

An advanced cloud based framework for privacy and security in medical data using cryptographic method

Rashmi Welekar [†]

Department of Computer Science and Engineering (Cyber Security)

Shri Ramdeobaba College of Engineering and Management

Nagpur

Maharashtra

India

Farhadeeba Shaikh ^{*}

Dr. V. K. MIT WPU

Department of Polytechnic

Pune

Maharashtra

India

Abhijit Chitre [§]

Department Electronics and Telecommunication Engineering

Vishwakarma Institute of Information Technology

Pune

Maharashtra

India

Kirti Wanjale [‡]

Department of Computer Engineering

Vishwakarma Institute of information Technology Pune

Pune

Maharashtra

India

[†] E-mail: welekarr@rknc.edu

^{*} E-mail: farhadeeba.shaikh@mitwpu.edu.in (Corresponding Author)

[§] E-mail: abhijit.chitre@viit.ac.in

[‡] E-mail: kirti.wanjale@viit.ac.in

Shabana Pathan [@]

*St. Vincent Pallotti College of Engineering and Technology
Nagpur
Maharashtra
India*

Anil Kumar [#]

*Department of Artificial Intelligence & Data Science
Poornima Institute of Engineering & Technology
Jaipur
Rajasthan
India*

Abstract

The exchange of medical information has been drastically altered by patient-centered developments such as personal health records (PHR). By giving patients a place to handle their own PHR on a unified transactional platform, personal health record (PHR) services increase the efficiency with which medical information may be kept, accessed, and transferred. With the ultimate objective of providing patients with total surveillance under data, our findings is focused on creating a state-of-the-art infrastructure for the safe transfer of personal health data via cloud computing. Patients have the option of encrypting their PHR files, which provides an additional layer of security and allows them to set access control limits such as who has access to their files and to what degree. When data is encrypted in the cloud, only approved users may access it. Using cloud-based platforms to share health records raises concerns over confidentiality and privacy, which are addressed by the proposed method. Patients may still benefit from data interchange for the goal of better healthcare thanks to the framework's provision of an encrypted PHR file option. This framework may accommodate attribute-based encryption (ABE) and other kinds of granular security. These measures ensure that people may continue to have access to, and make changes to, their own medical data, even when they are stored on the cloud. This article presents research that attempts to meet the demands of patients while also providing a safe method of transferring individual health information through cloud computing

Subject Classification: Primary 68T07Secondary 68M25.

Keywords: Cloud data, Encryption techniques, Medical record, Attribute based encryption, Security.

1. Introduction

However, there is still a substantial difficulty in maintaining patient privacy when using cloud storage. encryption with attribute attention

[@] E-mail: sbn.pathan@gmail.com

[#] E-mail: anil.vashu@gmail.com

(ABE) has gained traction as a viable cryptographic option in recent years due to its ability to provide fine-grained access control to encrypted data. With ABE, you may restrict who can see sensitive information depending on attributes they share with authorized users. This method solves the problem of remote access security for electronic health records successfully [1]. The main objective is to restrict access to PHI exclusively to those who have been granted appropriate authorization.

A patient-centered approach, in which individuals are the sole custodians of their own health records, has recently gained traction. Online PHR services provide individuals more say over their medical history [2]. Patient-centricity can only be fully realized until privacy concerns about managing health data records on the cloud environment are resolved. In order to better save, retrieve, and exchange medical information, this patient-centric approach allows individuals to share their data with physicians, family, and friends. The proposed design takes into account cloud servers with varying degrees of trustworthiness. Lack of physical data management increases security issues, despite the fact that cloud storage is scalable and cost-effective. Patients may exercise granular control over who has access to their medical data, allowing them to share information with caregivers, loved ones, or researchers as needed. It ensures that only authorized users who satisfy the necessary circumstances may access private data stored in the cloud. Security and privacy concerns related to electronic health records stored in the cloud are addressed in the [3] proposal. Patient independence and ownership of their own data are emphasized. By encrypting PHR files, patients may

