Ethical Encrypted Search Scheme for Medical Database

Bharathwaj N* [1], Mrs. Durgadevi * [2], Dr. J. Jayaprakash* [2], Dr. G. Victo Sudha George* [2]
Mail ID:- bharathwaj63633@gmail.com
*[1] IV Year B. Tech CSE Students, Dept of Computer Science and Engineering, *[2] Professor
Dr. M.G.R Educational and Research Institute, Maduravoyal, Chennai-95, Tamil Nadu, India

ABSTRACT-. E-medical records are highly sensitive and require secure storage, typically in encrypted form. However, encrypting the records can make them difficult to search and utilize within existing medical database systems. Additionally, managing access to these records, especially when multiple authorities are involved, presents challenges in ensuring security and scalability.To address these issues, we propose an authorized searchable encryption scheme designed for a multi-authority setting. This scheme utilizes the RSA (Rivest-Shamir-Adleman) function to enable each authority to control and limit search capabilities based on clients' privileges. Furthermore, to enhance scalability, we employ multi-authority attribute-based encryption, allowing the authorization process to be streamlined even across policies from multiple authorities.We have conducted thorough security and cost analyses, as well as experimental evaluations, demonstrating that our proposed scheme introduces only moderate overhead to existing searchable encrypted systems.

Keywords--e-medical system, cloud storage, forward security.

1. INTRODUCTION

E-medical record systems are pivotal in modernizing healthcare, empowering patients to manage their Personal Health Records (PHRs) online. Typically, to alleviate computational and communication burdens, these systems are outsourced to third-party cloud services. However, this outsourcing raises concerns about privacy due to the risk of data exposure. Consequently, cloud providers must implement robust strategies to safeguard e-medical records. A common approach is to encrypt data before uploading it to the cloud, ensuring that only authorized clients possessing the appropriate keys or permissions can decrypt it. In PHR systems, data owners are usually tasked with encrypting their PHRs and defining access policies dictating which keywords can be searched. However, achieving these requirements with encrypted data presents challenges. Once records are encrypted and stored in the cloud, traditional keyword searches become infeasible, as the server lacks access to record information. This limitation imposes significant computational and communication costs. To enable keyword searches on encrypted data, searchable encryption techniques have been proposed, allowing servers to search encrypted data using secure search tokens provided by clients. However, existing schemes primarily cater to single authority settings, which doesn't suffice for PHR systems with multiple authorities and encrypted records and queries managed by different keys. To illustrate the necessity of our design, consider a scenario in a smart PHR system where various doctors across different hospitals contribute to PHRs. Due to data sensitivity, access rights are restricted, such as granting a general practitioner access only to their patients' records, while a cardiologist may access all heart-related records. Additionally, patients may visit multiple hospitals, necessitating access to former records for diagnosis. Hence, clients require read and search privileges across multiple authorities. Moreover, due to medical data privacy concerns, access control must refine queries to authorized keywords. For instance, cardiologists should only query heart disease information and not access a patient's history of skin conditions. Therefore, client search capabilities must be managed to authorize searches for specific keywords. These requirements underscore the need to address authorization management for sensitive medical data and propose a practical, privacy-preserving encrypted data search solution for multi-authority scenarios.

2. LITERATURE SURVEY

(1) Introduction to the significance of safeguarding patient confidentiality in medical databases. (2) Exploration of cryptographic techniques such as homomorphic encryption and attribute-based encryption for secure querying. (3) Discussion on privacy-preserving protocols like private information retrieval and oblivious transfer to ensure query confidentiality. (4) Consideration of ethical principles, including patient consent mechanisms and data minimization strategies. (5) Review of existing case studies and implementations to highlight practical implications. (6) Evaluation of performance metrics including efficiency, scalability, and security. (7) Identification of current challenges such as computational overhead and scalability issues. (8) Proposal for future research directions, focusing on enhancing privacy-preserving protocols and addressing ethical concerns. (9) Importance of accountability and auditability in ensuring transparency and trustworthiness. (10) Conclusion emphasizes the critical role of ethical encrypted search schemes in balancing privacy and accessibility in medical databases, underlining the need for continued research and development in this evolving field.

