This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access

Security and Privacy-preserving Challenges of e-Health Solutions in Cloud Computing

Shekha Chenthara
School of Engineering and Science
Victoria University, Melbourne, Australia
Email: shekha.chenthara@live.vu.edu.au

Khandakar Ahmed
School of Engineering and Science
Victoria University, Melbourne, Australia
Email: khandakar.ahmed@vu.edu.au

Hua Wang
School of Engineering and Science
Victoria University, Melbourne, Australia
Email: hua.wang@vu.edu.au

Frank Whittaker
School of Engineering and Science
Victoria University, Melbourne, Australia
Email:frank.whittaker@vu.edu.au

***Abstract*—Objective: A systematic and comprehensive review of security and privacy-preserving challenges in e-health solutions which indicate various privacy preserving approaches to ensure privacy and security of Electronic Health Records (EHRs) in the cloud. This study highlights the research challenges and directions concerning cyber security to build a comprehensive security model for EHR.**

Method: We carry an intensive study in IEEE, Science Direct, Google Scholar, PubMed and ACM for papers on EHR approaches published between 2000 and 2018 and summarized them in terms of the architecture types as well as evaluation strategies.

Results: we surveyed, investigated and reviewed various aspects of several articles and identified the following tasks:1) EHR security and privacy (2) Security and privacy requirements of e-health data in cloud (3) EHR Cloud Architecture, (4) Diverse EHR cryptographic and non-cryptographic approaches. We also discuss some crucial issues and the ample opportunities for advanced research related to security and privacy of EHRs.

Discussion: Since big data provides a great mine of information and knowledge in e-Health applications, exist serious privacy and security challenges that require immediate attention. Studies must focus on efficient comprehensive security mechanisms for EHR and also explore techniques to maintain the integrity and confidentiality of patients' information.

***Index Terms*—e-health, Electronic Health Record, EHR cryptographic and non-cryptographic, security and privacy, systematic review.**

I. Introduction

The beginning of the 21^{st}century has witnessed great leaps in digital technology that are changing the landscape of healthcare system across the world. There is a gradual and systematic transformation in healthcare systems from paper based records to electronic records ushering in a revolution in the healthcare industry [1]. Such developments provide high efficiency and flexibility to healthcare services by providing a platform that efficaciously shares healthcare data among different stakeholders. This evolution converts paper based records into digitalized electronic records 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 either by patient or their relatives on a regular basis. EHD as electronic health records or computerised 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, immunisation 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]. The advantages of EHRs include easier and swift clinical data access, ability to maintain effective clinical workflows, mitigation of medical errors, enhanced patient safety, reduced medical costs and better and stronger support for clinical decision-making. Realising the benefits offered by EHD systems more than 90% of healthcare institutions in Australia have adopted this system to facilitate effective medical resource allocation and efficient healthcare [3]. The ability of EHDs to provide better management of healthcare has been ascertained and testified by various users. However the transition from conventional healthcare systems to e-health care throws unique challenges with respect to privacy, confidentiality, and security of medical information.

Cloud computing is a recent paradigm in digital technology and is being extensively used in the healthcare industry [4]. It not only provides convenient storage of medical information but also facilitates the easy exchange or transmission of medical data among various stakeholders. The large scale proliferation of health information in the age of big data necessitates the burgeoning role of cloud networks not only for hosting unlimited amounts of data but also for its easy access across the Internet [5]. It facilitates the creation, storage and retrieval of healthcare information by all stakeholders viz healthcare providers, doctors and patients with ease irrespective of the barriers posed by time and space. Cloud services provide immense benefits in terms of cost effective

storage, access, processing and updating of information with improved efficiency and effectiveness. Since the data is running on a wide network of remote servers, which are integrated and operated as a single ecosystem accessed from different locations by multiple users, it is susceptible to intrusion or compromise, thereby posing a threat to privacy and security. Moreover the majority of medical data is highly sensitive and strictly confidential, its storage on third party servers naturally increases these vulnerabilities [6]. Generally, a patient may have several healthcare providers viz primary care physicians, therapists, specialists and several insurer providers for medical, dental, vision etc [7]. Considering the susceptible nature of health information in the public domain there is an imminent need to devise a more secure, efficient and effective mechanism for sharing and accessing data among stakeholders.

In the healthcare sector, although the EHRs are subjected to various challenges with respect to privacy and unauthorised access, the most prominent one is pertaining to data privacy and security [6]. Risks vary from the malware attack, that compromises the integrity and confidentiality of medical data, to the Distributed Denial-of-Service (DDoS) attacks, which are capable of depriving the systems ability to provide efficient patient care. Cyber-attacks, such as those caused by Ransomware, have greater ramifications that go beyond financial loss or privacy breach [8]. In the USA, hackers broke [9] into the database of Community Health Systems (CHS) of a prominent hospital group and accessed a great deal of personal health information, including the social security numbers of more than a million patients. In a similar incident, Anonymous, an internet vigilante group, targeted several hospitals and launched a DDoS attack on their websites crippling medical services [10]. These incidents highlighted an imminent need to protect and secure the confidentiality, integrity, availability, security and privacy of Protected Health Information (PHI) as a primary priority in EHR. In this context, the role of cyber security is paramount in preventing, detecting, and acting on unauthenticated access to health data, and its impact towards social, economic, political and cultural conflicts. According to the Health Insurance Portability and Accountability Act (HIPAA), it is the responsibility of healthcare providers to maintain the confidentiality of the health data [11]. Several techniques are already being in use to secure the security and privacy of smart health systems in the cloud environment.

