ABE are in Figure 3. These algorithms are used by any KP-ABE scheme: 1. (MK, P)=Setup (Sec). This method produces a random master key MK and public parameters P, initializing the scheme with Sec's security strength and returns them.

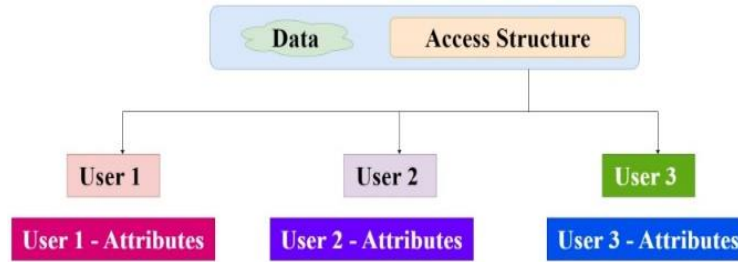


Figure 3. Diagram of the CP-ABE scheme

3.4. Comparative analysis of attribute-based encryption algorithms for dental records security

Protecting patient data in EDRs is crucial. This paper examines safe cloud-based EDR frameworks, concentrating on ABE methods. Access based on certain qualities simplifies patient care using ABE, reducing data exposure risk. Different ABE algorithms affect secure EDR system efficiency and resilience in this comparative study. Their merits, drawbacks, and performance indicators help choose the best algorithm for data security and accessibility. This work intends to improve cloud-based EDR privacy and reliability in fast-changing dental healthcare by illuminating ABE algorithm differences. Addressing these problems is essential for effective ABE deployment in internet of thing (IoT) settings. Proper design and execution of ABE may efficiently handle access control and improve data security and privacy in the IoT. Figure 4 illustrates the potential and obstacles of using ABE in IoT.

Table 1 show that key policy attribute-based encryption (KP-ABE), ciphertext-policy attribute-based encryption (CP-ABE), multi-authority attribute-based encryption (MA-ABE), and predicate encryption with attribute-based access control (PE-ABAC) protect data differently. KP-ABE and CP-ABE restrict access finely, MA-ABE controls authorities well, and PE-ABAC is versatile. These algorithms improve patient management in secure cloud-based electronic dental records by enabling customizable access control, scalability, and expressive rules.

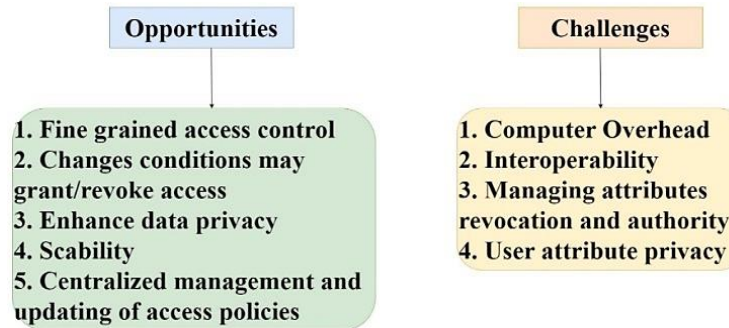


Figure 4. ABE IoT opportunities and problems

Table 1. Attribute-based encryption algorithms for streamlined patient management in secure cloud-based electronic dental records framework

| Aspect | Role | Benefit | Function |
|--|---|--|--|
| Key policy-attribute based encryption | Ensures data confidentiality | Provides fine-grained access control, allowing only authorized users to decrypt and access specific patient information | Encrypts based on predefined attributes |
| Ciphertext policy-attribute based encryption | Facilitates access control | Offers flexible and dynamic access policies, adapting to changing requirements without modifying the encryption scheme | Encrypts data with policies defined in terms of attributes |
| Multi-authority attribute-based encryption | Manages attribute authorities efficiently | Enhances scalability by allowing multiple authorities to independently manage and issue attributes, ensuring a robust system | Distributes attribute issuance in a decentralized manner |
| Predicate encryption with attribute-based access control | Combines attribute-based access control with predicate encryption | Enables expressive access policies, allowing complex conditions for data access, providing a high level of flexibility and control | Offers a versatile approach to data protection by combining attribute-based access control with predicate encryption |

