International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.7 May - June – 2023
DOI:10.46647/ijetms.2023.v07i03.001 ISSN: 2581-4621

ATTRIBUTE-BASED PROXY RE-ENCRYPTION WITH KEYWORD SEARCH ON PERSONAL HEALTH RECORD

R.Murugesan[1], V.Charumathi[2], V.Ishwarya[3], T.Kalaiyarasi[4], V.Kayathri[5]
[1]*Associate Professor, Computer Science and Engineering,Paavai college of Engineering, Namakkal, Tamilnadu*
[2] *UG - Computer Science and Engineering,Paavai college of Engineering, Namakkal, Tamilnadu*
[3] *UG - Computer Science and Engineering,Paavai college of Engineering,Namakkal,Tamilnadu*
[4] *UG - Computer Science and Engineering,Paavai college of Engineering,Namakkal,Tamilnadu*
[5] *UG - Computer Science and Engineering,Paavai college of Engineering, Namakkal, Tamilnadu*

ABSTRACT

Personal health records (PHRs) contain sensitive health information that needs to be protected from unauthorized access. At the same time, patients may need to share their PHRs with healthcare providers or researchers to receive appropriate care or participate in medical studies. Attribute-based proxy re-encryption with keyword search (ABPRE-KS) is a what cryptographic technique that enables secure and controlled sharing of encrypted PHR data while preserving privacy and confidentiality of sensitive patient information. ABPRE-KS works by encryption of the PHR data using a key derived from the patient's attributes and allowing the patient to delegate access to the data to third parties using a proxy re-encryption scheme. To enable keyword search on the encrypted PHR data, an additional searchable encryption scheme can be used. ABPRE-KS provides a powerful tool for securely sharing and searching PHR and it can be used to facilitate better healthcare outcomes and medical research while protecting patient privacy.

Keywords –PHR, ABPRE, Data access control, Image detection algorithm

1.INTRODUCTION

Attribute-Based Proxy Re-Encryption with Keyword Search (ABPRE-KS) is a cryptographic technique that allows for secure delegation of access to encrypted data based on a set of attributes or keywords. This technology can be applied to personal health records (PHRs) to enable patients to securely share their health data with healthcare providers, researchers, and other authorized parties while maintaining their privacy. PHRs are electronic records that contain an individual's health information, including medical history, test results, and treatment plans. They are typically stored on a central server or in the cloud and are accessed through a secure login process. However, patients may not always want to share their entire PHR with every healthcare provider they visit, especially if they have sensitive medical information that they prefer to keep confidential.

ABPRE-KS allows patients to selectively share their PHR data with specific healthcare providers based on their attributes or keywords, such as their medical specialty or area of expertise. This is achieved by encrypting the PHR data using a unique key that is derived from the attributes or keywords associated with each healthcare provider. The patient can then delegate access to the encrypted data to the healthcare provider by re-encrypting the data with the provider's attribute-based key. The provider can then use keyword search to efficiently retrieve specific data from the encrypted PHR without having access to the patient's entire record. This ensures that only authorized parties can access the patient's data while maintaining the patient's privacy and confidentiality.

2.CRYTOGRAPHIC TECHNIQUE

Cryptographic techniques are used to secure the transmission and storage of sensitive information. cryptographic technique that allows a proxy to transform a ciphertext encrypted under one set of attributes into a new ciphertext that is decryptable by a user possessing a different set of attributes. This technique is useful in scenarios where a user wants to delegate decryption rights to a third party without revealing their private key or the plaintext message. In ABPRE, attributes are used to define access control policies that determine who can decrypt the ciphertext. The proxy re-encrypts the ciphertext using a re-encryption key that is generated based on the attributes of the delegator and the delegate. The delegate can then decrypt the re-encrypted ciphertext using their own private key, which corresponds to their set of attribute. There are various cryptographic techniques, some of which include:

2.1 SYMMETRIC-KEY ENCRYPTION

This strategy utilizes an only one key to encode and unscramble the information. The comparative key is utilized for both encryption and decoding. Symmetric key encryption and quality based intermediary re-encryption (ABPRE) are two distinct cryptographic procedures used to get information.