A. Motivation

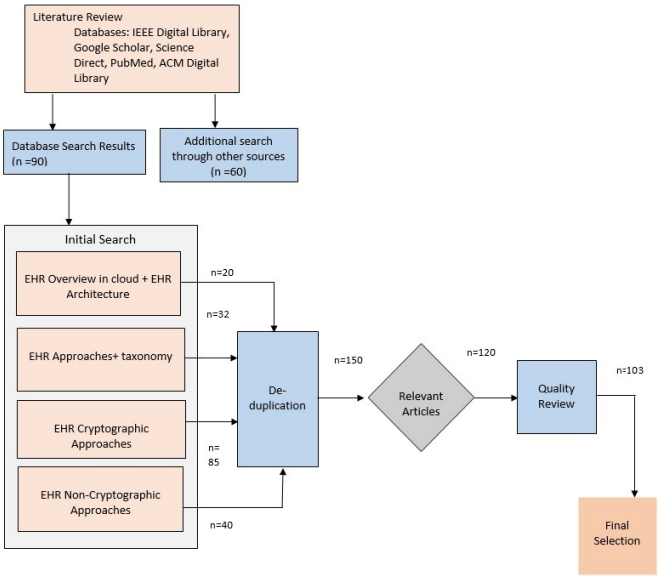
The existing privacy-preserving mechanisms are not adequate to ensure foolproof security in the e-health cloud. Contrary to most beliefs, the main risk faced by health records hosted in cloud servers is internal attacks from people who have authorized credentials to access data within organizations, where database administrators or key managers are attackers, which is significantly worse than the external attacks. This paper aims to provide a wide review of the strengths and drawbacks of existing security and privacy preserving mechanisms in e-healthcare environments that make electronic health records vulnerable to threats in the cloud arena. E-health data contains various sensitive and confidential information ranging from patient data to financial information including social security number, credit card details, whose leakage not only throws open sensitive patients information and cause financial losses but also infringes the most fundamental right of a citizen in any country i.e. right to privacy.

The existing advanced encryption techniques such as Attribute Based Encryption (ABE) is inefficient to resolve this issue due to its expensive computation [2]. Most of the existing solutions for Key Policy Attribute Based Encryption (KP-ABE) and Cipher text policy Attribute Based Encryption (CP-ABE) assumes that a single key management centre chooses a master key randomly and generates decryption keys for users on the basis of master key. In this case where the key manager is an attacker, these solutions cannot prevent from the inside attacks. The insider threats in healthcare include the theft of PHI such as Social Security Numbers or personal information for identity theft and fraud, theft of Intellectual Property and sabotage. Other non-malicious threats include the accidental loss/disclosure of sensitive information, such as disclosing sensitive patient information to others, sharing login credentials, writing down login credentials, or responding to phishing messages. For example, the largest healthcare data breach in history is the theft of 80 million healthcare records from Anthem Inc [12], American Health Insurance Company is believed to have been made possible because of stolen credentials. Data encryption, secure storage, authentication, access control, key management, efficient user revocation etc. are yet to be addressed and resolved. This paper analyses existing privacy-preserving approaches, their strengths, drawbacks, research issues and comes up with a new paradigm supported by blockchain technology that can offset certain shortcomings but also ensure a framework for providing efficient privacy preserving and security in e-health data.

B. Methods

This section begins with study selection to ensures the accuracy of search and retrieval process. The study selection narrows down to search for publications from different electronic databases related to computer science and healthcare that attempts to collect relevant empirical evidences in a particular field to assess the techniques critically and to obtain conclusions to summarise the research study. This section also performs a categorical study related to security and privacy preserving studies of EHR as a part of qualitative data analysis that makes it easy to compare and analyse the crux of the work.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access



*n= number of articles

Figure 1: Literature search study selection

1) Literature Review- Study Selection: This study performs a systematized review of security and privacy preserving approaches of EHRs in the cloud environment from different databases, including IEEE, Google scholar, PubMed, ACM, Springer, Elsevier, Scopus and Science Direct. The detailed summary of the slected studies and the keywords used for searching is shown in Table 1. This work also involves an extensive review of significant review papers published between 2000 and 2018.

