International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 11 | Nov 2019 www.irjet.net p-ISSN: 2395-0072

Comprehensive Study of E-Health Security in Cloud Computing

Ravi Bhagyoday[1], Chintan Kamani[2], Dhrumil Bhojani[3], Vivek Parmar[4]

[1,2,3,4]*B.Tech Cloud Technology and Information Security, Ajeenkya DY Patil University, Maharashtra, India*

Abstract - *Cloud movement have driven it to be adjusted in numerous viewpoints and application that serve human requests. One of the ongoing patterns in distributed computing is the e-health administrations, the same number of medicinal services organizations have started to exchange toward the digitized form of health records. E-health give simple sharing of individual social insurance records between numerous associations and offered real time monitoring for the patient's state by means of putting away this information over the cloud servers. Notwithstanding, having the information in such a disseminated setting rises the requirement for having a verified information imparting to fine-grained get to control, as the records are put away in a third party service provider. Additionally, a wide range of parts of security ought to be taken into check with e-health, for example, the information is basic and ought to be just accessible to its proprietors. Various works have been done to secure the medical data in cloud environment. This work centers around the security difficulties and answers for on Cloud-based E-health frameworks. In particular, a best in class is exhibited to safeguard and secure E-health information, which comprises of two levels: cryptographic and non-cryptographic methodology. Likewise, portions of the fundamental issues and open issues that can be utilized in future investigations are called attention to in this work.*

Key Words: e-health, electronic health record, EHR cryptographic, non-cryptographic, security, privacy, cloud.

1. INTRODUCTION

The application of information technology in healthcare (healthcare IT) has become important to an increasing extent in many countries from the beginning of the 21st Century. There is a moderate and organized transformation in healthcare systems from paper based records to electronic records, which is the mark of something new in the healthcare industry. Such growths provide high efficiency and flexibility on national and international standardization for interoperability and data exchange to the healthcare industry by providing a platform that shares healthcare data among different stakeholders. This advancement in technology has various applications such as Electronic Medical Records (EMR), Electronic Health Records (EHR), Personal Health Records (PHR), and Electronic Health Data (EHD). EHR and EMR are health records of patients handled by healthcare professionals, whereas PHR carry personal data, which is handled and monitored by either patient or their relatives on a regular basis. EHD as electronic health records or computerized patient records is a systematized collection of smart health records of patients [2] . These records are comprised of a wide variety of data, such as medical histories, demographics, medication, immunization status, laboratory test reports and other sensitive patient information. EHD systems have remarkable benefits over conventional paper based records. Unlike paper-based records, EHR incurs less manpower, time and physical storage [3]. Cloud computing is a new digital technology paradigm and is commonly used in the healthcare sector [4]. It not only offers convenient processing of medical information, but also enables simple sharing or transfer between different stakeholders of medical information. The widespread proliferation of health information in the age of big data involves the emerging function of cloud networks not only to host infinite amounts of data, but also to promote their Internet access. [5]. In the healthcare sector, although the EHRs face various challenges in terms of privacy and unauthorized access, information privacy and security are the most prominent of these challenges[6]. Risks range from ransomware attacks, which jeopardize the security and privacy of medical data, to Distributed Denial-of-Service (DDoS) attacks, which are capable of depriving the networks of efficient patient care. Cyber-attacks, such as those triggered by Ransomware, have more consequences than financial loss or invasion of privacy [7]. It is the duty of health care providers to protect the privacy of patient data [8], according to the Health Insurance Portability and Accountability Act (HIPAA). Several approaches are already being used in the cloud environment to protect the security and privacy of smart health systems.

1.1 Motivation

Current privacy mechanism is not sufficient to ensure proper security in the e-health cloud computing methods. The biggest risk faced by health records hosted in cloud is internal attacks from people who have access to the credentials within an organization, which is a lot more worse and dangerous than the external attacks. This research targets to provide a full overview of the strengths and weaknesses of current security mechanisms in e-health environments that make EHR vulnerable to attacks in the cloud industry. EHR contains different confidential and important information varying from patient personal data to financial information, which in case of leakage not only opens sensitive patient information but also causes financial loss.

The current propelled encryption methods, for example, Attribute Based Encryption (ABE) is wasteful to determine this issue because of its costly calculation [2]. The greater part of the current answers for Key Policy Attribute Based Encryption (KP-ABE) and Cipher text Policy Attribute Based Encryption (CP-ABE) expect that a solitary key administration focus picks an ace key arbitrarily and

produces unscrambling keys for clients based on ace key. For the situation where the key supervisor is an aggressor, these arrangements cannot keep from within assaults. The insider dangers in medicinal services incorporate the burglary of PHI, for example, Social Security Numbers or individual data for wholesale fraud and extortion, robbery of Intellectual Property and damage. Other non-noxious dangers incorporate the unintentional misfortune/exposure of touchy data, for example, revealing delicate tolerant data to other people, sharing login qualifications, recording login accreditations, or reacting to phishing messages. For instance, the biggest human services information break in history is the robbery of 80 million social insurance records from Anthem Inc. [9]; American Health Insurance Company is accepted to have been made conceivable because of taken accreditations. Information encryption, secure stockpiling, verification, get to control, key administration, effective client denial and so forth are yet to be tended to and settled. This paper examinations existing protection safeguarding approaches, their qualities, downsides, investigate issues and concocts another worldview bolstered by block chain innovation that can balance certain weaknesses yet in addition guarantee a structure for giving proficient protection saving and security in e-health data.

1.2 Methods

This section starts with the study selection to guarantee the precision of search and recovery process. The study limits to publications from various electronic databases related to health care that attempts to gather relevant experimental confirmations in a specific field to evaluate the methods fundamentally and to acquire ends to abridge the exploration study. This section additionally plays out security and protection safeguarding investigations of EHR as a piece of qualitative data analysis that makes it simple to compare, break and analyze the core of the work.

Table -1: Literature review

Publisher	Source	Keywords
IEEE	IEEE Journal of Biomedical and Health Informatics	EHR
	IEEE Access	e-Health
	IEEE International Cloud Computing Conference	e-Health privacy and security
	IEEE Transactions on Cloud Computing	Cyber-security attacks
	High Performance Computing and Communications	EHR Cryptographic Approaches
	IEEE Transactions on Information Technology in Biomedicine	EHR Non-Cryptographic Approaches
	IEEE open and big data conference	Security and Privacy of EHR in cloud
	IEEE Transaction on Information Forensics and Security	
ACM	ACM workshop on Cloud computing security	
	ACM International Health Informatics Symposium	
Google Scholar	Journal of Cyber Security	
Scopus	International Journal of Medical Informatics	
	Journal of Medical systems	
	Journal of Cloud Computing	
	Future Generation Computer Systems	
	International Journal of Security and Networks	
	Security and Communication Networks	

1.2.1 Literature Review – Study Selection

This study performs a systematized audit of security and privacy preserving approaches of EHRs in the cloud from various databases, including IEEE, Google researcher, PubMed, ACM, Springer and Scopus. The definite summary and the keywords utilized for searching is shown in Table 1. This work additionally includes a broad survey of noteworthy audit papers distributed between 2000 and 2019.