Symmetric key encryption is a type of encryption where the similar key is used for both encryption and decryption. The key is kept secret between the sender and receiver of the encrypted data, and anyone who doesn't have the key cannot read the encrypted information. Examples of symmetric key encryption algorithms include AES (Advanced Encryption Standard) and DES (Data Encryption Standard)

On the other hand, attribute-based proxy re-encryption is a type of encryption that allows a proxy to transform an encrypted message from one set of attributes to another set of attributes, without the proxy having access to the original message or the decryption key. This technique is useful in scenarios where a user wants to share encrypted data with another user, but only if that user has specific attributes (e.g., location, role, security clearance).Combining these two techniques, we get attribute-based symmetric key encryption or attribute-based encryption with a symmetric key (ABESK). In ABESK, the data is encrypted using a symmetric key encryption algorithm, and the key is then encrypted using attribute-based proxy re-encryption. This allows the encrypted data to be securely shared with users who have specific attributes without revealing the original symmetric key

2.2 ASYMMETRIC-KEY ENCRYPTION

This asymmetric encryption technique uses two different keys for encryption and decryption. One key is used to encrypt the data, and the another key is used to decrypt the data. Asymmetric encryption, PHR (Personal Health Record) attribute-based proxy re-encryption (ABPRE), and keyword-based data access control can be combined to provide a powerful solution for secure and efficient data sharing with complex access requirements.

Asymmetric encryption uses two different keys: a public key for encrypting data and a private key for decrypting it. In the context of data sharing, the public key is typically used to encrypt data that is then shared with other parties, while the private key is kept secret and used to decrypt the data only by authorized parties-ABPRE allows for the efficient and secure sharing of data with different access requirements. This is achieved by re-encrypting the data with different attributes based on the access requirements of the parties involved. For example, a doctor may be granted access to a patient's full medical record, while a nurse may only be granted access to certain parts of the record.

Keyword-based data access control allows for the retrieval of data based on specific keywords or phrases, without the need to decrypt the entire dataset. This can be useful in scenarios where only certain information is needed, such as when searching for specific symptoms or conditions in a patient's medical record. By combining these three concepts, asymmetric encryption with PHR-ABPRE and keyword-based data access control allows for the efficient and secure sharing of data with complex access requirements. Data can be encrypted using asymmetric encryption, re-encrypted using PHR-ABPRE with different attributes based on access requirements, and then searched using keyword-based access control. This provides a powerful tool for secure and efficient data sharing in scenarios where access requirements are complex and varied, while still preserving the confidentiality of the underlying data

3.METHODOLOGY

Attribute-based proxy re-encryption (ABPRE) is a cryptographic technique that allows a proxy to transform ciphertext encrypted under one attribute into a new ciphertext that can be decrypted by a user with a different attribute, without learning anything about the underlying plaintext. Attribute-based proxy re-encryption with keyword search (ABPRE-KS) is a technique used to enable secure sharing and retrieval of encrypted data in a cloud environment while maintaining the privacy of users. In the context of health records, ABPRE-KS can be used to permit the patients to securely share their medical data with healthcare providers or researchers.