This review limited its search to relevant papers published between 2000 and 2018 and found more than 200 articles. We filtered those by de-duplication based on titles and authors, then conducted a topic relevant article study based on abstract and keyword significance. 150 articles remained after de-duplication, 120 after relevant article study and 103 after quality review. The literature search study selection is showed on Fig. 1

2) Categorizing Security and Privacy Preserving Studies: The Objective of this review is three fold. Initially, this study investigates the security and privacy requirements of smart health data in cloud arena. Secondly, after summarising a brief architecture of e-Health system, a prevailing and up-to-date review of the e-Health clouds is presented using a taxonomy over privacy preserving approaches. The survey then discusses the merits and drawbacks of the furnished mechanisms and finally highlights some future research directions and open research issues. The rest of this study is categorized as follows. In section II, we discuss the security and privacy requirements of e-health data in the cloud. Section III summarizes E-health Overview and Section IV reviews an intensive analysis of security and privacy preserving mechanisms employed in

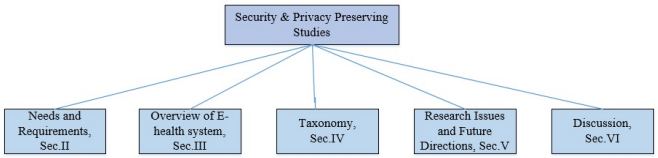


Figure 2: Categorizing studies to sections

the e-health cloud environment. Section V describes research issues and future directions and Section VI is a discussion of the research gaps in the existing literature and Section VII as conclusion. A sketch of categorizing studies is portrayed in Fig. 2

II. Security and Privacy Requirements of e-health data in Cloud

In the current Big data epoch, data proliferation demands outsourcing of healthcare information to the cloud servers. Regardless of the tremendous boons provided by the cloud, it also entails perilous threats to security and privacy of the healthcare data [1]. Some of the potential attacks include information disclosure, Denial of Service attacks (DoS), cloud malware injection attack, man-in-the middle cryptographic attack [13], spoofing [14], collusion attacks [15].The cloud service providers and many government organizations have suggested a variety of security measures and guidelines to ensure and enhance the confidence of patients and organizations. The first such legislative measure put forward by the US Congress in 1996 for the US healthcare industry was the (HIPAA) [11]. There are mainly three categories of cloud servers: trusted servers, semi-trusted, and untrusted servers. A trusted server is one that can be entirely trusted without any information disclosure and threats to the health data stored can be due to internal adversaries [16]. Semi trusted servers are honest but curious servers that acquire health data by colluding with malicious users [17] whereas untrusted servers are not trustable without any privacy preservation mechanisms and are vulnerable to attacks from both internal and external adversaries [18] as shown in Fig 3.

The vital security and privacy requirements in e-health systems are 1) Data integrity-ensures that the health information has not been altered by any unauthorised entity. 2) Data confidentiality-ensures that the sensitive health data is prevented from reaching unauthorised users. Data encryption is the most substantial approach to ensure data confidentiality. 3) Authenticity- ensures that only the authorised 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 requirement which ensures that the health data is monitored and protected by keeping track of the activity log and ensures assurance to the users associated of data privacy and security. 6) Non-repudiation- refers to the non-denial of authenticity of sender and receiver. For instance, the patients

Table 1: Literature review - Study selection

Publisher	Source	Keywords
IEEE	IEEE Journal of Biomedical and Health Informatics	e-Health
	High Performance Computing and Communications	EHR
	IEEE open and big data conference	Security and Privacy of EHR in cloud
	IEEE Access	Privacy-preserving techniques in EHR
	IEEE International Cloud Computing Conference	e-health privacy and security
	IEEE Transactions on Information Forensics and Security	EHR Cryptographic Approaches
	IEEE Consumer Communications and Networking Conference	EHR Non-Cryptographic Approaches
	IEEE Transactions on Information Technology in Biomedicine	Cyber-security attacks
	IEEE International Conference in Web Services	
	IEEE Transactions on Cloud Computing	
	IEEE Transactions on Parallel and Distributed Systems	
	IEEE Access	
ACM	ACM International Health Informatics Symposium	
	ACM workshop on Role-based access control	
	ACM workshop on Cloud computing security	
	ACM International Symposium in Cluster, Cloud and Grid Computing	
PubMed	BMC Medical informatics and decision making	
Google Scholar	Journal of Cyber Security	
	Security and Communication Networks	
	International Journal of Security and Networks	
Scopus	International Journal of Medical Informatics	
	Journal of Medical systems	
	Journal of Information Security and Applications	
	International Journal of Information Management	
	Journal of Cloud Computing	
	Journal of Biomedical Informatics	
	Future Generation Computer Systems	

or the doctors can't repudiate after embezzlement of the health data 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.

III. Overview of E-health system in the cloud

E-health system is a recent healthcare innovation utilising electronic processes and communication. In an e-health system, EHR or EMR is a systematized aggregation of electronic health information of patients [2]. These records involve all the health data information including demographics, medical histories, medications, laboratory reports, radiology images, billing information and any additional sensitive patient information. The cloud offers great service to both healthcare providers and patients alike in terms of cost effective storage, processing and updating of information with enhanced efficiency and quality. Since all this data is stored in multiple servers, it can be easily accessible by users from various locations on demand. E-health systems promise rapid, steadfast and on-demand access to medical records, fewer medical flaws, enhanced healthcare quality, however they equally expose patient privacy, via improper authorization and misuse of EHR data. Therefore security and privacy are considered to be critical requirements when sharing or accessing patient data between several stakeholders. An overview of e-health architecture is depicted in Fig 3.