4. RESULTS AND DISCUSSION

4.1. Secure dental records with policy attribute-based encryption in cloud frameworks

Maintaining the security and integrity of electronic dental information is crucial in modern healthcare systems. This discusses KP-ABE and how it improves cloud-based electronic dental record security. As healthcare organizations use digital systems for patient management, data access must be fast and safe. The revolutionary KP-ABE system allows attribute-based access control rules to restrict critical patient data to authorized users with specified credentials. This paper examines attribute-based encryption algorithms in dental records and their effectiveness in protecting patient data. By understanding this encryption paradigm, the dentistry sector can create a secure electronic records framework that builds confidence and meets growing data protection standards. Using the ABE technique, a secure patient management system may encrypt data as shown in Figure 5. The collection contains encrypted values for characteristics such as patient ID, age, medical history code, diagnosis code, and treatment code. To make sure that only those with the right qualities may access the data, the ABE algorithm generates these values. Patient data kept in the cloud is now more secure because of this.

The ABE algorithms KP-ABE, CP-ABE, MA-ABE, and PE-ABAC are crucial to protect cloud-based electronic dental records in Table 2. Each has unique hurdles, such as key management and policy complications, yet they all simplify patient management. These algorithms are used for access control, dental data sharing, cross-institutional data sharing, and dynamic patient attribute control. Granular access control, flexible rules, decentralized administration, and fast attribute handling improve dental record management security and cooperation.

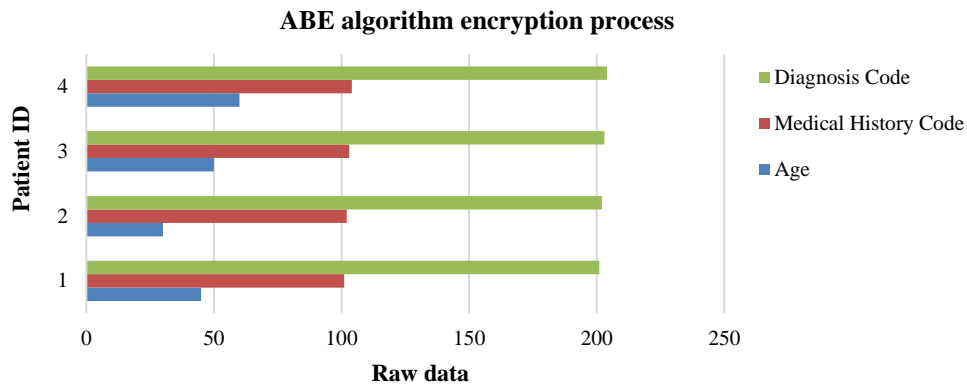


Figure 5. ABE algorithm encryption process

Table 2. Enhancing patient management in secure cloud-based electronic dental records through attribute-based encryption algorithms

| Aspect | Challenges | Application | Advantages |
|---------|---------------------------------|--|---|
| KP-ABE | Complex key management | Access control in dental records | Granular access, fine-grained control |
| CP-ABE | Policy complexity | Data sharing among dental professionals | Flexible access policies, enhanced collaboration |
| MA-ABE | Multiple authority coordination | Cross-institutional patient data sharing | Decentralized management, interoperability |
| PE-ABAC | Predicate complexity | Dynamic patient attribute control | Efficient attribute handling, adaptive access control |

4.2. Improved cloud-based electronic dental record security with ciphertext policy attribute-based encryption algorithms

Advanced cryptography is essential for safe healthcare information management. CP-ABE is integrated with secure cloud-based electronic dentistry records to protect patient confidentiality and comply with privacy laws. This explores attribute-based encryption methods and their significance in improving electronic dental record system security, enabling a resilient and privacy-conscious healthcare environment. Figure 6 shows how the patient management system incorporates ABE and RBAC. The dataset contains information about roles, including their IDs, names, attribute codes, and access level codes. Levels of access are determined by the qualities granted to each position. This keeps the patient data secure and private by limiting access to just those people who have the proper responsibilities and qualities.