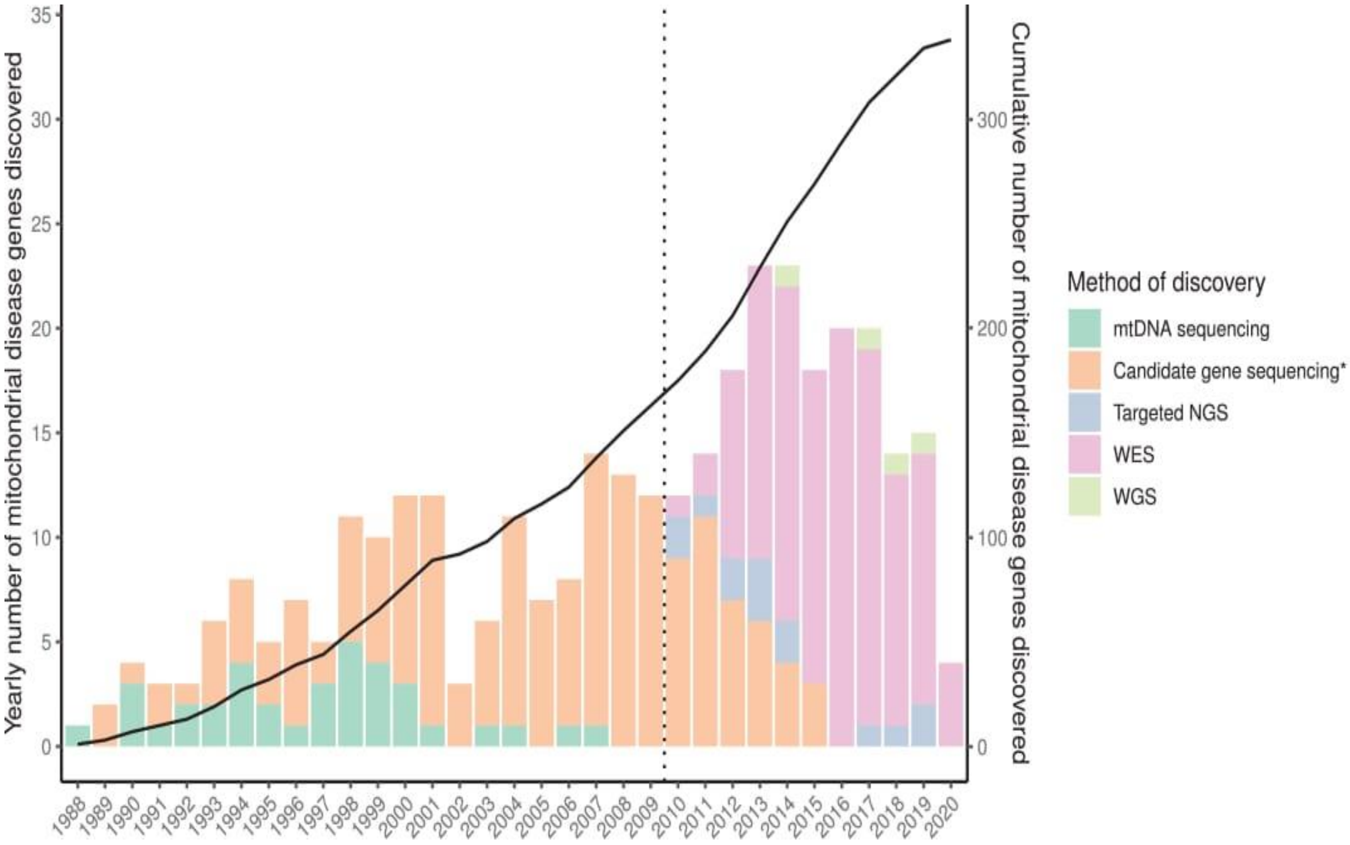

Fig.1. Methods of Disease Genes Discovery

There are several methods involved in implementing ABPRE-KS for health records:

3.1 KEY GENERATION

In ABPRE, a user generates a public key and a private key. The public key is used for encrypting messages, and the private key is used for decrypting messages. The key generation process involves generating keys based on user attributes and keywords associated with the attributes. A user generates a public key and a private key. The public key is used for encrypting messages, and the private key is used for decrypting messages Key generation is an important aspect of many cryptographic systems, including those used in image detection algorithms. The purpose of key generation is to create a unique and secure key that can be used to encrypt and decrypt data.

3.2 Attribute-Based Encryption (ABE)

ABE is a cryptographic technique that allows data to be encrypted and decrypted based on a set of attributes. In the context of health records, attributes can represent patient information, such as age, gender, and medical conditions. ABE enables access control policies to be enforced, such as only allowing doctors with specific attributes to access certain medical records. It is a type of public-key encryption that allows data owners to encrypt data using a set of attributes as the encryption key. The data can then only be decrypted by someone who possesses a decryption key that satisfies a set of attributes specified by the data owner.