E-health cloud architecture types can be public, private, hybrid and community according to the data stored. Since EHR data is strictly confidential, carries sensitive patient information and housed in third party servers, access control mechanisms are required. Access control is a security barrier which preserves data privacy by restricting the operation and access of healthcare documents in the healthcare system. The predominant access control techniques in the healthcare systems are Role-Based Access Control (RBAC), Attribute-Based Access Control(ABAC) and Identity-Based Access Control (IBAC) techniques. Role based systems [19] provide for the assignment of certain roles to the users for data access. ABAC [20], which employs cryptographic and non-cryptographic techniques, whereas IBAC uses identity-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access

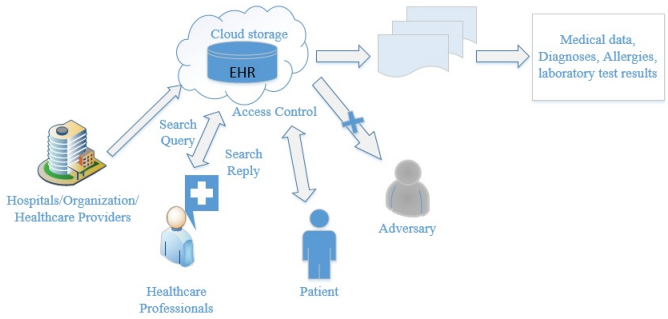


Figure 3: Architecture of Electronic health data in cloud

based encryption mechanisms that utilizes user identity for data encryption. Data sharing is a distinctive feature of e-health systems. It can be shared among various stakeholders such as healthcare providers, hospitals, healthcare organizations etc. Search is an alternate substantial function of an e-Health system. Proxy encryption and public-key encryption are widely used encryption techniques for data search.

A. Cloud computing security: State of the art and research challenges in e-health

Cloud computing has seen a tremendous growth that has reformed the landscape of computing with its storage, elastic resources, easy and fast deployment and reduced costs such that, it instigated many organizations to move their data in the cloud. Even though cloud services provide massive benefits, it still suffers from several security threats. For instance, users are not aware of the massive amount of data stored with the cloud service provider [21]. Due to lack of transparency, it is difficult to be aware of where, how and when the data is processed and therefore makes it difficult to trust the service provider, who in turn can also be a reason for huge data loss. There has been several schemes and developments in the area of cloud security. Some of the advanced cloud security techniques are discussed and the pros and cons are outlined in Table 2.

Some of the advanced privacy-preserving mechanisms that preserves cloud security can be adopted to e-health, while some are not due to security concerns. Cloud computing is a centralized mainframe computing paradigm owned by cloud provider which is less patient-centric and is prone to insider attacks that makes the health records more vulnerable. This is one of the major downsides of cloud computing. Even though cloud techniques adhere strict security measures, it does not offer a fool proof solution to be adopted into e-health, taken into account of its security issues. Zhu et al [22] proposes an efficient privacy preserving biometric identification scheme in which a huge volume of biometric data such as fingerprints, irises, voice patterns, facial patterns are encrypted and outsourced to the cloud to avoid expensive storage and computation costs. The scheme is resistant against collusion attacks and provides a maximum level of data privacy.This approach can be applicable to e-health cloud for efficient data storage in which the health records can be encrypted and stored in the cloud that achieves a certain level of data protection. However, as the health records are extremely sensitive and the data is exposed to the database owner, this scheme is less acceptable in terms of security. Also, this scheme cannot be considered for EHRs as it is not patient-centric and computationally infeasible for real scale problems. This work [23] proposes a robust and verifiable hybrid multiauthority CP-ABE access control scheme by combining (t, n) threshold secret sharing and multi-authority CP-ABE scheme for public cloud storage with which both security and performance are improved by overcoming the single point bottleneck problem. Xue et al [24] proposes a robust and efficient access control scheme that resolves the single-point performance bottleneck in most of the existing CP-ABE using an auditing mechanism. Eventhough these schemes [23] [24] are advanced access control schemes that has high security measures, they cannot be adopted directly to e-health as these schemes cannot guarantee protection from insider attacks since it is controlled by Central Authority and multiple Attribute Authorities. A special encryption technique named Deniable ABE scheme based on Waters cipher text policy-attribute based encryption (CP-ABE) scheme was proposed that allows cloud storage providers to create forged user secrets from stored cipher text to prevent the data from outside coercers [25]. This scheme combines the advantage of both ABE and symmetric key encryption as it supports a multi-privileged access control for PHRs by combining the encryption of data from multi-patients that falls under the similar access policy [26]. Zhang et al [27] proposes an efficient privacy preserving disease prediction scheme by using Single layer Perceptron learning algorithm. This model encrypts the symptom information submitted by the patient and the cloud uses the encrypted prediction models trained by it to diagnose the patient disease without revealing the patient privacy. These mechanisms [26] [27] imparts high level of data privacy, but still impractical for health records due to its computational complexity and scalability issues. Another work presented an anonymous CP-ABE with hidden access policy and provides authorized access control with constant key length [28]. Wei et al [29] proposed a revocable storage Identity Based Encryption (IBE) that provides forward and backward security of ciphertext. Most of the existing cloud storage systems with secure provenance lacks poor access control, incur excessive performance overhead and do not support dynamic user management. This work solves the problem by presenting an attribute-based cloud storage system with secure provenance [30]. Eventhough ABE schemes are most efficient among encryption techniques and provide fine-grained, well-formed access to health records, it is still impractical for proper execution on EHRs due to its expensive computation [28] [30], key management complexity and challenge in managing access control policies [25] when