In this research, we have collected relevant papers published between 2000 and 2019, and found almost 87 research papers and articles. Then we reduced those papers based on quality, title, authors name, relevant abstract and keyword significance. After this filtration, we were left with 59 relevant papers and articles.

1.2.1 Categorizing Security and Privacy Preserving Studies

Initially, this review researches the security and privacy prerequisite of E-health data in cloud arena. On the other hand, after recapping a brief structure of e-Health system, a prevailing and updated review of the E-health clouds is presented using a floristics over privacy preserving approaches. The survey then discusses the merits and faults of the updated mechanisms and finally highlights some future research directions and open research issues. The rest of this study is recognized as follows.

In section 2, we discuss the security and privacy requirements of e-health data in the cloud. Section 3 E-health Overview, Section 4 reviews an enhanced analysis of security and privacy preserving mechanisms employed in the E-health cloud environment. Section 5 describes research issues and future paths, and Section 6 as conclusion.

2. Security and Privacy Requirements of e-Health Data in Cloud

In the current Enormous information age, data proliferation demands re-appropriating of healthcare information to the cloud servers. Notwithstanding the enormous help given by the cloud, it additionally involves the potential threats to security and protection of healthcare data [1]. A portion of the potential attack incorporate data divulgence, Denial of Service attack (DoS), cloud malware injection attack, man-in-the middle crypto-graphic attack [10],spoofing [11], collusions attack [12].The cloud service provider and numerous administration associations have proposed an assortment of security measures and guidelines and improve the certainty of patients and organizations. The principal such administrative measure set forward by the US Congress in 1996 for the US healthcare industry was the (HIPAA) [8]. There are mostly three classes of cloud servers: trusted servers, semi-trusted, and untrusted servers. A trusted server is one that can be totally trusted with no data exposure and dangers to the healthcare data stored can be due to internal adversaries [13]. Semi trusted servers are straight forward however inquisitive servers that get healthcare data by plotting with malicious clients [14] while untrusted servers are not trustworthy with no privacy mechanisms components and are defenseless against assaults from both interior and outer adversaries [15] as appeared in Fig 1.

The vital security and privacy requisites in e-health models are: 1) Data integrity-ensures that the health information has not been modified by any unauthorized entity. 2) Data confidentiality guarantees that the delicate health information is prevented from arriving at unauthorized clients. Data encryption is the most generous way to deal with guarantee data confidentiality. 3) Authenticity- ensures that only the authorized and authentic authority should have access to the sensitive health data 4) Accountability- an obligation to be responsible and to justify the actions and decisions of individuals or organizations. 5) Audit is a prerequisite, which guarantees that the health information is checked and secured by monitoring the action log, and guarantees affirmation to the clients associated with data protection and security. 6) Non-repudiation- refers to the non-denial of authenticity of sender and receiver. For example, the patients or the specialists cannot revoke after misappropriation of health information 7) Anonymity - ensures that the identity of the subject can be made anonymous so that the cloud servers fails to access the identity of the stored health data.

3. Overview of e-Health System in the Cloud

E-health model is an ongoing medicinal services advancement using electronic procedures and correspondence. In an e-health model, EHR or EMR is a systematized accumulation of electronic health data of patients [2]. These records include all the health information data including demographics, medical histories, lab reports, radiology pictures, billing data and any extra delicate patient data. The cloud offers incredible support to both healthcare services providers and patients the same in terms of cost effective storage, processing and updating of information with enhanced efficiency and quality. Since this information is put away in different servers, it very well may be effectively available to clients from different areas on request. E-health model guarantee fast, resolute and on-request access to medicinal records, upgraded social insurance quality, anyway they similarly uncover understanding security, by means of ill-advised approval and abuse of EHR information. In this manner, security and protection are viewed as basic prerequisites when sharing or getting to persistent information between a few partners. A review of e-health model is delineated in Fig 1.

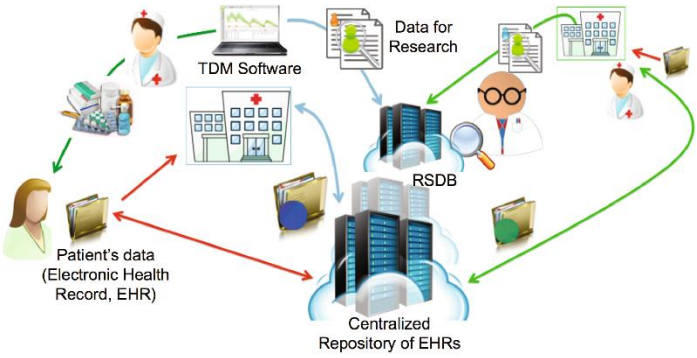


Fig - 1: Architecture of electronic health data in cloud

E-health cloud model types can be open, private, hybrid and community as per the information put away. Since EHR information is confidential, consists of patient data that are housed in third-party servers, access control mechanisms are required. Access control is a security hindrance, which preserves data privacy by confining the operation and access of healthcare documents in the healthcare system. The access control procedures in the healthcare systems are Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC) and Identity-Based Access Control (IBAC) methods. Role-based models [16] accommodate the task of assigning roles to the clients for data access. ABAC [17], which utilizes cryptographic and non-cryptographic strategies, though IBAC utilizes identity based encryption mechanism that uses client identity for data encryption. Information sharing is a particular component of e-health systems. It very well may be shared among different stakeholders, for example, healthcare providers, emergency clinics, medicinal services associations, and so on. Search is another considerable capacity of an e-Health model. Proxy

encryption and public key encryption are generally utilized encryption procedures for data search.

3.1 CLOUD COMPUTING SECURITY: STATE OF THE ART AND RESEARCH CHALLENGES IN E-HEALTH

Cloud computing has seen a colossal development that has changed the scene of figuring with its storage, flexible resources and decreased costs to such an extent that, it prompted numerous associations to move their information in the cloud. Despite the fact that cloud administrations give enormous benefits, regardless it experiences a few security dangers. For example, clients do not know about the massive amount of data stored put away with the cloud service provider [18]. Because of absence of lucidity, it is hard to know about where, how and when the data is prepared and subsequently makes it hard to confide in the service provider, who thus can likewise be an explanation behind huge data loss. There have been a few plans and improvements in the area of cloud security.