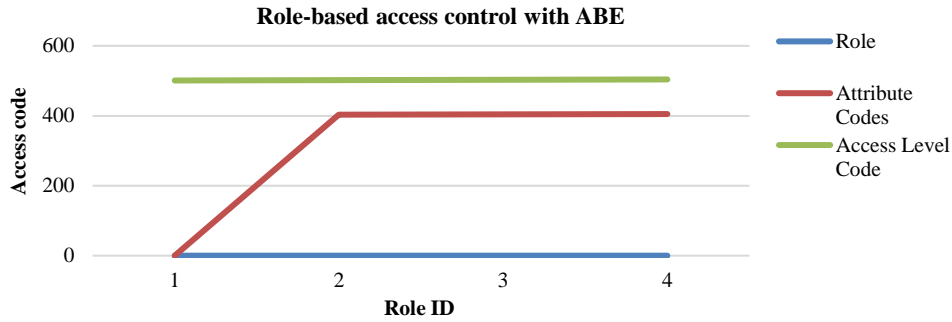


Figure 6. Role-based access control with ABE

4.3. Enhancing cloud dental record management security: predicate encryption with attribute-based access control

A new technique employs attribute-based encryption algorithms to ease patient administration in the ever-changing dental healthcare business. When sensitive data is digitalized, PE-ABAC leads in confidentiality and access control. This outlines how attribute-based encryption secures dental records for easy management and patient privacy. The PE-ABAC research shows that cloud-based frameworks can transform electronic dental record systems. While the dental healthcare industry struggles with data management, this research evaluates PE-ABAC's practical effects and benefits for electronic dental record administration security and efficiency. Table 3 shows how attribute-based encryption might improve a cloud-based patient management system.

Table 3. Enhancing a secure and cloud-based patient management system with attribute-based encryption

| Aspect | Problem statement | Proposed solution | What is new |
|----------------------------------|--|--|---|
| Dynamic attribute handling | Managing dynamic changes in patient attributes and access policies over time is challenging. | Implement dynamic attribute management capabilities for real-time updates in access policies. | Introduces dynamic attribute handling, allowing immediate adjustments in access control policies based on evolving patient data and organizational needs. |
| Scalable encryption architecture | Efficiently managing large volumes of patient data and access requests without performance degradation. | Develop a scalable encryption infrastructure to handle increasing data volumes while maintaining performance. | Introduces a scalable encryption architecture designed for efficient management of large data volumes, ensuring consistent system performance and security. |
| Context-aware access control | Need for fine-grained access control based on specific patient attributes and contextual factors. | Implement context-aware access control mechanisms for precise permissions based on patient attributes and context. | Introduces context-aware access control, enabling granular permissions based on patient attributes and contextual factors, enhancing data security and access management. |
| Integrated regulatory compliance | Ensuring seamless adherence to healthcare data protection regulations (e.g., HIPAA) in encryption practices. | Embed regulatory compliance standards into attribute-based encryption policies and practices. | Integrates regulatory compliance directly into encryption policies, ensuring adherence to healthcare data protection laws without additional administrative burden. |
| Enhanced key management | Securely managing attribute issuance, revocation, and cryptographic key lifecycle in encryption processes. | Utilize advanced key management practices tailored for attribute-based encryption systems. | Enhances key management with secure attribute issuance, revocation processes, and lifecycle management, ensuring robust data security and access control management. |
| Real-time audit and monitoring | Providing continuous visibility into access to patient records for proactive detection of unauthorized activities. | Deploy real-time auditing and monitoring capabilities for immediate detection and response to security incidents. | Implements real-time audit and monitoring capabilities to enhance security by detecting and responding promptly to unauthorized access attempts and potential breaches. |