3.3 PROXY RE-ENCRYPTION (PRE)

Proxy Re-Encryption is a cryptographic technique that allows an intermediary to transform an encrypted message from one key to another without revealing the contents of the message. In the context of health records, PRE can be used to enable patients to delegate access to their medical records to healthcare providers or researchers without revealing the contents of the records. It allows a third party, known as the proxy, to transform a ciphertext encrypted under one key into a ciphertext that can be decrypted under a different key, without revealing the original plaintext or the secret keys. The process of transforming the ciphertext is known as re-encryption.

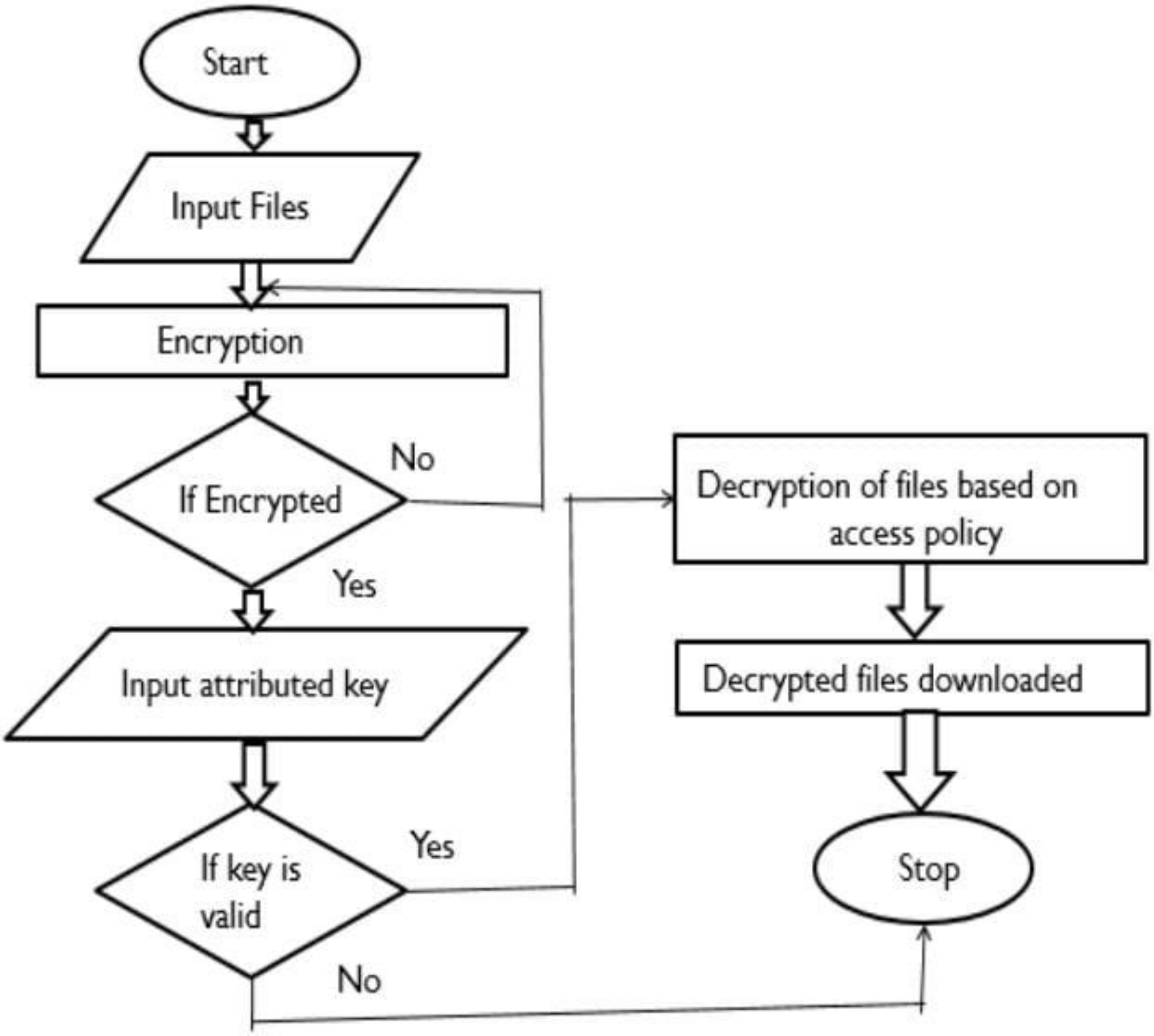

Fig.2. Attribute Based Encryption

3.4 KEYWORD SEARCH

Keyword search enables encrypted data to be searched for specific keywords without revealing the contents of the data. In the context of health records, keyword search can be used to enable healthcare providers or researchers to search for specific medical conditions or treatments without revealing the identity of the patient.