Some of the advanced privacy-preserving mechanisms that preserves cloud security can be embraced to e-health, while some are not because of security concerns. Cloud computing does cloud supplier, which is less patient-driven and is prone to insider attack, which makes it more vulnerable; own a centralized mainframe-computing paradigm. This is one of the significant drawbacks of cloud computing. Despite the fact that cloud strategies stick to severe safety efforts, it does not offer a reliable answer for adopted into e-health, assessed its security issues. Zhu et al. [19] proposes an efficient privacy preserving biometric identification scheme in which a tremendous volume of biometric information, for example, fingerprints, irises, voice patterns, facial examples are encrypted and redistributed to the cloud to evade costly storage and computation costs. The scheme is safe against intrigue attacks and gives the greatest degree of data privacy. This methodology can be applied to e-health cloud for proficient data storage in which the health records can be encrypted and put away in the cloud that accomplishes a specific degree of data protection. Nonetheless, as the health records are very sensitive and the data exposed to the database owner, this scheme is less satisfactory as far as security. Likewise, this scheme cannot be considered for EHRs, as it shows no restraint driven and computationally infeasible for genuine issues. This work [20] proposes a powerful and variable half and half multi authority CP-ABE get to control plot by consolidating (t, n) edge mystery sharing and multi-authority CP-ABE conspire for open public storage with which both security and execution are improved by overcoming the single point bottleneck issue. Xu et al. [21] proposes a strong and productive access control scheme that resolves the single-point execution bottleneck in a large portion of the current CP-ABE utilizing an examining instrument. Despite the fact that these schemes [20], [21] are advanced get to control schemes that has high security measures, they can't be received assuredly to e-health as these schemes can't ensure protection from insider attacks since it is constrained by Central Authority and different Attribute Authorities. A special encryption procedure named Deniable ABE conspire dependent on Waters cipher text policy-attribute based encryption (CP-ABE) scheme was recommended that permits cloud storage suppliers to create cast client secrets from stored cipher text from outside coercers [22]. This scheme consolidates the pros and cons of both ABE and symmetric key encryption a multi-privileged access control for PHRs by combining the encryption of data from multi-patients that falls under the similar access approach [23]. Zhang et al. [24] proposes a productive protection disease prediction expectation scheme by utilizing Single layer Perceptron learning algorithm. This model encrypts the side effect data presented by the patient and the cloud utilizes the encrypted forecast models prepared by it to analyze the patient illness without uncovering the patient privacy. These mechanisms [23], [24] imparts a high level of data privacy, yet at the same time unrealistic for health records because of its computational complexity and scalability issues. Another work introduced an unknown CP-ABE with hidden access arrangement and provides authentic access to control with consistent key length [25]. Wei et al. [26] proposed a revocable storage Identity Based Encryption (IBE) that gives forward and backward security of cipher text. The greater part of the current cloud storage frameworks with secure provenance lacks poor access control, cause extreme performance overhead and do not support dynamic user management. This work solves problems by displaying an attributed based cloud storage framework with secure provenance [27]. Despite the fact that ABE plans are the most effective among encryption systems and give fine-grained, well-framed access to health records, it is still impractical for proper execution on EHRs because of its costly computation [25], [27], key administration complexity and challenge in managing access control policies [22] when attributes in the access structure develops.

Regardless of the appealing features that cloud offers, the progress of healthcare field towards cloud condition builds the worries about privacy, security, access control and consistency because of the inherent security provokes identified with cloud technology. Patients lose their physical control by storing health information in the cloud servers, which can be viewed as a risk to patient privacy. Data security and data integrity have additionally been a difficult issue while storing and accessing data in the cloud field [28]. Another drawback is that cloud service provider have an imperative job in transaction analysis, access control, data protection, and services integration. With the development in technology, the rise of cyber threats has heightened, which prevents the privacy and security of EHRs [29]. In this manner, it is imperative to ensure integrity, confidentiality, reliability just as authenticity of e-health data in a private, either open or hybrid cloud environment. Thus, this work presents the idea of an authorization patient-centric Block chain for EHRs that takes out a large portion of the current bottlenecks in the cloud.

4. Classification of Privacy Preserving Mechanisms in e-Health Records

In this paper, various strategies dependent on cryptographic and non-cryptographic methodologies are utilized dependent on their utilization of healthcare system in the cloud field. Likewise, a few methods are analyzed that preserve data security, data protection and data secrecy in the cloud. Besides, some Searchable Encryption (SE) methods are displayed to query the encrypted information in the cloud. As the information is encoded and put away in outside cloud servers, ordinary looking plans cannot be applied. Searching encrypted data is difficult, Searchable Symmetric Encryption (SSE) has been proposed that enable keyword searches across encrypted cloud data. Different from the recent surveys, our research study systematically covers all aspects and methods of privacy and security of EHR in cloud.

Numerous approaches have been proposed to preserve the privacy of the patient health data. However, there is no clear classification of the privacy preserving approaches. Therefore, we classify the privacy preserving approaches used in the e-Health clouds into: (a) cryptographic and (b) non-cryptographic approaches at top level. The cryptographic ways to deal with moderate the protection dangers use certain encryption plans and cryptographic primitives. The cryptographic plans utilize encryption methods, to be specific: symmetric key encryption, open key encryption and a few cryptographic natives, while non-cryptographic methodologies incorporate access control systems, for example, RBAC, ABAC, and IBAC and so on.

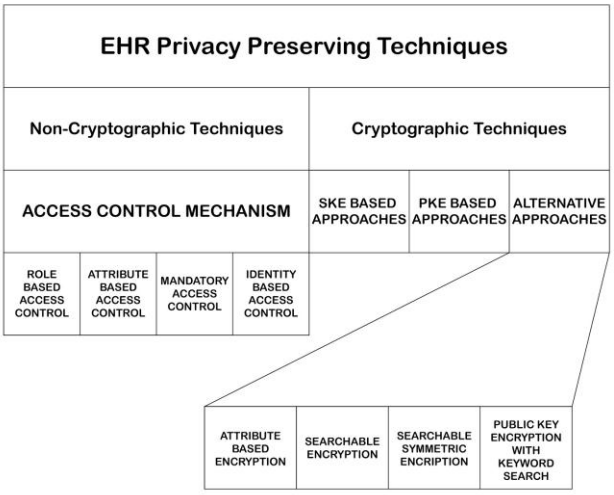


Fig - 2: Classification of Privacy Preserving Mechanisms in e-Health Records

4.1 Cryptographic Approaches

Cryptography is a technique for shrouded composing, i.e. ensuring data and interchanges using conventions with the end goal that those for whom the data is planned can pursue and investigate it. Countless approaches have been proposed to defend the protection of the patient's healthcare information. Nonetheless, the Cryptographic methodologies can be characterized into two sorts, symmetric-key cryptography and Asymmetric-key cryptography (see Fig. 5) in which the earlier uses a similar key for the encryption and decoding while the latter utilizes different keys. The methodologies ordinarily utilized in the e-Health cloud-based models to secure information, use encryption plans, for example, Public Key Encryption (PKE) and Symmetric Key Encryption (SKE). In this area, we quickly characterize and present the methodologies dependent on the PKE, SKE, and a few cryptographic natives that are utilized to safeguard the protection of the e-Health cloud. In PKE, two diverse arrangement of keys are utilized i.e. open key and a private key pair for information encryption and decoding though SKE based methodologies use a solitary shared mystery key for the equivalent.

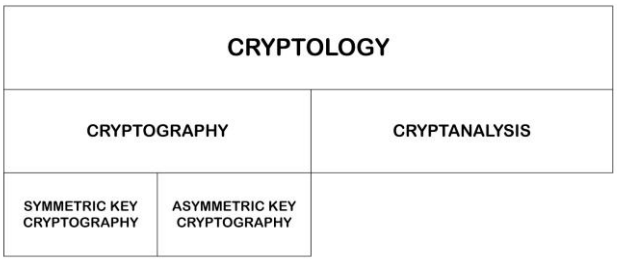


Fig - 3: Basic types of cryptography

4.1 SKE Based Approaches

The SKE utilizes the same-shared key for encryption as well as decryption and it is profoundly powerful in EHR structure. Yet, it presents unavoidable extra complexity since it requires additional access control mechanisms for the effective sharing of EHR. The normally used SKE based algorithms are Data Encryption Standard (DES), Advanced Encryption Standard (AES), stream ciphers such as A5/1, RC4, and Blow Fish and show on.