It highlights crucial issues such handling dynamic patient characteristics, scalability of encryption infrastructure, and fine-grained access control based on patient attributes and regulatory compliance. Dynamic attribute handling for real-time policy changes, scalable encryption structures, and context-aware access control are suggested. The direct integration of regulatory compliance into encryption processes, improved key management for safe attribute handling, and real-time audits to improve data security distinguish this approach. User-centric security, adaptive security protocols, interoperability improvements,

and cost-effective deployment methodologies emphasize a holistic approach to enhancing healthcare data protection, operational efficiency, and compliance. These advances improve system efficiency and usability for healthcare providers and administrators while ensuring data security, regulatory compliance, and seamless integration.

5. CONCLUSION

Using the ABE method to create a secure, cloud-based patient management system requires managing dynamic attributes, scalability, and seamless integration with current healthcare systems. These challenges may affect system performance, data security, and user acceptance. Complex key management, latency concerns, and significant training may reduce encryption system efficiency. Implementing ABE improves data privacy, regulatory compliance, and fine-grained access control, which protects sensitive patient data. More advanced encryption techniques to decrease computational cost and delay are planned. Data interchange across healthcare systems will be easier with improved interoperability. Continuous improvements in adaptive security and real-time monitoring will boost the system's resistance against new cyber threats, assuring data safety and operational efficiency in the changing healthcare data management scenario. First, Secure Patient Management System Dataset results reveal ABE Algorithm Encryption. The encrypted values are 8F5D6A..., 7C4A3B..., 6E3B2C..., 9D8A7B..., 5E4D3C... in the second instance, derived from role-based access control of ABE. The patients are 25-60 years old, have medical codes 101-105, 201-205, and 301-305. For roles from different fields, attribute code is 401-406, level code is 501-505.