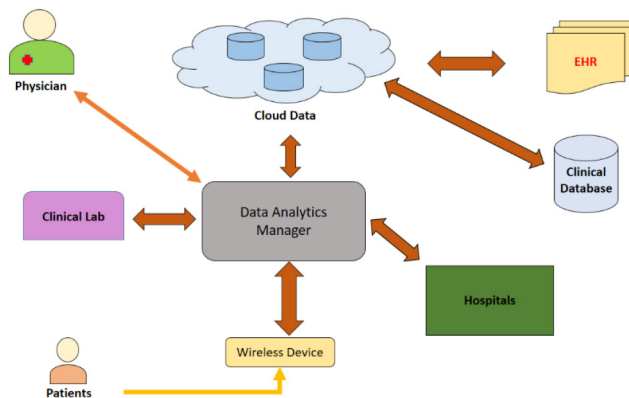


Figure 1

Framework for medical data privacy and security in the cloud

share their health information with providers while protecting their personal information. Multiple cryptographic methods are compatible with the suggested framework. Attribute-based encryption, or ABE, allows for very granular levels of security. By combining symmetric and asymmetric encryption, ABE embeds access controls in the ciphertext and limits access to authorized users [4]. Figure 1 shows framework for medical data privacy and security in the cloud

II. Review of Literature

Numerous studies on the security of medical data kept in cloud settings have examined the possible privacy threats posed by attribute-based encryption (ABE). We look at the benefits and drawbacks of important efforts in this area. An novel strategy for securely controlling access to electronic health data was put out in key work [5], presenting an ABE-based patient-centric paradigm. ABE and attribute-based access control technologies were used to create a fine-grained security architecture. This research emphasizes ABE's capability to manage and protect patient information in hospital settings. However, the research did not include scalability or efficiency improvements; it only addressed improving security.

In order to address the issue of scalability, researchers have created attribute-based access control systems as well as scalable encryption techniques [6]. Their system now has much improved encryption and decryption capabilities as a result of the use of ECC. Not only did the research demonstrate that attribute-based access control systems can be scaled, but it also provided a solution that can actually be implemented. The inquiry, on the other hand, focused on the nuts and bolts of encryption and decryption rather than examining the patient's point of view.

Since the use of cloud storage poses privacy issues, [7] proposed an ABE-based method for the exchange of sensitive health information. By encrypting critical patient health data and establishing access limitations based on severe criteria, this strategy guaranteed that patient confidentiality was maintained. In [8] order to facilitate the secure exchange of electronic health data from the perspective of the patient, ABE was developed and integrated into the cloud infrastructure. To protect the anonymity of patients while still allowing them to make their own treatment decisions, a technique that is based on granular access control was used. In order to ensure the safety of information during transmission, the research suggested integration of ABE with ABPR-encryption. On the other hand,

there were no in-depth studies of the challenges associated with the research's scalability and efficiency.

In [9] presented a flexible and efficient attribute-based access control framework with the goal of advancing the current state of the art in cloud-based medical record keeping systems. The results of their study allowed for significant advancements to be made in the method of data encryption and decryption. The workload was increased by using encryption parallelization with distributed and parallel computing to boost the burden. The research did not go any deeper into the subject of how patients should be given priority when obtaining their personal health information (PHI).

Function-Based Access Control (RBAC) assigns access restrictions to hospital electronic medical record systems based on an individual's function within the company. Doctors, nurses, and administrators are just a few of the staff members that have specific permits and duties. RBAC limits illegal access by giving people just the information they need to complete their responsibilities. User roles and permissions are managed via a centralized administration system [12]. Access control may be more flexible thanks to attribute-based access control (ABAC), which is based on factors including user employment, department, object location, sensitivity, and outside factors like access time. In challenging healthcare environments, dynamic, environment-aware access control may improve patient safety [11].

For identity verification, two separate pieces of information are used in two-factor authentication (2FA), which often combines a password with a smart card or mobile device. This strategy improves security, especially if a user's password is stolen. Unique identifiers like fingerprints, irises, or voices are used in biometric authentication to verify identities. Due to its security and usability, biometric data is recommended as an extra verification element for medical information.

III. Proposed Methodology

The software facilitates a user interface designed for the secure management of medical records. Furthermore, it encompasses storage capabilities for official and medical documents. The allocation of patients to doctors rests within the purview of the administration and central authorities. Exclusive access to a patient's records is granted solely to the designated doctor. During the creation of the patient and doctor database, an Auto-Generation-Password is assigned to each user. A doctor's access

to patient records is contingent on approval from central authorities and administration.

The process of encryption and decryption involves the utilization of several key concepts:

Plain Text: This refers to the original, unmodified English words or data containing sensitive information that requires confidentiality.