A secure EMR sharing has been proposed by Li et al. [30] to move forward the unsinkability between patient and EMR. EMRs are encrypted using symmetric key encryption using a one-time key and records are stored namelessly. Doctors use digital signatures using a private key to handle electronic medical records. This approach requires an EMR number i.e. the PID, SID, the identity seed that is stored within the patients' medical card and the random value R, which was made by the doctor to get to the EMR of the patient. For encrypting one EMR, every key is used in this method, which increases confidentiality of each electronic medical record. Identity seed SID is based on smart data card and medical records therefore it cannot be read without permission.

An EHR sharing and integration system has been proposed by Chen et al. [31] to secure the EHRs in normal and emergency circumstances in hybrid healthcare clouds. In this approach, each medical record used an individual symmetric

key using a symmetric encryption scheme in private and public cloud environments. Here, the specialist makes the patients' health record and it is scrambled by the symmetric key alongside a permit License. This license gives an emergency key to get the encrypted data by the cloud in case the server is not given with access. The patient needs to give the smart card to the doctor for the decryption of their EHR. This plan encrypts all the medical records and decryption is conceivable as it were by patients' private keys in which the private key is part into two parts, though the hospital server will escrow one among the keys and the other key will be put away on the patient's smart card. The drawback of this approach is that the permit license too ought to be encrypted with the hospital's public key as searching encrypted information is challenging, Searchable Symmetric Encryption (SSE) [32] has been proposed that enables keyword search over encrypted cloud data. This approach presents an exceedingly efficient and Secure Energetic Searchable Symmetric Encryption (SEDSSE) in medical cloud data by leveraging the secure k-nearest neighbor (kNN) and ABE methods. This approach utilized an AES symmetric encryption algorithm to encrypt the records and shares the symmetric secret key as it were with authorized doctors who fulfill the get to policy related to ABE.

4.2 PKE Based Approaches

In PKE approach, there are two Different keys.

1. Public Key
2. Private Key.

PKE techniques are arithmetically less efficient because of its slower Processing and large key sizes. Therefore, PKE techniques can be highly efficient in combination with SKE techniques in which SKE techniques is used for encrypting the Data and public private key pairs are used to secure the symmetric key.

This structure [33] utilizes Public Key Infrastructure (PKI) to guarantee security necessities, for example, confidentiality, integrity, access control and non-repudiation, EHR is encrypted utilizing a shared symmetric key created by healthcare providers. PKI ties public keys with exceptional client identities, which comprise digital certificates, a Registration Authority, a Certificate Authority, a Certificate Repository Database, and a Certificate Management System. This proposed design manufactures a protected EHR sharing system that guarantees the compelling sharing of EHRs among patients and a few healthcare providers. Authentication between EHR sharing cloud and healthcare providers is accomplished by marking the archives with the sender's private key, therefore letting the healthcare provider confirm the mark signature to recover the identical health records.

Mashima and Ahamad [15] patterned a patient-centered monitoring system to secure the risk of storing and accessing e-Health data in the cloud. This work evolved a system that allows the patients to have explicit or implicit control related to when and how the e-Health data is accessed.

4.3 Overview of Alternative Cryptographic Primitive Approaches

This section addresses an overview of alternative cryptographic approaches in e-health clouds to protect confidentiality. The primitives are ABE, SE, homomorphic authentication, re-encryption of proxies, etc.

4.3.1 ATTRIBUTE-BASED ENCRYPTION (ABE) APPROACHES

Sahai and Waters [34] attribute-based authentication is based on public key encryption to secure cloud data where user attributes are used for encryption and decryption. The encryption in ABE is based on the access-structure principle where the cipher text can only be decrypted if the user attributes match the cipher text attributes. Cipher text Policy-Based Encryption (CP-ABE) [35] and Key Policy Attribute-Based Encryption (KP-ABE) are the two main types of ABE. In KP-ABE, the access policy is encrypted into the user's secret key and decryption of cipher text is only possible when the user's attribute matches the access policy [34], while in CP-ABE [36] each user's private key is linked to a set of attributes and a cipher text is linked to a universal set of attributes that can be decrypted when the user's attributes match the access policy. This approach based on ABE [37] protects EHR's privacy with PKE for flexible authorization. The patient's smartcard produces a secret authorization Transaction Code (TAC) before uploading the medical data to the cloud server. PKE is used as identification and for authorization the patient's smart card and TAC.The health professional has to access the TAC to decrypt the medical data, and the Encryption / Decryption feature provides a shared encryption key that is the hash value of the patient's identity and TAC.The decryption can be done using TAC and authentication from a Private Key Generator (PKG). Yu et al. [14] lists the problem of confidentiality, scalability, and fine-grained access to outsourced data in the cloud. This method solves problems by incorporating strategies such as ABE, KP-ABE, Proxy Re-encryption (PRE) and lazy re-encryption as a hybrid encryption scheme to secure fine-grained access control. Through key distribution, the information encrypted by a single user will be exchanged among different users.Re-encryption of data files and secret key updates are consigned to cloud servers in this method. Cloud servers keep a copy of user's secret key to update secret key components and re-encrypt data files. Lazy re-encryption is used in cloud servers to reduce overhead computing. It can stop the revoked users from collecting the updated information once the file contents and keys have been changed after the revoke of the client.

4.3.2 SEARCHABLE ENCRYPTION

Because of the enormous development of huge data, there exists huge scale re-appropriating of data into cloud servers. As medical data and EHRs are redistributed to remote cloud servers that are presented to cloud services, this prompts different attacks, for example, either DoS attack or adversary attack that annihilates the data confidentiality in the cloud. For security of data and prevention of data leakage, cloud data will be encrypted. Since the health data is encrypted and put away in outside Cloud servers, ordinary looking through plans cannot be applied. It requires some accessible encryption usage to question the data as appeared in Fig. 6. As searching encrypted data enable keyword searches across, it is challenging. SSE has been suggested that cloud information. These stances difficulties, for example, (1) how the data owner grants search consents to the data client? (2)How the verified data clients search the encrypted stored data? One of the arrangements is SE. SE is a cryptographic primitive that licenses search tasks over encrypted data without uncovering the data to untrusted servers. These search activities are performed on encrypted cipher text with the help of a trapdoor function from client. The fundamental two sorts are symmetric searchable encryption and asymmetric searchable encryption.