REFERENCES

- [1] T. R. Saravanan, A. R. Rathinam, J. Lenin, A. Komathi, B. Bharathi, and S. Murugan, "Revolutionizing cloud computing: evaluating the influence of blockchain and consensus algorithms," in *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, Dec. 2023, vol. 7, pp. 1–6, doi: 10.1109/SMARTGENCON60755.2023.10442008.
- [2] M. J. Kumar, S. Mishra, E. G. Reddy, M. Rajmohan, S. Murugan, and N. A. Vignesh, "Bayesian decision model based reliable route formation in internet of things," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 34, no. 3, pp. 1665-1673, Jun. 2024, doi: 10.11591/ijeecs.v34.i3.pp1665-1673.
- [3] A. R. Rathinam, B. S. Vathani, A. Komathi, J. Lenin, B. Bharathi, and S. Murugan, "Advances and predictions in predictive auto-scaling and maintenance algorithms for cloud computing," in *2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS)*, Dec. 2023, pp. 395–400, doi: 10.1109/ICACRS58579.2023.10404186.
- [4] M. D. A. Hasan, K. Balasubadra, G. Vadivel, N. Arunfred, M. Ishwarya, and S. Murugan, "IoT-driven image recognition for microplastic analysis in water systems using convolutional neural networks," in *2024 2nd International Conference on Computer, Communication and Control (IC4)*, Feb. 2024, pp. 1–6, doi: 10.1109/IC457434.2024.10486490.
- [5] M. Amru *et al.*, "Network intrusion detection system by applying ensemble model for smart home," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 3, pp. 3485-3494, Jun. 2024, doi: 10.11591/ijece.v14i3.pp3485-3494.
- [6] R. Walid, K. P. Joshi, and S. G. Choi, "Comparison of attribute-based encryption schemes in securing healthcare systems," *Scientific Reports*, vol. 14, no. 1, p. 7147, Mar. 2024, doi: 10.1038/s41598-024-57692-w.
- [7] J. Li, "Attribute based signature encryption scheme based on cloud computing in medical social networks," *Journal of Cyber Security and Mobility*, pp. 517–540, Apr. 2024, doi: 10.13052/jcsm2245-1439.1338.
- [8] T. Suneetha and D. J. Bhagwan, "A secure framework for enhancing data privacy and access control in healthcare cloud management systems," *Educational Administration Theory and Practices*, May 2024, doi: 10.53555/kuey.v30i5.5783.
- [9] X. Li, H. Wang, S. Ma, M. Xiao, and Q. Huang, "Revocable and verifiable weighted attribute-based encryption with collaborative access for electronic health record in cloud," *Cybersecurity*, vol. 7, no. 1, p. 18, Mar. 2024, doi: 10.1186/s42400-024-00211-1.
- [10] R. Walid, K. P. Joshi, and S. G. Choi, "Leveraging semantic context to establish access controls for secure cloud-based electronic health records," *International Journal of Information Management Data Insights*, vol. 4, no. 1, p. 100211, Apr. 2024, doi: 10.1016/j.ijime.2023.100211.
- [11] Y. Mahi Gayathri and K. S. Rekha, "Comparative analysis of identity-based-broadcast encryption with attribute-based encryption for reduced storage cost of multi users in a public cloud," in *AIP Conference Proceedings*, 2024, vol. 2729, p. 030001, doi: 10.1063/5.0168813.
- [12] A. Binbusayyis *et al.*, "A secured cloud-medical data sharing with a-BRSA and salp-ant lion optimisation algorithm," *CAAI Transactions on Intelligence Technology*, May 2024, doi: 10.1049/cit2.12305.
- [13] Z. Sultana and D. Kumar, "Medical data privacy representation with improved encryption algorithm," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 8, pp. 581–591, 2023.
- [14] M. N. Jayakumar and J. Samraj, "Secure medical sensor monitoring framework using novel hybrid encryption algorithm driven by internet of things," *Measurement: Sensors*, vol. 33, p. 101122, Jun. 2024, doi: 10.1016/j.measen.2024.101122.
- [15] K. Sravanthi and P. C. Sekhar, "An efficient integrity verification based multi-user cloud access control framework using block chain technology on EHR database," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 9, p. 536, 2023.
- [16] U. Nauman, Y. Zhang, Z. Li, and T. Zhen, "Q-ECS: quantum-enhanced cloud security with attribute-based cryptography and quantum key distribution," *Research Square Platform LLC*, Mar. 13, 2024, doi: 10.21203/rs.3.rs-4006533/v1.
- [17] J. Qiao, N. Wang, J. Fu, J. Wang, J. Liu, and L. Deng, "A lightweight cp-ABE scheme for EHR over cloud based on blockchain and secure multi-party computation." Elsevier BV, 2024, doi: 10.2139/ssrn.4769328.
- [18] A. Haddad, M. H. Habaebi, E. A. A. Elsheikh, M. R. Islam, S. A. Zabidi, and F. E. M. Suliman, "E2EE enhanced patient-centric blockchain-based system for EHR management," *PLOS ONE*, vol. 19, no. 4, p. e0301371, Apr. 2024, doi: 10.1371/journal.pone.0301371.