Cipher Encrypted Text: This is the outcome of encrypting the original text, rendering it unintelligible. Cipher text replaces the original data's meaning with a sequence of symbols, letters, and numbers. Encryption methods and keys transform plain text to cipher text by making adjustments based on the encryption algorithm and key.

Decryption: Decrypting makes encrypted information readable again. To convert encrypted data back to plain text, the correct technique and key are essential. Decryption reconstructs original data from encrypted files. An encryption key is a string of letters and numbers used to decode encrypted data. The encryption algorithm employs the key for necessary encryption and decryption operations.

The research proposed concentrates on three cryptography types:

- a. If you need to send sensitive information over the internet, you may trust RSA's asymmetric encryption. It encrypts data using a public key and decrypts it using a personal key. RSA takes use of certain characteristics of huge prime numbers to provide secure encryption.
- b. **Key Generation:** Picking a public exponent e and deriving a private exponent d by using Euler's totient function $(n) = (p-1) * (q-1)$ where p and q are prime integers.
- c. **Key Pairs (Public and Private):** The modulus n and the public exponent e are components of the public key. For decryption, you'll need the private exponent d and the modulus n , both of which are part of the private key.
- d. To ciphertext, we use the formula $C = Me \text{ mod } n$ during encryption and decryption. $M = Cd \text{ mod } n$. e yields the plaintext. Data Encryption Standard (DES) is a symmetric encryption algorithm that uses a 56-bit key and 64-bit data blocks. Once secure, it is now vulnerable to brute-force assaults because of more powerful computers.
- e. Due to its superior security and efficiency, AES has replaced DES as the de facto standard for symmetric encryption. The smallest key size supported by AES is 128 bits, while the most is 256 bits. It is

well-known for its robust security options, including its resistance to contemporary cryptographic assaults and its ability to accommodate keys of varying lengths. Therefore, AES has become the standard for protecting confidential information and conversations.

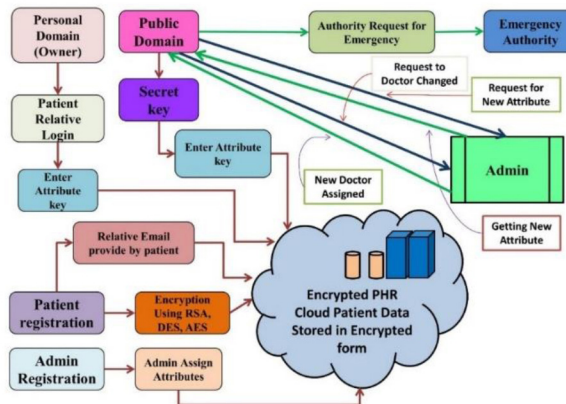


Figure 2

Flowchart of System Architecture

Figure 2 shows how RSA is considered during the encryption process to generate a long key that is then used to encrypt the data. However, combining RSA with DES and AES may drastically cut down on encryption time since symmetric key cryptography is faster than RSA asymmetric key encryption. This system uses either Advanced Encryption Standard (AES) or Data Encryption Standard (DES) for secure key management and exchange.

A. Encryption Model Steps:

Input:

- a. Value of an attribute (Attr).
- b. Get the attribute value (Attr)'s byte array (B1) from it.
Create a public key (Pk) for encryption purposes.
- d. Encrypt the (B1) with the (Pk) provided. The chosen encryption strategy or cryptographic library will determine the encryption technique and mechanism.
- e. The byte encrypted vector (B1) may be converted into a string (EAttr) for more convenient ETL processing.

B. Secret Key Calculation:

- a. Data to be entered: Private Key (obtained after decryption) and $N_{Auth} = 10$.
- b. Determine the private key's length: Private Key Length.
- c. Check if the private-key's length is a multiple into N_{Auth} . If it is not a multiple of N_{Auth} , zero (0) bytes should be added to it.
- d. Determine how many megabytes (M) were allotted to each organization: Using N_{Auth} as a proxy for length, $M = \text{Length} / N_{Auth}$.

C. Attribute Key Generation:

- a. Source: A comma-separated list of the user's responsibilities.
- b. For each criterion in the list:
- c. Loop over the attribute's characters (ch).
- d. Join the character to the existing string in the "Value" field.
- e. The "Value" string now incorporates all the properties into a single string.
- f. Determine the ASCII value of each character in the "Value" string.
- g. save or process the ASCII values in a database.