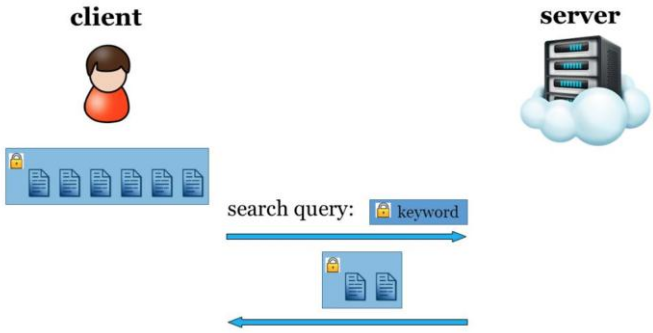


Fig - 4: Searchable Encryption

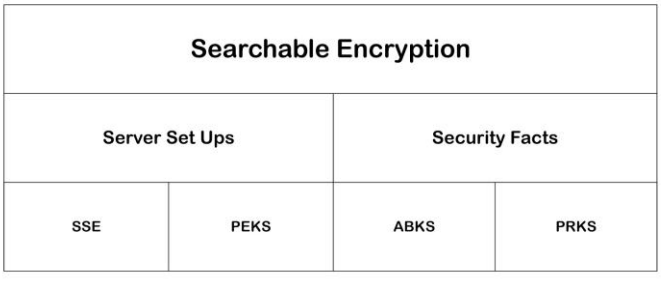


Fig - 5: Classification of SE techniques.

4.3.2.1 Searchable Symmetric Encryption (SSE)

SSE is a symmetric key encryption procedure, which outsources the information confidentially from one party to another by giving particular look capabilities. This model uses proxy re-encryption[58] that offers medical information within the cloud with end-to-end information encryption that cones information get to as it were to confirmed beneficiaries. This approach [39] conserves the privacy and security in e-Health models with a modern cryptographic procedure named as a conjunctive keyword search with assigned analyzer and timing subordinate SE plans named intermediary re-encryption work (Re-dtPECK). The EHR reports are encoded by symmetric encryption calculations and a symmetric key is summarized with the patient's open key-by-key embodiment. This makes utilization of an assignment work to perform operations and employ a conjunctive watchword look instrument. This approach proposes a novel SSE conspire [40] which gives looking concurring to the interesting watchwords put away on the server. The look time is logarithmic and the client can look and overhaul the record at whatever point required.

4.3.2.2 Public Key Encryption with Keyword Search (PEKS)

PEKS is a cryptographic approach that uses an open key model to look over scrambled information. Boneh et al. [41] proposed PEKS as an introductory scheme, which does not uncover any data relating to user's searching within the public-key setting and with lesser communication complexity. This strategy [42] proposes a powerless key unsinkability that supply a broader view on trapdoor protection in asymmetric encryption for IBE. The reason of this model is to construct a mysterious IBE scheme that fulfills both key unsinkability and upgraded useful security. This approach [43] addresses three fundamental issues of a PEKS scheme vise evacuation of secure channel, reviving keywords, and processing different keywords. The thought of PKE with keywords search (PERKS) has been displayed by Tang and Chen [44]. This model gives adaptability in such a way that the sender is able to enroll a catchphrase with the receiver prior to the sender producing a tag to construct searchable content. This makes the model more proficient and secure against offline keyword-guessing attacks.

4.3.2.3 Attribute Encryption with Keyword Search (ABKS)

ABKS is a cryptographic search approach that uses data encryption based on attributes. This search technique allows users whose attributes fulfill the access policy to scan keywords over encrypted EHR information. Yang [45] has suggested a multi-sender and client scenario that improves fine-grained access control and facilitates account revocation by using a robust keyword search technique and authentication based on attributes. This scheme implemented a fundamental novel with Synonym Keyword search method (SK-ABSE) called attribute-based searchable encryption. An ABE scheme defined by Li et al. [46] integrates keyword search functions with key outsourcing and decryption (KSFOABE) outsourcing. The cloud service provider undertakes partial decryption tasks assigned by data users in this scheme without providing any knowledge about the plaintext that is secure and resilient against

selected plaintext attacks. Verifiable Attribute-Based Keyword Search (VABKS) solution[47] allows a data user to search only the outsourced encrypted data of the data owner whose credentials suit the access control policy of the data owner. Liu et al. [48] introduced a new approach called Key Policy Attribute-Based Keyword Search (KP-ABKS), which removes from the cloud a secure channel for validating the searched result, which reduces the computational complexity of VABKS.

4.3.2.3 Proxy Re-Encryption with keyword Search (PRKS)

Proxy Re-Encryption with keyword Search (PRKS) PRKS is a cryptographic fundamental that uses a proxy re-encryption system for searching encrypted data. An authenticated user, which gives permits to other clients by re-encrypting the outsourced data, permits by PRKS [38]. The proxy re-encryption with keyword search functions (PRKS) as the union of two schemes, Proxy Re-Encryption (PRE) and PEKS. This approach [49] gives two security concepts for bidirectional PRES (Intermediary Re-encryption Plot): privacy for keyword and privacy for message. In keyword privacy, the adversary is allowed to get the plaintext of any cipher text, and about all trapdoors, barring those, which are associated with the two particular keywords. Overall, it cannot decide which keyword matches to a given cipher text. This security thought ensures that the individual who has the trapdoor or token can as it were do the test. For message security, the opponent is allowed to get the plaintexts of about all cipher texts, excluding all the trapdoors, but it cannot decide which message matches with the specific plaintext. This security concept guarantees that the one who holds the private key can decrypt the cipher texts. We have discussed a study of Searchable encryption techniques for healthcare applications. Be that as it may, all existing multi-user SE schemes are not practical with regard to the execution required by basic real-world applications and don't scale well for broad databases. We categorize and compare the diverse SE schemes in terms of their security, efficiency, and functionality. However, SSE is not a favored strategy [43] for querying the search in EHR due to key administration issues. Overall, PEKS and PRKS exhibit way better execution in terms of security, privacy, and are commonly received to EHR that supports search functionality.

4.3.3 PROXY RE-ENCRYPTION

Proxy Re-encryption may be a cryptographic approach that grants a semi trusted proxy server to re-encrypt the cipher-text, which is encrypted by one user's public key, into another cipher text i.e. encrypted by the public key of another client [50]. For illustration, Alice sends a message (RK) to Bob through a semi-trusted proxy server, without sharing Alice's private key to either the proxy or Bob, and without disclosing the secret message to the proxy appeared in Fig. 8. Yang and Ma [39] presented a novel cryptographic approach called as Conjunctive Keyword Search with an assigned tester and a timing enabled proxy re-encryption function, RedtPECK that uses an assignment pointer θ to perform operations and uses conjunctive keyword for searching mechanism. This scheme proposes a proxy re-encryption instrument [51] for on the road emergencies that permits an emergency medical center to decrypt a patient's health records with the help of cloud servers and client credentials without disclosing the secret key.

Timing enabled proxy re-encryption systems over conjunctive keyword search have been proposed [52] that permit clients to get to the patient records beneath a predefined time interim, T. This strategy accomplishes objectives such as Time based disavowal, Effective Access Control, User revocation, Efficiency.