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access

Table 2: Cloud computing security techniques

Scheme	Advantage	Disadvantage	Reference
Privacy-preserving Biometric Identification Scheme	Maximum data privacy Resistant to collusion attacks	Need to trust the cloud service provider, Centralised data Storage, Computationally expensive for real scale problems	[22]
TMACS	Security and System level robustness,Ensures security and efficient performance	No attribute revocation function, re-using master key shared among multiple attribute authorities (AA), Computational and Communication overhead	[23]
RAAC	Robust and secure access control, Resolves single-point performance bottleneck-problem	Need to trust Central Authority (CA) for key generation and distribution, Honest-but-curious cloud servers, AA can be compromised, Storage overhead for key generation and auditing, Communication overhead on CA and AA	[24]
Identity based encryption	Reduces encryption complexity	Secure channel required between user and key generator	[21]
Attribute based encryption	Fine-grained access control, Collusion-resistant and minimal communication overhead	Data owner requires each authenticated users' public key to encrypt data	[21]
Attribute based cloud storage with secure Provenance	Protects data privacy, fine-grained access control, efficient user revocation, scalability, dynamic user management, data provider anonymity and traceability	Data decryption is expensive due to the complexity in bilinear pairing computations and high data latency	[30]
Audit-free cloud storage via Deniable ABE	fine-grained access control mechanism, ensures data privacy	chances of decryption errors, extra overhead of generating deniable keys	[25]
Unified fine-grained access control for PHR in cloud computing	Flexible and fine-grained access control to PHR, reduced encryption decryption costs	Complex key generation, Required to trust AA and policy manager, No User revocation, Limited to a few users	[26]
PPDP	High level of privacy, Highly efficient technique for disease prediction	Computation complexity, communication cost increases with increase in EHRs, verification mechanism is not specified	[27]
Efficient anonymous ABE with access policy hidden for cloud computing	Anonymity, Data security, fine-grained access control	Requires a trusted AA, Computational complexity and storage overhead due to the addition of fake attributes to the access structure	[28]
Secure data sharing in cloud computing using revocable storage IBE	confidentiality, forward/backward secrecy	system is not scalable, key authority can be compromised	[29]

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access

attributes in the access structure grows.

Despite the attractive features that cloud offers, the transition of healthcare field towards cloud environment increase the concerns about privacy, security, access control and compliance due to the inherent security challenges related to the cloud technology. Patients lose their physical control by storing health information in the cloud servers which can be seen as a threat to patient privacy. Data security and data integrity has also been a challenging issue while storing and accessing data in the cloud arena [31]. Another downside is that cloud service providers have a vital role in transaction analysis, access control, data protection and services integration. With advancement of technology, the emergence of advanced cyber threats has escalated, which hinders the privacy and security of EHRs [32]. Therefore, it is very important to guarantee integrity, confidentiality, reliability as well as authenticity of the e-health data in either a private, public or hybrid cloud environment. Consequently, this research introduces the concept of a permissioned patient-centric Block chain for EHRs that eliminates most of the existing bottlenecks in the cloud.

IV. Classification of Privacy preserving mechanisms in Electronic health records

In this work, different techniques based on cryptographic and non-cryptographic approaches are considered based on their application of healthcare systems in the cloud arena. Furthermore, some techniques are analysed that preserves data security, data privacy and data anonymity in the cloud. In addition to this, some Searchable Encryption(SE) techniques are presented to query the encrypted data in the cloud. Since the data is encrypted and stored in third-party cloud servers, normal searching schemes cannot be applied. Searching encrypted data is arduous, Searchable Symmetric Encryption (SSE) has been proposed that enable keyword searches across encrypted cloud data. Different from the recent surveys, our research study has systematically covers all aspects and methods of privacy and security of EHR in cloud. Moreover, the survey also reveals the advanced cloud computing security techniques and their research challenges and at the same time incorporating the potential benefits of Block chain technique to offset those shortcomings. Apart from that we also conclude the discussion with open research problems and future directions that expands the scope of further research in data security and privacy.

There are several research investigations conducted for preserving e-health data privacy in the cloud. The two main types are Cryptographic and Non-Cryptographic. The cryptographic schemes employ encryption techniques, namely: symmetric key encryption, public key encryption and several cryptographic primitives, whereas non-cryptographic approaches include access control mechanisms such as RBAC, ABAC, IBAC etc. Classification of the privacy preserving mechanisms is portrayed in Fig. 4