- [19] K. K. Singamaneni, G. Muhammad, and Z. Ali, "A novel quantum hash-based attribute-based encryption approach for secure data integrity and access control in mobile edge computing-enabled customer behavior analysis," *IEEE Access*, vol. 12, pp. 37378–37397, 2024, doi: 10.1109/ACCESS.2024.3373648.
- [20] K. Pradeep Kumar, B. R. Prathap, M. M. Thiruthuvanathan, H. Murthy, and V. Jha Pillai, "Secure approach to sharing digitized medical data in a cloud environment," *Data Science and Management*, vol. 7, no. 2, pp. 108–118, Jun. 2024, doi: 10.1016/j.dsm.2023.12.001.
- [21] L. Yan *et al.*, "Attribute-based searchable encryption: a survey," *Electronics*, vol. 13, no. 9, p. 1621, Apr. 2024, doi: 10.3390/electronics13091621.
- [22] R. Siyal and J. Long, "Secure cloud data with attribute-based honey encryption." Research Square Platform LLC, Mar. 20, 2024, doi: 10.21203/rs.3.rs-4115057/v1.
- [23] Z. Wenhua *et al.*, "A lightweight security model for ensuring patient privacy and confidentiality in telehealth applications," *Computers in Human Behavior*, vol. 153, p. 108134, Apr. 2024, doi: 10.1016/j.chb.2024.108134.
- [24] G. Liu, H. Xie, W. Wang, and H. Huang, "A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption," *Journal of Cloud Computing*, vol. 13, no. 1, p. 44, Feb. 2024, doi: 10.1186/s13677-024-00608-w.
- [25] D. N. Joy and C. S. Yadav, "A survey on secure framework for privacy-preserving over EHR in cloud environment," *Nanotechnology Perceptions*, vol. 20, no. S2, pp. 377–394, Mar. 2024, doi: 10.62441/nano-ntp.v20iS2.28.
- [26] B. Guo, N. S. A. Shukor, and I. S. Ishak, "Enhancing healthcare services through cloud service: a systematic review," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 1, pp. 1135–1146, Feb. 2024, doi: 10.11591/ijece.v14i1.pp1135-1146.
- [27] D. Wijayanti, E. I. H. Ujjianto, and R. Rianto, "Uncovering security vulnerabilities in electronic medical record systems: a comprehensive review of threats and recommendations for enhancement," *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, vol. 10, no. 1, pp. 73–98 3, Feb. 2024, doi: 10.26555/jiteki.v10i1.28192.
- [28] P. Malathi, D. S. Suganthi, and J. Jospin Jeya, "Intelligent encryption with improved zealous method to enhance the anonymization of public health records in cloud," *Journal of Autonomous Intelligence*, vol. 7, no. 1, Oct. 2023, doi: 10.32629/jai.v7i1.567.
- [29] L. J. R. Lopez, D. M. Mayorga, L. H. M. Poveda, A. F. C. Amaya, and W. R. Reales, "Hybrid architectures used in the protection of large healthcare records based on cloud and blockchain integration: a review," *Computers*, vol. 13, no. 6, p. 152, Jun. 2024, doi: 10.3390/computers13060152.
- [30] N. H. Kamarudin, N. H. S. Suhaimi, F. A. Nor Rashid, M. N. A. Khalid, and F. Mohd Ali, "Exploring authentication paradigms in the internet of things: a comprehensive scoping review," *Symmetry*, vol. 16, no. 2, p. 171, Feb. 2024, doi: 10.3390/sym16020171.

BIOGRAPHIES OF AUTHORS






Senthilkumar Kalarani     is a professor in the Department of Computer Science and Engineering at PSG Institute of Technology and Applied Research. She has more than 20 years of teaching and ten years of R&D experience. She completed her Ph.D. at Anna University, Chennai and her postgraduate studies (2002-2004) at Sathyabama Institute of Science and Technology and undergraduate (1988-1992) studies at Madurai Kamaraj University. Her research interests lie in the area of web services, programming languages, ranging from theory to design to implementation, with a focus on improving software quality. In recent years, she has focused on better techniques for web mining and cloud-based information retrieval, AI, machine learning and data analytics. Dr. S. Kalarani has served on roughly 40+ conference and workshop and faculty development programs. Till date she has published more than 45 research papers in various national, international journals (Scopus index, Web of science, UGC impact factors) and conferences in India and abroad. She has also published 2 textbooks along with 5 Indian and foreign patents (both granted, published and filled) She has served as review member in International Journal of Software Engineering and Knowledge Engineering and British Journal of Educational Technology. She has visited Singapore, Malaysia and Japan to present her research work in various international conferences. Kalarani is the proud and obsessed mother of two sons, born December 2001 and March 2006. She enjoyed cooking, listening to music and reading. She can be contact at email: kalarani@psgitech.ac.in.