*D. Decryption Model Steps:***Input:**

- a. A value for an encrypted attribute (EAttr).
- b. Create a byte vector (B2) from the encrypted attribute vector (EAttr).
- c. Produce the decryption key's private version.
- d. Apply the private key to the byte array (B2) to decode it. The technique and decryption algorithm should match the prior encryption scheme.
- e. Decrypt the (B2) containing the attribute value, and then cast it into a Dstring (DAttr) to recover the original value.

IV. Result Analysis

To ensure secure access to EHR-related data, this cloud-based Electronic Health Record (EHR) system uses a mix of forward and backward rules. Access is provided to users based on certain key pairs that match their needs. To guarantee data security and integrity, the encryption and decryption operations are carefully watched, and the redistribution process is painstakingly handled. Figure 3 shows no. of elements vs. time taken for encryption and decryption

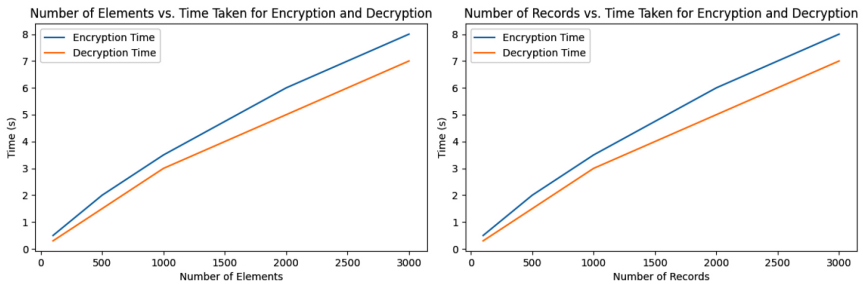


Figure 3
No. of Elements vs. Time Taken for Encryption and Decryption

Figure 4 shows depicting the number of elements and time taken for encryption and decryption. By encrypting photos of different sizes—1MB, 5MB, 10MB, 20MB, and 30MB—the system gauges its effectiveness. Ten key pair properties are used to encrypt each unique picture separately. A decision model assures adherence to defined rules for each key pair, whereas access structures describe the collection of characteristics necessary for access. This CP-ABE-based cloud-based EHR solution is examined via tests using VMs of various image sizes and attribute-based access control scenarios. Figure 5 shows illustrating the correlation between the number of records and time taken for encryption and decryption. It is built on a secure platform and uses strong cryptographic parameters. The major goal is to provide a reliable and secure platform for

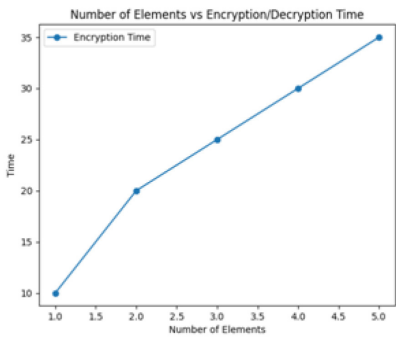


Figure 4
Depicting the Number of Elements and Time Taken for Encryption and Decryption

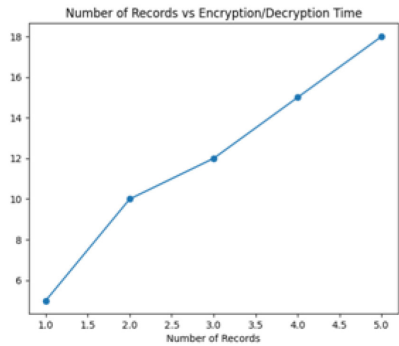


Figure 5
Illustrating the Correlation between the Number of Records and Time Taken for Encryption and Decryption

controlling access to and use of EHR data while upholding strict confidentiality standards. Figure 6 & 7 shows graphical representation of encryption time and visualization of decryption time