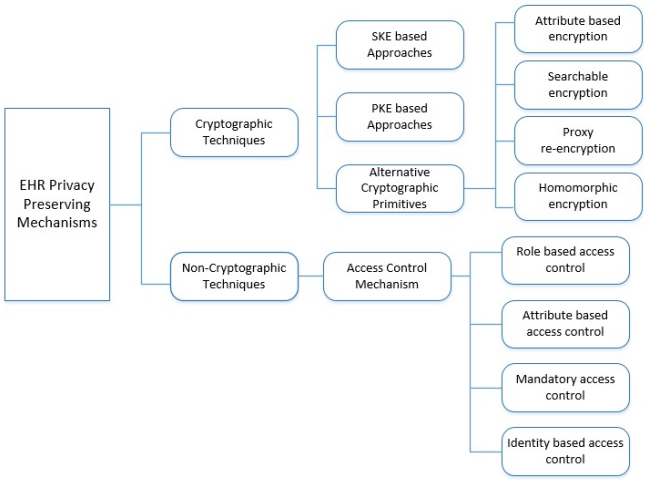


Figure 4: Classification of privacy preserving mechanisms in electronic health records

A. Cryptographic Approaches

Cryptography means hidden writing that analyses and constructs protocols to prevent third parties from reading secret messages. Cryptographic approaches can be symmetric key cryptography as well as asymmetric key cryptography (see Fig. 5) in which the prior uses the same key for the encryption and decryption whilst the latter uses different keys. This study includes encryption schemes such as Symmetric Key Encryption (SKE), Public Key Encryption (PKE) and a few alternative cryptographic primitives.In PKE schemes, two different set of keys are employed ie public key and a private key pair for data encryption and decryption whereas SKE based approaches utilizes a single shared secret key for the same. Alternative cryptographic primitives include several encryption schemes viz Attribute Based Encryption(ABE), Searchable Encryption (SE), proxy re-encryption, homomorphic encryption, Identity Based Encryption (IBE) etc.

Non-cryptographic approaches mainly associates with policy based authorization infrastructure labelled as access control mechanisms viz RBAC, ABAC, Mandatory Access Control (MAC), IBAC etc. This section gives a detailed survey of significant research works based on SKE, PKE and alternative cryptographic primitives that enforce the security and privacy of electronic health solutions.

1) SKE based Approaches: The SKE employs the same shared secret key for encryption and decryption and it is highly effective in EHR systems. But it introduces inevitable additional complexity since it requires additional access control mechanisms for the effective sharing of EHR. The commonly used SKE based algorithms are Advanced Encryption Standard (AES), Data Encryption Standard (DES), stream ciphers such as RC4, A5/1, and Blow Fish etc. Some

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access

of the SKE based approaches are described below and the comparison is shown in Table 3.

Lee [33] proposed a cryptographic key management protocol based on symmetric cryptosystems to meet HIPAA regulations. The three entities used are government healthcare office (SG), server of a healthcare provider (SH), and patients. The main three phases of the scheme include registration, encryption and decryption.Initially, the patient needs to register with SG to avail a healthcare card that makes him appropriate for the medical services offered by SH. The encryption phase involves encrypting PHI through enabling the health data card by entering the user PIN or by biometric verification. This can be done by generating a session key and cryptographic checksum by concatenating the hash value of patients' master key and the session key of healthcare provider. The decryption conducted is two fold, one with patient consent and the other with emergency cases. This can be done by computing the master key and session key of the healthcare provider. A secure EMR sharing scheme has been proposed by Li et al. [34] to improve the unlinkability between patient and EMR. EMRs are encrypted using symmetric key encryption using a one-time key and records are stored anonymously. Doctors use digital signatures using a private key to process electronic medical records. This approach requires an EMR number i.e. the PID, SID, the identity seed which is stored in the patients' medical card and the random value R, which created by the doctor to access the EMR of the patient. Each key used in this process is used for encrypting one EMR, increasing the confidentiality of each electronic medical record. Since the identity seed SID is based on smart data card, medical records cannot be read without authorization.

An EHR sharing and integration system has been proposed by Chen et al. [35] to protect the EHRs in normal and emergency situations in hybrid healthcare clouds. This approach encrypts each medical record using an individual symmetric key ck using a symmetric encryption scheme in public and private cloud environments. Here, the doctor creates the patients' health record and it is encrypted by the symmetric key ck along with a license L. This license provides an emergency key to access the encrypted data by the cloud even if the server is not provided with direct access. The patient has to provide the smart card to the doctor for the decryption of their EHR. This design encrypts all the medical records and decryption is possible only by patients' private keys in which the private key is split into two parts, whereas one among the keys will be escrowed by the hospital server and the other key will be stored on the patient's smart card. The downside of this approach is that the license file also need to be encrypted with the hospital's public key. A new dynamic access control scheme for PHR is proposed by Chen et al. [36] under the cloud computing environment. This scheme uses Lagrange interpolation polynomial to establish a secure PHR information access that ensures security which

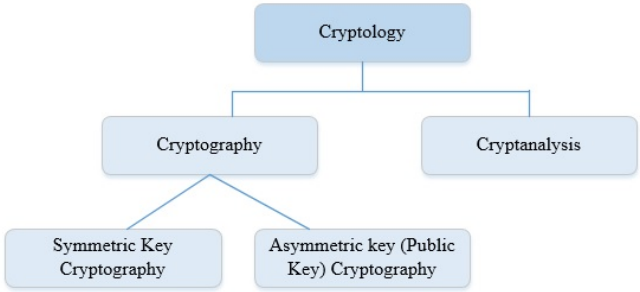


Figure 5: Basic types of Cryptography

is suitably scaled for large number of users. The approach adopted cryptography based on Lagrange multipliers for encrypting the health records ensuring that every patient has maximum control over their medical records. By allowing every patient to generate his/her own related keys, users can choose with whom to share their health records.This reduces key management complexity, and at the same time allows users to not only retain access control of PHR, but also permits issuance of limited access rights to other users, such as doctors, pharmacists, nurses, researchers etc. This approach carries computational overhead. To reduce the complexity of key distribution, this method overhaul past hierarchical models and created partial order relation to manage users. This is a very flexible approach for multi-user dynamic access control in coordinating the needs for immediate addition, or removal of user access, and also for the addition and modification of PHR, making it more suitable for PHR cloud application.