3.5 ATTRIBUTE-BASED PROXY RE-ENCRYPTION (ABPRE)

ABPRE combines ABE and PRE to enable secure sharing of encrypted data based on attributes. In the context of health records, ABPRE can be used to enable patients to delegate access to their medical records to healthcare providers or researchers based on specific attributes, such as medical condition or geographic location. It is commonly used in cloud computing environments where data needs to be securely shared among different users with different access levels. It allows a user to delegate decryption rights to another user, based on attributes such as job title or security clearance, without revealing the underlying plaintext to the proxy.

4.SYSTEM ARCHITECTURE

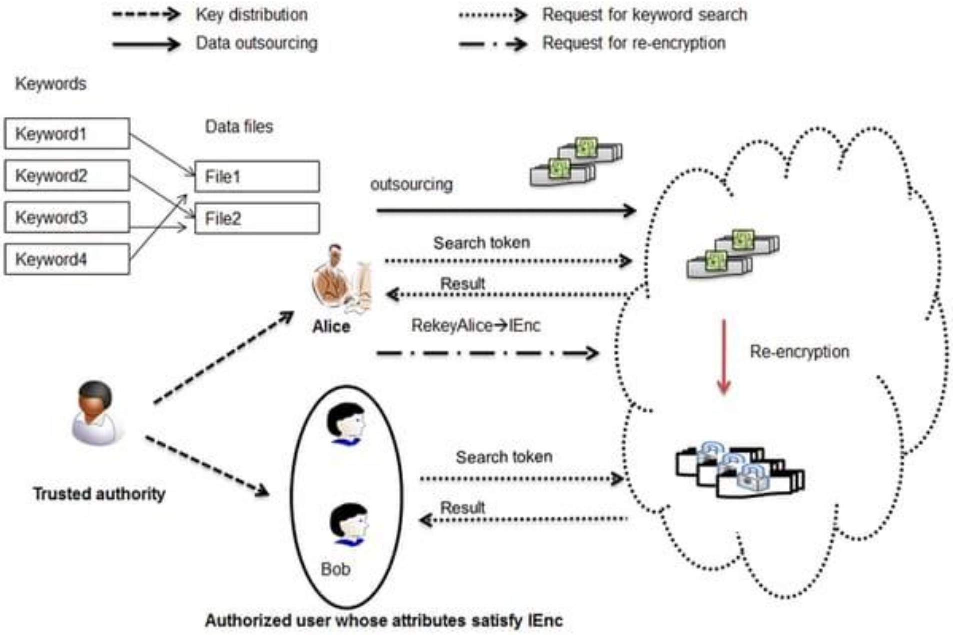

Fig.3. System Architecture

5.MODULE

5.1. KEY MANAGEMENT

This component manages the public and private keys of the various entities involved in the AB-PRE-KS scheme, including healthcare providers, patients, and other authorized parties. The keys are generated based on the attributes of the data and the access policies defined by the data owner. The keys are generated in such a way that only the authorized users who satisfy the access policies can decrypt the data.

The keys are distributed to the authorized users who are allowed to access the data. The key distribution process must be secure and ensure that the keys are only distributed to the authorized users. If an authorized user's access to the data is revoked, their key must also be revoked to ensure that they cannot access the data anymore. The key revocation process must be implemented carefully to ensure that the revoked key is not used by unauthorized users.

5.2. Encryption/Decryption

This component provides functions for encrypting and decrypting health records using the AB-PRE-KS scheme. It enables authorized users to encrypt a health record with the patient's attributes and keywords associated with the record, and then re-encrypt it with a proxy key, which can be used by other authorized users to access the record.