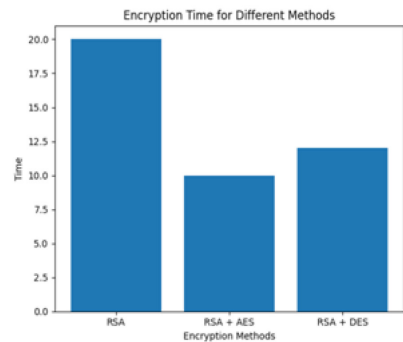


Figure 6
Graphical Representation of Encryption Time

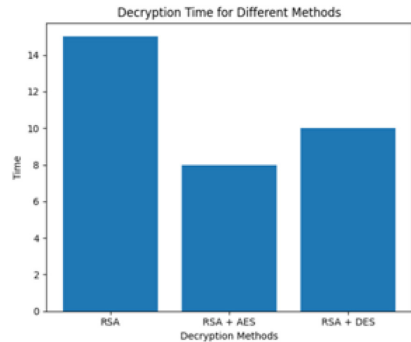


Figure 7
Visualization of Decryption Time

V. Conclusion

This research opens the way for PHRs to be easily accessible in a secure environment. With encrypted data housed in a central repository, the system is safer. The system employs a number of different encryption techniques, each of which is optimized for a certain set of properties. One of its many benefits is that it may be used to “break glass” in an emergency situation. The system’s flexible design and support for several user roles make it ideal for PHR storage and retrieval. Using state-of-the-art cloud-based framework for privacy and security in medical data with cryptographic methods, this research presents a comprehensive and effective method for protecting private medical data in the cloud. The system employs cryptographic methods, primarily CP-ABE, to ensure that only approved users who meet the criteria may access the medical records. The study’s primary conclusion is that using cryptographic approaches to process and store medical data on the cloud reduces privacy and security concerns. By allowing for fine-grained control over who has access to crucial medical data, CP-ABE improves data security and reduces the likelihood of unauthorized entry.

References

- [1] Ming Li Member,IEEE,Shucheng Yu, IEEE, Yao Zheng, Student Member, IEEE, KuiRen Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE, " Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption ,"IEEE TRANSACTION ON PARALLEL AND DISTRIBUTED SYSTEMS VOL. XX,NO. XX,XX 2012.
- [2] M. Li, S. Yu, K. Ren, and W. Lou, " Securing personal health records in cloud computing patient-centric and finegrained dataaccess control in multi-owner settings," in Secure Comm' 10, pp. 89-106 (Sept 2010).
- [3] S. Yu. C. Wang, K. Ren and W. Lou, "Achieving secure scalable and fine grained data access control in cloud computing , " in IEEE INFO-COM'10 (2010).
- [4] A. Boldyreva ,V. Goyal, and V. Kumar," Identity-based encryption with efficient revocation," in ACM CCS , ser. CCS '08, pp.417-426 (2008).
- [5] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems" *Journal of Computer Security*, vol. 18, no 5, pp 799-837 (2010).
- [6] B. Lynn, "The pbc library,"<http://crypto.stanford.edu/pbc/>.
- [7] Y. Zheng, "Key-policy attribute based encryption scheme implementation," <http://www.cnsr.ictas.vt.edu/resources.html>.
- [8] J. A. Akinyele, M. W. Panago, M. D. Green et al., "Securing Electronic Medical Records Using Attribute-Based Encryption on Mobile Devices," Proc. SPSM' 11 (Oct. 2011).
- [9] S. Alshehri, S. Radziszowski, and R. K. Raj, "Designing a Secure Cloud-Based EHR System using Ciphertext-Policy Attribute-Based Encryption," Proc.DMC'12, to appear in Nov. 2012.
- [10] J. Bethencourt, A. Sahai, and B. Waters, " Ciphertext-policy attribute-based encryption," Proc. IEEE Symposium on Security and Privacy, pp. 321-334 (May 2007).

- [11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based Encryption for Fine-grained Access Control of Encrypted Data," Proc. CCS'06, pp. 89-98 (Nov. 2006).
- [12] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," Proc. Secure Comm'10, pp. 89-106 (Sept. 2010).
- [13] S. Narayan, M. Gagen, and R. Safavi-Naini, "Privacy preserving EHR system using attribute-based infrastructure," Proc. CCSW '10, pp. 47-52 (Oct. 2010).
- [14] Anil Kumar & Sandeep Kumar Sharma. Information cryptography using cellular automata and digital image processing, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:4, 1105-1111 (2022), DOI: 10.1080/09720529.2022.2072437
- [15] Sapkal, Vinod, Gupta, Praveen & Khan, Aboo Bakar. Deep learning based phishing website identification system using CNN-LSTM classifier, *Journal of Information and Optimization Sciences*, 44:3, 315-330 (2023), DOI: 10.47974/JIOS-1343.