Mahalingam Shobana     has been in academia for the past 21 years imparting engineering education. She has completed her bachelor's degree (B.E) in electronics and communication engineering from Bharathidasan University, Tamil Nadu in 2001. She has completed her master's degree (M.E) in computer science and engineering (University Rank holder) from Anna university, in 2010. She has completed her doctorate from Anna University in June 2019 She is currently, working for SCOFT in Saveetha Engineering College, Thandalam, Chennai. Her research interests are in cloud computing, quantum computing and networking. She can be contact at email: dshobana@saveetha.ac.in.






Edamakanti Uma Shankari    received her B.Tech. degree in computer science and engineering in JNTUH University, M.Tech. degree in computer science and engineering from JNTUH University in 2011 and 2013 respectively and pursuing Ph.D. from Koneru Lakshmaiah Education Foundation. Her research area of interests are data mining, big data and cloud computing. She has been working as an assistant professor in the Department of Computer Science and Engineering, Koneru Lakshmaiah College of Engineering and Koneru Lakshmaiah University since Jan 2024. She can be contacted at email: e.umashankari@klh.edu.in.






Bolly Joshi Praveena    is a research scholar at SRMIST Chennai, she holds an M.Tech in computer science and engineering from JNTU and has 20 years of teaching experience. With approximately 15 papers published in international journals and conferences, her research interests lie in network security and Blockchain technology. Additionally, she is a member of IEEE and ISTE. She can be contact at email at pb2102@srmist.edu.in.






Subramaniam Shanthi    Awarded PhD in 2015 from Anna University, Chennai for the research work “A study on computer aided diagnosis system for breast cancer detection and classification using data mining approach”. Area of interest includes data analytics, image processing, deep learning, internet of things and soft computing. Received grants from various funding agencies like AICTE, CSIR, DBT, ICMR and DRDO to organize national and international seminar, workshops and conferences. Recently received a research grant of Rs. 900,000/- from All India Council for Technical Education (AICTE) for conducting research on “Design and development of AI powered deep learning model for COVID-19 identification, diagnosis and prediction of outbreak management”. More than 20 years of teaching and 10 years of research experience. Published more than 40 research articles in National and International journal and conferences. She is currently working as an associate professor in the Department of Computer Science and Engineering, Kongu Engineering College, Tamil Nadu, and India. She can be contact at email: shanthi.kongumca@gmail.com.



Rathinasabapathy Ramadevi    She completed her Ph.D. specialization on condition monitoring using computational intelligence. Her research interests include instrumentation, condition monitoring, signal/image processing and analysis, applications of artificial neural network, fuzzy logic and wavelet transform. She has more than 25 years of teaching and research experience and authored nearly 50 research articles/books in reputed journals/conferences in these fields. She is serving as an editorial member and reviewer of several national/international reputed journals. Dr. R. Ramadevi is the member of many international affiliations. He can be contact at email: sarvamkumaran@gmail.com.



Rajendar Sandiri    received his B.Tech. degree in electronics and communication engineering, M.Tech. degree in digital systems and computer electronics and Ph.D. in VLSI Design from Jawaharlal Nehru Technological University, Hyderabad. He has published more than 50 papers in international and national journals and conferences, eight Indian patents and one book published. He is a senior member of IEEE, life member of ISTE, and IETE. His areas of research interests include modeling and optimization of high-speed VLSI interconnects, design of low power and high-performance VLSI circuits. Presently he is currently working as professor in the Department of Electronics and Communication Engineering, Vardhaman College of Engineering, Hyderabad, Telangana, India. He can be contacted at sandiri.rajendar@gmail.com.