3. EXISTING SYSTEM

The conventional medical database system faces a challenge when records are encrypted, rendering them unsearchable. Additionally, managing private medical records, which may involve multiple authorities, presents complexities in authorizing clients to access data securely and at scale. While many existing searchable encryption schemes focus on a single authority setting, they fall short of meeting the demands of PHR systems, where multiple authorities are involved, and data records and queries are encrypted using different keys.

4. PROPOSED SYSTEM

Our proposal introduces an authorized searchable encryption framework tailored for a multi-authority environment. We employ the RSA function to enable each authority to restrict search capabilities based on clients' privileges. Additionally, we enhance scalability by implementing multi-authority attribute-based encryption, streamlining the authorization process across policies from multiple authorities. In our system, users authorize requests, such as those from doctors, before key generation, and doctors verify the validity of these keys. With the keys, authorized parties can access user details securely.

5. METHODOLOGY USED

The methodology for developing an ethical encrypted search scheme for a medical database involves a systematic approach. It begins with project initiation, wherein project goals, scope, and stakeholders are defined, forming a dedicated interdisciplinary team. Requirements analysis follows, with inputs gathered from healthcare professionals, existing system analysis, and regulatory compliance needs assessment. The encryption technique most suitable for medical data is selected, and an architectural framework integrating encryption, access control, and user interfaces is designed. Implementation includes the actual integration of encryption and access control mechanisms, with a focus on robust key management. Rigorous testing ensures data privacy and system functionality. Compliance with healthcare regulations is diligently addressed, and comprehensive documentation of security measures and procedures is maintained. User training is conducted to educate healthcare staff and administrators on system use and security practices. Finally, deployment, maintenance protocols, and continuous monitoring of security and user satisfaction complete the methodology, ensuring a secure and ethical encrypted search scheme for the medical database

6. SYSTEM ARCHITECTURE

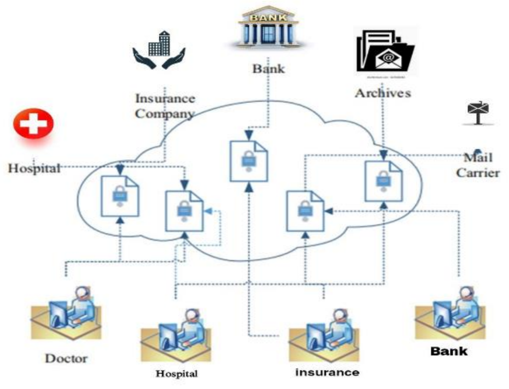


Fig: system architecture

The architecture illustrates the design of the encryption file web-base

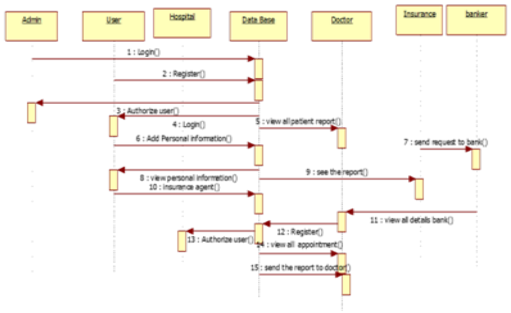

Admin
User
Hospital
Data Base
Doctor
Insurance
banker
1 : Login()
2 : Register()
3 : Authorize user()
4 : Login()
5 : view all patient report()
6 : Add Personal information()
7 : send request to bank()
8 : view personal information()
9 : see the report()
10 : insurance agent()
11 : view all details bank()
12 : Register()
13 : Authorize user()
14 : view all appointment()
15 : send the report to doctor()

Fig: sequence Design

The sequence design illustrates How the database will work Under the 6 modules as a protocol

7. MODULES

There are 6 modules I have used here: (ADMIN**,** USER**,** HOSPITAL**,** INSURANCE**,** and BANK)

ADMIN: Login to the account with the correct username and password only authorized admin can log in to our system. Admin has to accept and authorize the user logout

USER: Register the account with the basic information authorized by the admin owner can log in to the account Personal Data (including Insurance and Bank Data also)Add personal details like (username, mobile, email, address, etc.)Add insurance details like (username, insurance type, policy number, email, and address). Add bank details like (username, bank name, bank type, account number, address). View Personal Data Detail User can fix an Appointment with a Doctor. View request. Users can view messages. Logout.