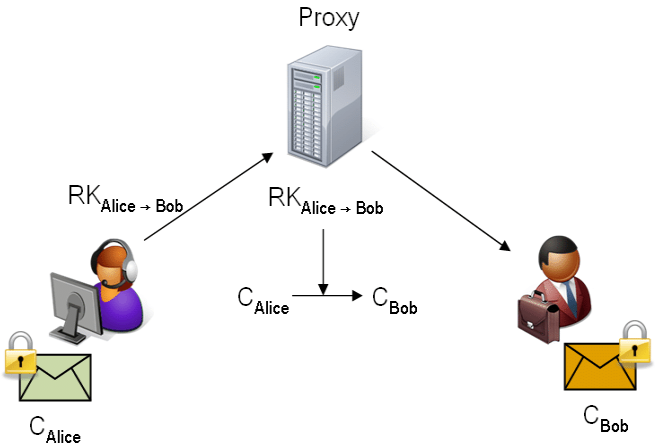


Fig - 6: Proxy Encryption

4.3.4 HOMOMORPHIC ENCRYPTION

A Homomorphic Encryption is the change of data into cipher text that can be analyzed and worked with as if it were still in its original shape. Homomorphic encryption plays a critical portion in cloud computing, permitting patients to store encrypted PHR (Patient Health Record) records in a public cloud and take advantage of the cloud provider's analytic administrations. The scheme avoids rebel insiders from violating privacy and avoids accidental leakage of private data. Homomorphic Encryption systems are utilized to perform operations on encrypted data without knowing the private key (i.e. without decryption); the client is the holder of the secret key. When the result of the operation is decrypted, it is the same as if it had carried out the calculations on the raw data. The homomorphic encryption scheme algorithm consists of four steps: 1. Key Generation - creates two keys i.e. the privacy key sk and the public pk. 2. Encryption - encrypts the plaintext m with the public key pk to yield cipher text C. 3. Decryption - decrypts the cipher text C with the privacy key sk to retrieve the plaintext m 4. Evaluation - outputs a cipher text C off (m) such that Decrypt (skip) = f (m) [59].

4.2 NON-CRYPTOGRAPHIC APPROACHES

Non-cryptographic approaches primarily use policy-based authorization infrastructure such as policies on access control to enforce data privacy control. In EHR systems where access to data is highly confidential and data is stored on third-party servers. Mechanisms of access control are necessary and vital as approaching towards encryption. Access control in a health care information system provides fundamental data privacy and security barriers by limiting document access and operation in the EHR system. Some of the main access control techniques are shown in Fig.10. Comparison of a few non-cryptographic mechanisms that protect privacy is shown in the table 8.

Discretionary access control (DAC) is a form of control of access in which the owner of the object has complete control over the programs. DAC is based on making objects accessible based on the identity of the subject [83].Access policy decisions in MAC are not made by an object's individual owners, but by a central authority, and the owner cannot change access rights [53].RBAC determines access decisions based on their job functions in which tasks are delegated to subjects, and the roles are combined with permissions to determine which activities can be performed on which objects.

ABAC is an authentication-based access control in which access decisions are made in accordance with the set of user-defined attributes and requesters are given access to objects in accordance with attributes that comply with the policy rules.IBAC is a way of regulating access based on an individual's authenticated identity.

Khan and Sakamura [54] suggested, through discretionary access control and RBAC models, a context-sensitive, fine-grained access control system for personal health data. This approach uses eTRON architecture where encryption is done using public-key cryptography, and the Diffie-Hellman algorithm establishes stable key sharing.

Pussewalage and Oleshchuk [55] proposed a patient-centred attribute-based approach in which each PHR file is encrypted and stored in an e-health cloud with an attribute-based access policy, which regulates access to the particular resource and uses a proxy re-encryption technique, which helps authenticated users, decrypt correct PHR files. This scheme can withstand attacks mounted via collusion attribute and can provide client revocation on-demand. This research introduced a BiLayer Access Control (BLAC) to combine attributes with roles and to analyse an access request against pseudo-roles before testing the rules in the law. Sandhu et al. [56] proposed RBAC in which the functions are allocated to subjects and roles are correlated with permissions specifying what behaviour over which objects can be controlled. There are several disadvantages to this scheme. Defining and structuring the functions is an expensive process, and it only supports policies that are stable and pre-defined. It is also unable to support rapidly evolving environments[57], and the coarse-granularity of RBAC also triggers internal attacks[58].Yuan and Tong [17] proposed ABAC to use specific attributes of each subject to explain access permission policies. ABAC solves RBAC issues, but it has two issues.

Initially, ABAC is challenging due to the large number of rules that need to be examined for access decisions, and secondly, ABAC may require 2n rules for n attributes [17].

5 RESEARCH ISSUES AND FUTURE DIRECTIONS

This section talks about the research issues and future directions identified with privacy and security in EHR. Since EHR, data is delicate, confidential, and housed in third-party servers, which involves serious risks as far as data privacy and security goes. A portion of the issues includes:

1. How to verify and safeguard the security of data in the cloud?
2. Which access control system will be increasingly effective for the protected exchange of EHR?
3. Which encryption plan could be utilized for preserving data security?
4. How to actualize security preserved in health care data storage?
5. How the health data can be successfully shared against various healthcare providers?
6. How to keep up with integrity of health records?
7. Who will have the option to get to the patient information with healthcare providers during a crisis circumstance?
8. How to deal with key administration intricacy while sharing healthcare data between different healthcare providers?

This audit featured different research issues relating to the protection and security of e-health data. Along these lines, we found that there is an inevitable need to strengthen the security foundation in e-health models assured towards patients' to guarantee the privacy and security of information accordingly verifying patient privacy and sovereignty. Along these lines, we deliver some future research directions:

- From the discussion, we have inspected a few cryptographic and non-cryptographic components. Despite the fact that ABE is generally productive among encryption plans, Yi et al. [2] investigated and proved that despite the fact that ABE is generally proficient among encryption plans, regardless it experiences costly computation and complexity in bi-linear pairing tasks. Along these lines, perceiving new systems for reducing the

multifaceted nature of bi-linear operations or discovering approaches to re-appropriating calculations will be a fascinating research direction.

- Integrity of health data in the cloud can be another enthusiasm in research direction
- We have watched a few access control systems that guarantee security wherein ABAC is the most adaptable and advantageous giving fine-grained access. Along these lines, ABAC will be productive to bring greater adaptability into authorizations, which can likewise be considered as an examination bearing.
- A blend of encryption instruments and access control systems to save big data security and privacy can also be considered as a future research direction for maintaining a reliable security mechanism in e-healthcare.

6. Conclusion

Since most of the information is put away in cloud servers, which is exceptionally weak to attacks and breaches, thereby leading to an upcoming need to safeguard them. Current e-health solutions equip us with a certain level of security, which is not all-around, a foolproof mechanism. In this specific circumstance, a research to support the certainty and validity of patients is essential for the wide-scale use and accomplishment of the computerized medical services. This survey features a comprehensive study of existing e-health cloud protecting cryptographic and non-cryptographic systems to verify security and privacy in the cloud and their vulnerabilities in the quick changing era. Besides, our work likewise furnishes and recognizes key research areas vise models, encryption techniques, access control systems and has additionally distinguished some wonderful research issues and future research directions to bring upon a forceful action for ensuring secure data privacy in shrewd health arrangements.