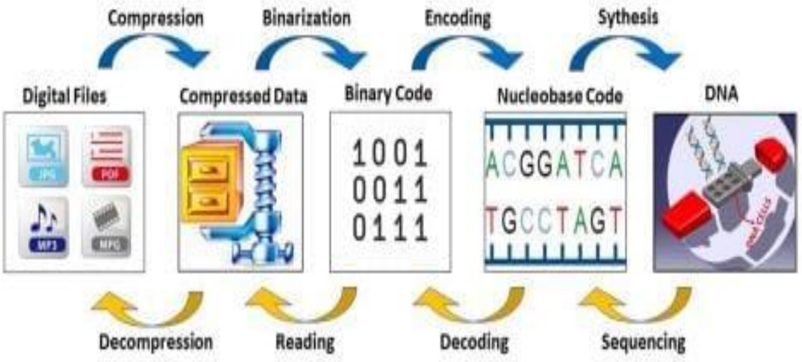

Fig.4. Encryption/Decryption Process

5.3 Search functionality

This component enables authorized users to search for and retrieve specific health records based on keywords or attributes associated with the records. It provides mechanisms for securely querying the encrypted records and retrieving only the records that match the specified search criteria.

When a search query is submitted, the system compares the query image features to the indexed features to find the most similar images. The similarity can be measured using techniques such as Euclidean distance, cosine similarity, or correlation. search functionality in image detection algorithms can provide efficient and accurate identification of specific objects or patterns within an image, enabling a wide range of applications in fields such as computer vision and medical image.

5.4 Revocation functionality

This component provides mechanisms for revoking access to a health record, in case an authorized user's privileges need to be changed or revoked. This is essential for ensuring the security and privacy of health records, especially in case of unauthorized access or breaches.

5.5 FLOW OF DATA

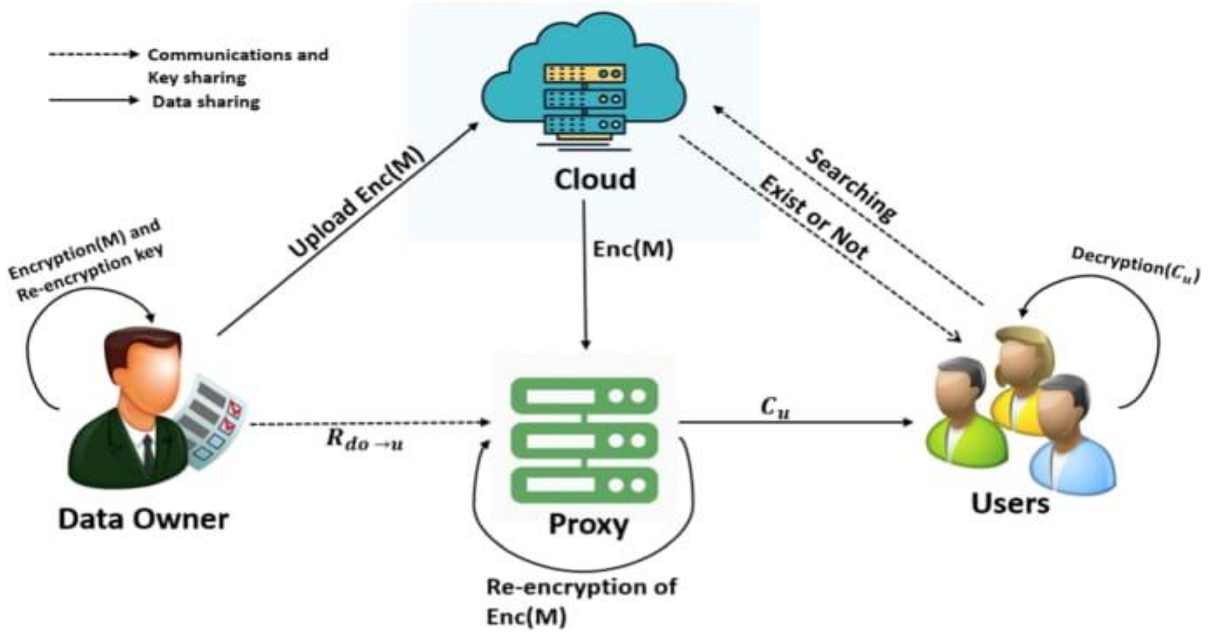

Fig.5. Data flow diagram

CONCLUSION

In this paper, we propose an original fractional picture based homomorphic conspire is proposed for protecting the security of information caught from clinical picture . The proposed conspire permits search at the pixel level and uses Paillier homomorphic encryption. The created search question/secret entryway is likewise probabilistic, prompting keeping up with indistinctness. The proposed approach is in this manner alluded to as a security safeguarding accessible encryption scheme.In the future we are the arrangement of upgrading our venture by identifying high precision level of sickness in DNA individual wellbeing record.