HOSPITAL: Login to the account with the correct username and Password. Authorize the Doctor View All Appointment Data details: Here the hospital can see which patient has an appointment with which Doctor. View the keys and Send them to the doctor. Logout.

DOCTOR: Register the account with the basic information.After authorization by the Hospital can log in to the account, view The Reports --> See all the Patient's reports sent by (user) --> (Hospital) --> (Doctor) in decrypted format. The doctor has to approve the report.

INSURANCE: Login to the account with the correct username and Password. View request and patient detailsInsurance agent can see the report and cost of the amount. After successful verification, the insurance agent can send a request to the bank log

BANK: Log in to the account with the correct username and Password. View insurance and patient details View Bank Request After Verification the bank can transfer the amount and send a message to the user saying that your request has been approved Logo

8. IMPLEMENTATION

I Implemented the user authentication mechanisms for each module (doctor, user, admin, insurance, bank, hospital) to verify their identity before accessing the system..

Doctor Module: This allows doctors to securely query patient records for diagnosis and treatment purposes. Implement functionalities for encrypted search queries tailored to medical data, ensuring that doctors can retrieve relevant information while maintaining patient privacy.

User Module: Enable users (patients) to access their medical records securely. Implement features for users to query their encrypted medical data, ensuring that only authorized users can access their information.

Admin Module: Provide administrators with tools to manage user accounts, access control policies, and system configurations. Implement functionalities for administrators to monitor system activity, manage encryption keys, and enforce compliance with ethical guidelines.

Insurance, Bank, and Hospital Modules: Enable insurance companies to securely access patient information for claims processing and risk assessment purposes. Implement functionalities for banks to securely access medical data for processing healthcare-related financial transactions. Provide hospitals with secure access to patient records for medical research, collaboration, and continuity of care.

RSA ENCRYPTION ALGORITHM: The RSA encryption algorithm is a type of public-key encryption algorithm. To better understand RSA, let's first understand what public-key encryption algorithm

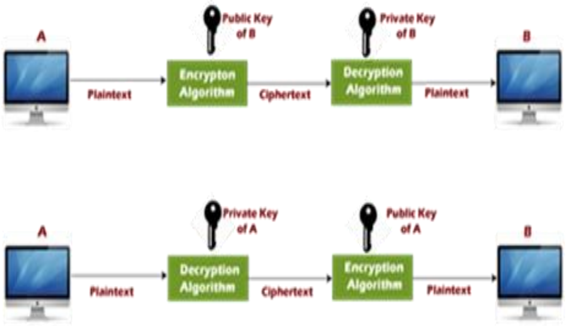
PUBLIC KEY ENCRYPTION ALGORITHM: The Public Key encryption algorithm is also called the Asymmetric algorithm. Asymmetric algorithms are those algorithms in which the sender and receiver use different keys for encryption and decryption. Each

the sender is assigned a pair of keys**:**

o **Public key**

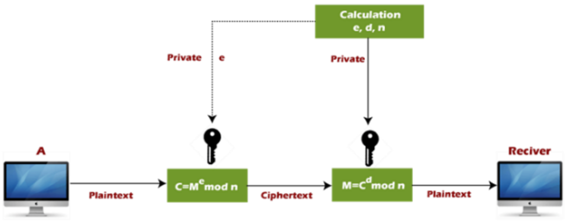
o **Private key**

Encryption relies on a pair of keys: a public key for encryption and a private key for decryption. While the public key is used to encrypt data, decryption is solely performed using the corresponding private key. The keys are interconnected, but the private key cannot be deduced from the public key. While the public key is openly accessible, the private key remains confidential and known only to its owner. This setup allows anyone to send encrypted messages to the user employing their public key, while only the user possesses the capability to decrypt these messages using their private key.