Zhang et al. [37] presents a role-based and time-bound access control (RBTBAC) model which is an integration of RBAC and a time-based access control model that ensures the security and privacy of EHRs on untrusted cloud servers. This model is a logorithmic composition of RBAC and time-bound hierarchical key management in which an authorized user of the EHR system who is alloted a time period can access the data on the basis of his role. This model extends greater flexibility in spatial and temporal capabilities to restrict access to sensitive data. The EHR are encrypted through SKE. This work developed a role-based privacy aware access control and management of EHR data and also utilized a time tree method which offers time bound access control and authorization. In this approach, a user requires to work in several roles and also owns and administers multiple keys. It is requisite to encrypt the sensitive medical healthcare records prior to uploading to the semi-trusted cloud servers. As searching encrypted data is arduous, Searchable Symmetric Encryption(SSE) [38] has been proposed that enables keyword searches across encrypted cloud data. This approach presents a highly efficient and Secure Dynamic Searchable Symmetric Encryption(SEDSSE) in medical cloud data by leveraging the secure k-nearest neighbor (kNN) and ABE techniques. This

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access

Table 3: SKE based Approaches

Sl No.	Technique(s) used	Strength	Weakness	Privacy Requirements							Reference
				IN	CO	AU	NR	AC	AN	UN	
1	Symmetric Key Encryption (SKE), Smart Card (SC) , Digital Signature	-	Usage of smart card for every access	✓	✓	✗	✓	-	-	-	[33]
2	Symmetric Key Encryption (SKE)	Unlinkability among Electronic health records	Infeasible Portability technique	✓	✓	✓	✗	✗	-	-	[34]
3	SKE, SC,license file	Data Ownership is ensured	Smart card is required for retrieval	✓	✓	✓	✓	-	-	-	[35]
4	SKE	Ensures patients' data ownership	Emergency access provision is insecure	✓	✓	✗	✓	✓	✗	✗	[36]
5	SKE	Key distribution issue is resolved	Difficult to manage multiple user roles	✓	✓	✓	✓	-	-	-	[37]
6	Searchable Symmetric Encryption(SSE), AES	Dynamic searchable symmetric key encryption and resolves key sharing problem	Cannot support multi-keyword search	✓	✓	✓	-	-	✓	-	[38]

* IN: Integrity, CO: Confidentiality, AU: Authentication, NR: Non Repudiation, AC: Accountability, AN: Anonymity, UN: Unlinkability

approach used an AES symmetric encryption algorithm to encrypt the documents and shares the symmetric secret key only with authorized doctors who satisfy the access policy related to ABE.

From Table 3, it is evident that even though most of the SKE based approaches satisfies IN and CO, but still lacks AN, UN, AC and NR due to the following reasons. In SKE approaches, both the sender and the receiver are required to trust each other as they will be sharing the same secret key for encryption and decryption that makes anonymity almost impossible. In SKE techniques, non-repudiation and unlinkability would be violated if the user-credentials such as passwords or smart cards were lost, shared or stolen. Moreover, the use of shared user IDs and passwords destroys accountability. Most of the methods in SKE fails to mention the procedure to restore anonymity or the key. Moreover, these schemes are unable to operate in dynamically changing cloud environment because of its inflexible access control and inability to manage multiple user roles.

2) PKE based Approaches: The PKE approaches entails two separate keys; one public key and one private key. Autonomous PKE schemes are computationally inefficient because of its slower operations and large key sizes. Therefore, PKE schemes can be more efficient in combination with SKE schemes in which SKE schemes can be used for encrypting the contents and public private key pairs can be used to secure the symmetric keys. This framework [39] used Public Key Infrastructure (PKI) to address diverse security requirements such as authentication, confidentiality, integrity, access-control, non-repudiation etc whereas the EHR are encrypted using a shared symmetric key generated by healthcare providers. PKI binds public keys with unique user identities which consist of digital certificates, a Registration Authority, a Certificate Authority, a Certificate Repository Database and a Certificate Management System. This proposed architecture builds a secure EHR sharing framework that ensures effective sharing of EHRs between patients and several healthcare providers. Authentication between EHR sharing cloud and healthcare providers are achieved by signing the documents with senders private key so that only the targeted healthcare

provider can verify the signature to retrieve the equivalent health records. PHR privacy is ensured in this framework [40] by creating a security model called Online Referral and Appointment Planer (ORAP) in which medical information is encrypted at the client side. In ORAP model, EHR are cached in a trusted environment, i.e. at physicians practice locale. EHRs are encrypted by the public key of the receiving entity and signed before being transmitted to the cloud and decryption is restricted to authenticated entities only. This framework used the Amazon S3 cloud for temporary storage and German healthcare telematics infrastructure components for providing secure and strong encryption and signatures for all documents transferred to the patients health record. Comparison of a few PKE based approaches is portrayed in Table 4.