REFERENCE

[1] W. M. Tierney, J. C. Leventhal, J. A. Cummins, P. H. Schwartz and D. K. Martin,“Designing a system for patients controlling providers’ access to their electronic health records: Organizational and technical challenges,” J.General Internal Med., vol. 30, no. 1, pp. 17–24, 2015.

[2] Google Inc. Google Health. [Online]. Available: https://www.google.com/health, accessed Jan. 1, 2013.

[3] Microsoft.Microsoft HealthVault. [Online]. Available: http://www.healthvault.com, accessed May 1, 2015.
[4] K.Omote, K.Emura and A.Miyaji, “A timedrelease proxy re-encryption scheme,” IEICE Trans. Fundam. Electron.,Commun.Compute. Sci., vol. 94, no. 8– pp. 1682–1695, 2011.
[5] Q. Liu, J. Wu and G. Wang, “Time-based proxy re-encryption scheme for secure data sharing in a cloud environment,” Inf. Sci., vol. 258, pp. 355– 370, Feb. 2014.
[6] H. Zhang, F. Gao, M. Ding, and Z. Jin, “An efficient public key encryption with conjunctive keyword search scheme based on pairings,” in Proc. 3rd IEEE Int. Conf. Netw. Infrastructe.Digit. Content (IC-NIDC), Beijing, China, Sep. 2012, pp. 526–530.
[7] P. Liu and C. Hu, “An enhanced searchable public key encryption scheme with a designated tester and its extensions,” J. Compute., vol. 7,no. 3, pp. 716–723, 2012.
[8] D. H. Lee and J. W. Byun “On a security model of conjunctive keyword search over encrypted relational database,” J. Syst. Softw., vol. 84, no. 8, pp. 1364–1372, 2011.
[9] W. Susilo, L. Fang, J. Wang and C. Ge, “Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search,”Theoretical Compute. Sci., vol. 462, pp. 39– 58, Nov. 2012.
[10] D.Cashet al.,“Dynamic searchable encryption in very-large databases: Data structures and implementation,” in Proc. Netw. Distrib.Syst. Security Symp. (NDSS), Feb. 2014, pp. 1–32
[11] Ziqing Wang, Yi Ding, Weidong Zhong and XuAn Wang, “Proxy re-encryption with keyword search from Anonymous Conditional Proxy Reencryption,”2011 Seventh International Conference on Computational Intelligence and Security
[12] J. Wang, C. Ge, L. Fang and W. Susilo, “Public key encryption with keyword search secure against keyword guessing attacks without random oracle,” Inf. Sci., vol. 238, pp. 221–241, Jul. 2013.
[13] Y. Zhang, J. Li and Y. Shi, “Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage,” Int. J. Commun. Syst., doi: 10.1002/dac.2942, 2015.
[14] J. H. Park, W. Susilo, H. S. Rhee and D. H. Lee, “Trapdoor security in a searchable public-key encryption scheme with a designated tester,”J. Syst. Softw., vol. 83, no. 5, pp. 763–771, 2010.
[15] W. Susilo, J. Baek and R. Safavi-Naini, “Public key encryption with keyword search revisited,” in Proc. Int. Conf. ICCSA, vol. 5072.Perugia, Italy, Jun./Jul. 2008, pp. 1249–1259.
[16] H. S. Rhee, J. H. Park, and D. H. Lee, “Generic construction of designated tester public-key encryption with keyword search,” Inf. Sci.,vol. 205, pp. 93–109, Nov. 2012.
[17] Fang LM, Susilo W, Ge CP, Wang JD (2012) Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search. Theoretical Computer Science 462: 39–58**.**