Encryption/decryption using public/private keys

RSA ENCRYPTION ALGORITHM: RSA is the most common public-key algorithm, named after its inventors **Rivest, Shamir, and Adelman (RSA)**.



RSA

The RSA algorithm follows a specific procedure to generate public and private keys:

Firstly, two large prime numbers, denoted as p and q, are selected. These numbers are multiplied to **obtain n = p x q,** where n serves as the modulus for encryption and decryption.

Next, a number e is chosen such that it is less than n and relatively prime to **(p - 1) x (q - 1).** In other words, e and **(p - 1) x (q - 1)** share no common factors except 1. This ensures that e satisfies the condition gcd**(e, φ(n)) = 1**, where φ(n) represents Euler's totient function.

With **n = p x q**, the public key is represented as **<e, n>.** To encrypt a plaintext message m using the public key, the following formula is employed: **C = m^e** mod n. It's essential that m is less than n; for larger messages, the plaintext is divided into smaller segments, each encrypted separately.

To compute the private key, the value of d is determined such that it satisfies the equation **De mod φ(n) = 1**. The private key is then represented as **<d, n>.**

To decrypt a ciphertext message c using the private key, the formula **m = c^d** mod n is applied.

9. RESULT AND DISCUSSION

The discussion of an ethical encrypted search scheme for a medical database represents a significant advancement in preserving patient privacy and confidentiality while still allowing for efficient data retrieval by authorized healthcare professionals. By encrypting sensitive medical information and enabling secure search functionality, this scheme ensures that patient data remains protected from unauthorized access or breaches.

(front-end interface webpage)

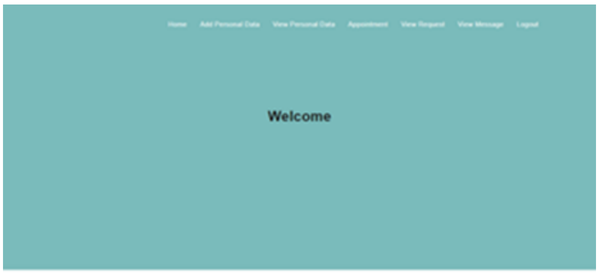


Fig: User Home Page

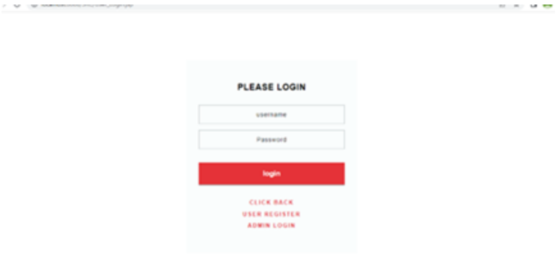


Fig: user login Page

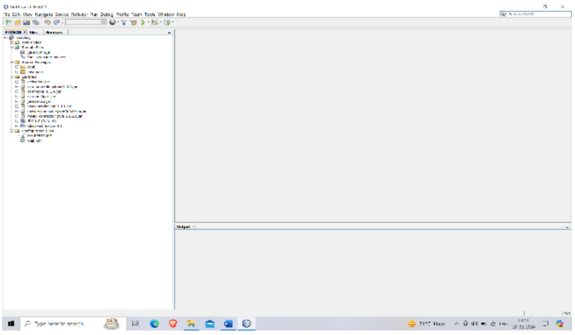
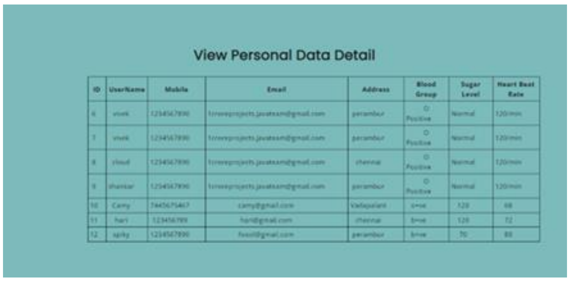