REFERENCES

[1] N. Dong, H. Jonker, and J. Pang, ‘‘Challenges in ehealth: From enabling to enforcing privacy,’’ in Proc. Int. Symp. Found. Health Inform. Eng. Syst. Berlin, Germany: Springer, 2011, pp. 195–206.

[2] X. Yi, Y. Miao, E. Bertino, and J. Willemson, ‘‘Multiparty privacy protection for electronic health records,’’ in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2013, pp. 2730–2735.

[3] C. S. Kruse, M. Mileski, A. G. Vijaykumar, S. V. Viswanathan, U. Suskandla, and Y. Chidambaram, ‘‘Impact of electronic health records onlong-termcarefacilities:Systematicreview,’’JMIRMed.Inform.,vol.5, no. 3, p. e35, 2017.

[4] L. Griebel, H.-U. Prokosch, and F. Köpcke, D. Toddenroth, J. Christoph, I. Leb, I. Engel, and M. Sedlmayr, ‘‘A scoping review of cloud computing in healthcare,’’ BMC Med. Inform. Decis. Making, vol. 15, no. 1, p. 17, Mar. 2015.

[5] P. Li, S. Guo, T. Miyazaki, M. Xie, J. Hu, and W. Zhuang, ‘‘Privacypreserving access to big data in the cloud,’’ IEEE Cloud Comput., vol. 3, no. 5, pp. 34–42, Sep./Oct. 2016.

[6] A. Abbas and S. U. Khan, ‘‘A review on the state-of-the-art privacypreserving approaches in the e-health clouds,’’ IEEE J. Biomed. Health Informat., vol. 18, no. 4, pp. 1431–1441, Apr. 2014. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6714376/

[7] M. Ahmed and A. S. S. B. Ullah, ‘‘False data injection attacks in healthcare,’’ in Proc. Australas. Conf. Data Mining, 2017, pp. 192–202.

[8] D. McGraw, ‘‘Building public trust in uses of health insurance portability and accountability act de-identified data,’’ J. Amer. Med. Inform. Assoc., vol. 20, no. 1, pp. 29–34, Jan. 2013.

[9] B. Edwards, S. Hofmeyr, and S. Forrest, ‘‘Hype and heavy tails: A closer look at data breaches,’’ J. Cybersecur., vol. 2, no. 1, pp. 3–14, Dec. 2016.

[10] N. Asokan, V. Niemi, and K. Nyberg, ‘‘Man-in-the-middle in tunnelled authentication protocols,’’ in Proc. Int. Workshop Secur. Protocols. New York, NY, USA: Springer, 2003, pp. 28–41.

[11] Y. Chen, W. Trappe, and R. P. Martin, ‘‘Detecting and localizing wireless spoofing attacks,’’ in Proc. 4th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Netw., Jun. 2007, pp. 193–202.

[12] C. Meadows, R. Poovendran, D. Pavlovic, L. Chang, and P. Syverson, ‘‘Distance bounding protocols: Authentication logic analysis and collusion attacks,’’ in Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks, New York, NY, USA: Springer, 2007, pp. 279–298.

[13] S. Narayan, M. Gagné, and R. Safavi-Naini, ‘‘Privacy preserving EHR system using attribute-based infrastructur,’’ in Proc. ACM Workshop Cloud Comput. Secur. Workshop, Oct. 2010, pp. 47–52.

[14] S. Yu, C. Wang, K. Ren, and W. Lou, ‘‘Achieving secure, scalable, and fine-grained data access control in cloud computing,’’ in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.

[15] D. Mashima and M. Ahamad, ‘‘Enhancing accountability of electronic health record usage via patient-centric monitoring,’’ in Proc. 2nd ACM SIGHIT Int. Health Inform. Symp., Jan. 2012, pp. 409–418.

[16] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," Computer, vol. 29, no. 2, pp. 38–47, 1996.

[17] E. Yuan and J. Tong, "Attributed based access control (ABAC) for Web services," in Proc. IEEE Int. Conf. Web Services, Jul. 2005, p. 569.

[18] R. Charanya and M. Aramudhan, "Survey on access control issues in cloud computing," in Proc. Int. Conf. Emerg. Trends Eng., Technol. Sci. (ICETETS), pp. 1–4, Feb. 2016.

[19] L. Zhu, C. Zhang, C. Xu, X. Liu, and C. Huang, "An efficient and privacypreserving biometric identification scheme in cloud computing," IEEE Access, vol. 6, pp. 19025–19033, Mar. 2018.

[20] W. Li, K. Xu, Y. Xu, and J. Hong, "TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 5, pp. 1484–1496, May 2016.

[21] K. Xu, Y. Xu, J. Hong, W. Li, H. Yue, D. S. Wei, and P. Hong, "RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage," IEEE Trans. Inf. Forensics Security, vol. 12, no. 4, pp. 953–967, Apr. 2017.

[22] P.-W. Chi and C.-L. Lei, "Audit-free cloud storage via deniable attributebased encryption," IEEE Trans. Cloud Comput., vol. 6, no. 2, pp. 414–427, Apr./Jun. 2018.

[23] W. Li, B. M. Liu, D. Liu, R. P. Liu, P. Wang, S. Luo, and W. Ni, "Unified fine-grained access control for personal health records in cloud computing," IEEE J. Biomed. Health Informat., vol. 23, no. 3, pp. 1278–1289, May 2018.

[24] C. Zhang, L. Zhu, C. Xu, and R. Lu, "PPDP: An efficient and privacypreserving disease prediction scheme in cloud-based e-healthcare system," Future Gener. Comput. Syst., vol. 79, pp. 16–25, Feb. 2018.

[25] C. Huang, K. Yan, S. Wei, G. Zhang, and D. H. Lee, "Efficient anonymous attribute-based encryption with access policy hidden for cloud computing," in Proc. Int. Conf. Progr. Informat. Comput. (PIC), Dec. 2017, pp. 266–270.

[26] J. Wei, W. Liu, and X. Hu, "Secure data sharing in cloud computing using revocable-storage identity-based encryption," IEEE Trans. Cloud Comput., vol. 6, no. 4, pp. 1136–1148, Oct./Dec. 2016.

[27] H. Cui, R. H. Deng, and Y. Li, "Attribute-based cloud storage with secure provenance over encrypted data," Future Gener. Comput. Syst., vol. 79, no. 2, pp. 461–472, Feb. 2018.

[28] N. S. Safa, M. Sookhak, R. von Solms, S. Furnell, N. A. Ghani, and T. Herawan, "Information security conscious care behaviour formation in organizations," Comput. Secur., vol. 53, pp. 65–78, Sep. 2015.

[29] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, "Security techniques for the electronic health records," J. Med. Syst., vol. 41, no. 8, p. 127, Aug. 2017.

[30] Z.-R. Li, E.-C. Chang, K.-H. Huang, and F. Lai, "A secure electronic medical record sharing mechanism in the cloud computing platform," in Proc. IEEE 15th Int. Symp. Consum. Electron. (ISCE), Jun. 2011, pp. 98–103.