Fig: net beans ide



View Personal Data Detail

ID	UserName	Mobile	Email	Address	Blood Group	Sugar Level	Heart Beat Rate
6	vivek	1234567890	1croreprojects.javateam@gmail.com	perambur	○ Positive	Normal	120/min
7	vivek	1234567890	1croreprojects.javateam@gmail.com	perambur	○ Positive	Normal	120/min
8	vinod	1234567890	1croreprojects.javateam@gmail.com	chennai	○ Positive	Normal	120/min
9	shankar	1234567890	1croreprojects.javateam@gmail.com	perambur	○ Positive	Normal	120/min
10	Camy	7445675467	camy@gmail.com	Vadapalani	o+ve	120	68
11	hari	123456789	hari@gmail.com	chennai	b+ve	120	72
12	spiky	1234567890	fossil@gmail.com	perambur	b+ve	70	88

Fig: view data

(Back end interface of the database)

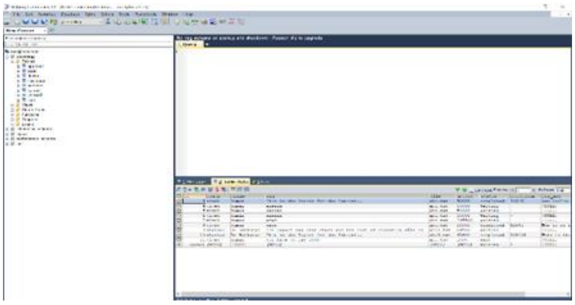


Fig: my SQL interface

10. CONCLUSION

The adoption of an ethical encrypted search scheme for medical databases represents a positive step towards safeguarding patient privacy and confidentiality in healthcare settings. By leveraging encryption and secure search functionalities, healthcare organizations can balance the need for data access with the imperative to protect sensitive patient information, ultimately enhancing trust and confidence in the healthcare system.

REFERENCES

1. M. J. Steinberg and E. R. Rubin, The HIPAA Privacy Rule: Lacks Patient Benefit, Impedes Research Growth, Association of Academic Health Centers, 2009.

2. P. Samarati and L. Sweeney, Protecting Privacy when Disclosing Information: K-Anonymity and Its Enforcement through Generalization and Suppression, Electronic Privacy Information Center, 1998.

3. C. Dwork, “Differential privacy: a survey of results,” in Theory and Applications of Models of Computation. TAMC 2008, pp. 1–19, Springer, 2008.

4. J. Soria-Comas, J. Domingo-Ferrer, D. Sánchez, and S. Martínez, “Enhancing data utility in differential privacy via microaggregation-based k-anonymity,” The VLDB Journal, vol. 23, no. 5, pp. 771–794, 2014.

5. Y. Wu, J. Su, and B. Li, “Keyword search over

shared cloud data without secure channel or authority," in 2015 IEEE 8th International Conference on Cloud Computing, pp. 580–587, New York, NY, USA, 2015.

6. E. Shi, J. Bethencourt, T. H. H. Chan, D. Song, and A. Perrig, "Multi-dimensional range query over encrypted data," in 2007 IEEE Symposium on Security and Privacy (SP'07), pp. 350–364, Berkeley, CA, USA, 2007.

7. K. LeFevre, D. J. DeWitt, and R. Ramakrishnan, "Mondrian multidimensional k-anonymity," ICDE, vol. 6, p. 25, 2006.

8. J. H. Friedman, J. L. Bentley, and R. A. Finkel, "An algorithm for finding best matches in logarithmic Expected time," ACM Transactions on Mathematical Software, vol. 3, no. 3, pp. 209–226, 1977.

9. J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: ciphertext- policy attribute-based encryption," Future Generation Computer Systems, vol. 52, pp. 67–76, 2015.

X. Wang, A. Zhang, X. Xie, and X. Ye, "Secure-aware and privacy-preserving electronic health record searching in a cloud environment," International Journal of Communication Systems, vol. 32, no. 8, article e3925, 2019.

10. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: using blockchain for medical data access and permission management," in 2016 2nd International Conference on Open and Big Data (OBD), pp. 25–30, Vienna, Austria,.