[31] Y. Y. Chen, J. C. Lu, and J. K. Jan, "A secure EHR system based on hybrid clouds," J. Med. Syst., vol. 36, no. 5, pp. 3375–3384, 2012. [Online]. Available: https://link.springer.com/article/10.1007/s10916-012-9830-6

[32] H. Li, Y. Yang, Y. Dai, J. Bai, S. Yu, and Y. Xiang, "Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data," IEEE Trans. Cloud Comput., to be published.

[33] A. Ibrahim, B. Mahmood, and M. Singhal, "A secure framework for sharing electronic health records over clouds," in Proc. IEEE Int. Conf. Serious Games Appl. Health (SeGAH), May 2016, pp. 1–8.

[34] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn., New York, NY, USA: Springer, pp. 457–473, 2005.

[35] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attributebased encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[36] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attributebased encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.

[37] T. Hupperich, H. Löhr, A.-R. Sadeghi, and M. Winandy, "Flexible patientcontrolled security for electronic health records," in Proc. 2nd ACM SIGHIT Int. Health Informat. Symp. Jan. 2012, pp. 727–732.

[38] R. Zhang, R. Xu, and L. Liu, "Searchable encryption for healthcare clouds: A survey," IEEE Trans. Services Comput., vol. 11, no. 6, pp. 978–996, Nov. /Dec. 2017.

[39] Y. Yang and M. Ma, "Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds," IEEE Trans. Inf. Forensics Security, vol. 11, no. 4, pp. 746–759, Apr. 2017.

[40] P. van Liesdonk, S. Sedghi, J. Doumen, P. Hartel, and W. Jonker, ''computationally efficient searchable symmetric encryption,'' in Proc. Workshop Secure Data Manage. New York, NY, USA: Springer, 2010, pp. 87–100.

[41] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith, ''Public key encryption that allows PIR queries,'' in Proc. Annu. Int. Cryptol. Conf., 2007, pp. 50–67.

[42] A. Arriaga, Q. Tang, and P. Ryan, ''Trapdoor privacy in asymmetric searchable encryption schemes,'' in Proc. Int. Conf. Cryptol. Afr. New York, NY, USA: Springer, 2014, pp. 31–50.

[43 J. Baek, R. Safavi-Naini, and W. Susilo, ''Public key encryption with keyword search revisited,'' in Proc. Int. Conf. Comput. Sci. It is Appl., 2008, pp. 1249–1259.

[44] Q. Tang and L. Chen, ''Public-key encryption with registered keyword search,'' in Proc. Eur. Public Key Infrastruct. Workshop. New York, NY, USA: Springer, 2009, pp. 163–178.

[45] Y. Yang, ''Attribute-based data retrieval with semantic keyword search for e-health cloud,'' J. Cloud Comput., vol. 4, no. 1, p. 10, Dec. 2015.

[46] J. Li, X. Lin, Y. Zhang, and J. Han, ''KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage,'' IEEE Trans. Services Comput., vol. 10, no. 5, pp. 715–725, Sep./Oct. 2017.

[47] Q. Zheng, S. Xu, and G. Ateniese, ''VABKS: Verifiable attribute-based keyword search over outsourced encrypted data,'' in Proc. IEEE Conf. Comput. Commun. Apr. 2014, pp. 522–530.

[48] P. Liu, J. Wang, H. Ma, and H. Nie, ''Efficient verifiable public key encryption with keyword search based on KP-ABE,'' in Proc. 9th Int. Conf. Broadband Wireless Comput., Commun. Appl., Nov. 2014, pp. 584–589.

[49] J. Shao, Z. Cao, X. Liang, and H. Lin, ''Proxy re-encryption with keyword search,'' Inf. Sci., vol. 180, no. 13, pp. 2576–2587, 2010.

[50] M. Blaze, G. Bleumer, and M. Strauss, ''Divertible protocols and atomic proxy cryptography,'' in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. New York, NY, USA: Springer, 1998, pp. 127–144.

[51] K. Rabieh, K. Akkaya, U. Karabiyik, and J. Qamruddin, ''A secure and cloud-based medical records access scheme for on-road emergencies,'' in Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC), Jan. 2018, pp. 1–8.

[52] R. Bhateja, D. P. Acharjya, and N. Saxena, ''Enhanced timing enabled proxy re-encryption model for E-health data in the public cloud,'' in Proc. Int. Conf. Adv. Comput., Commun. Inform. (ICACCI), Sep. 2017, pp. 2040–2044.

[53] V. C. Hu, D. Ferraiolo, and D. R. Kuhn, Assessment of Access Control Systems. Gaithersburg, MD, USA: Nat. Inst. Standards Technol., 2006.

[54] M. F. F. Khan and K. Sakamura, ''Fine-grained access control to medical records in digital healthcare enterprises,'' in Proc. Int. Symp. Netw. Comput. Commun. (ISNCC), May 2015, pp. 1–6.

[55] H. S. G. Pussewalage and V. Oleshchuk, ''A patient-centric attribute based access control scheme for secure sharing of personal health records using cloud computing,'' in Proc. 2nd Int. Conf. Collaboration Internet Comput. (CIC), Nov. 2016, pp. 46–53.

[56] R. Sandhu, D. Ferraiolo, and R. Kuhn, ''model for role-based access control: Towards a unified standard,'' in Proc. ACM Workshop Role-Based Access Control, Jul. 2000, pp. 1–11.

[57] D. R. Kuhn, E. J. Coyne, and T. R. Weil, ''Adding attributes to role-based access control,'' IEEE Comput., vol. 43, no. 6, pp. 79–81, Jun. 2010.

[58] E. Chickowski. (May 2012). ''Healthcare unable to keep up with insider threats,'' Dark Reading, 2012. Accessed: May 12, 2018. [Online]. Available: https://www.darkreading.com/vulnerabilities—threats/ healthcare-unable-to-keep-up-with-insider-threats/d/d-id/1137610?

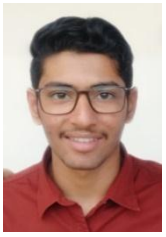
[59] Aderonke Justina. Ikuomola1,Oluremi O. Arowolo, "Securing Patient Privacy in E-Health Cloud Using Homomorphic Encryption and Access Control" International Journal of Computer Networks and Communications Security VOL.2, NO.1, JANUARY 2014, 15–21. Available online at: www.ijcncs.org ISSN 2308-9830

[60] https://slideplayer.com/slide/10511425/

BIOGRAPHIES

Ravi Bhagyoday is pursuing his B.Tech in Cloud technologies and Information security at ADYPU, Pune India. He is also researching new technologies in Cloud technology and working on different cloud platforms like AWS, Google Cloud, Azure, etc.

Chintan Kamani is currently pursuing his B.Tech degree in Cloud Computing and Information Security at Ajeenkya DY Patil University, Pune India and pass out in the year 2021.Currently following his passion about the world.



Dhrumil Bhojani is a cyber-security enthusiastic currently pursuing his B.Tech in Cloud technologies and Information security at ADYPU, Pune India. Currently researching on new technologies in cyber security field and Penetration testing.

Vivek Parmar is currently pursuing his B.Tech degree in Cloud Computing and Information Security at Ajeenkya DY Patil University Pune. Currently interested in machine learning and Artificial Intelligence.