Mashima and Ahamad [18] designed a patient-centered monitoring system to safeguard the risk of storing and accessing electronic health information in the cloud. This work developed a system that allow the patients to have explicit or implicit control regarding when and how the medical information is accessed. Health records are encrypted through Public Key Encryption with associated hash values [41]. Universal Designated Verifier Signatures (UDVS) that generates a designated verifier signature is also introduced as part of this work to ensure patient record usage is restricted to authorized entities. The main drawback with this system is that the confidentiality of the record is compromised as the health data is initially built by an issuer who has information about the details of record, hash values, and signatures. One of the prominent works mentioned in the literature is that of Xun Yi et al. [2] that provides a multiparty framework which ensures patient privacy in which all the EHRs are encrypted with a common public key and decryption needs the cooperation of all concerned parties. This approach is constructed on PKI based on the ElGamal Threshold public key encryption scheme [2]. This scheme uses modular exponentiation which is less computationally expensive and where re-encryption is not required. This prevents any server and collusion of upto $n-1$ servers and therefore can succeed from internal and external attacks and also achieves n server joint authentication over only one database. Narayan proposed a cloud based EHR system by integrating [16] symmetric key cryptography, public key cryptography and attribute based encryption. In this approach, medical data will be encrypted by a patient's symmetric key and the metdata file which describes information regarding access policy. Location information is encrypted using broadcast CP-ABE before storage in the cloud. This approach supports direct revocation without data re-encryption but entails additional costs on the patient side since re-encryption and updating of access policies are borne by them. Another drawback is that all the encrypted files can be accessible by the trusted authority.

A solution to address the security issues is by using a security architecture on Trusted Virtual Domains(TVDs) in e-health infrastructure. This work [42] make use of TVD to establish access control by employing three privacy domains; trusted, e-Health and untrusted domains. TVDs are a collection of different Virtual Machines that have common security policies and trust each other. TVD systems have the advantage of flexibility when integrating with legacy systems. This approach make use of PKE encryption for storing and transmitting e-health data in external storage. The main drawback associated with this approach is the complexity to deploy the TVD based solutions and scalability issues where these domains are executed on a host computer. Pecarina et al. [43] described a PKE-based framework to enhance privacy by providing anonymity in data storage and efficient access control to authorized collaborators in a semi-trusted health cloud [44]. PHRs will be encrypted by the patient using the public key of a CSP (Cloud Service Provider) prior to storage in the cloud. Decryption of the patient records is carried out by CSP using its private key. After storing PHR at a location, the location is finally encrypted through the SKE of CSP. This work [45] proposed an efficient homomorphic encryption for the encryption of medical data images without hindering the data confidentiality. A Probabilistic algorithm is used for both key generation and encryption. This approach stored images in a standard format, namely Digital Imaging and Communications in Medicine (DICOM), and converts the input image into a matrix followed by performing key generation based on the homomorphic property and encryption using homomorphic public key encryption before transmitting to the cloud. Efficiency of the data is performed by using Peak Signal to Noise ratio (PSNR) and Mean Square Error (MSE) analysis, histogram analysis, and correlation analysis etc. An efficient key word search mechanism which employes public key encryption has been proposed by Mimi Ma et al. [46] for a flexible healthcare system in cloud servers. This approach constructs an encrypted keyword index with users public key attached to encrypted health data prior to uploading to the cloud server. It makes use of a trusted key generation center to generate the master key, public parameters and the users partial private key. This work addressed key management problems and key escrow problems with minimum computational cost and complexity.

From the discussion, indisputably PKE schemes in the cloud are computationally inefficient to some scenarios due to their larger key sizes. Some of the existing PKE techniques fails on the confidentiality of health data as it is compromised by an authorised entity who exploits the data ownership. In some PKE techniques, authenticity is not satisfied considering all the encrypted files are accessible by the trusted authority who exploits the trust. Many of the Public key systems use a third party called a Certification authority (CA) to digitally sign their public key, turning into a digital certificate to make it safe. However, if the CA gets compromised, the attacks can happen by masqueraders so that the data will be sending to a wrong destination. Furthermore, public key cryptography can

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access

Table 4: PKE based approaches

Sl No.	Technique(s)	Strength	Weakness	Privacy Requirements							Ref.
				IN	CO	AU	NR	AC	AN	UN	
1	PKI,SKE,Digital Signature	Secure Electronic Health Record Sharing	Incompatibility in different EHR representations	✓	✓	✓	✓	-	-	-	[39]
2	Public Key Encryption (PKE), Digital Signatures	Secure EHR referral	Inadequate patient centric functions	✓	✗	✓	✓	✓	-	-	[40]
3	PKE, Signature verification	Patient control over health data	Misuse by record issuer	✓	✓	✓	✓	✓	-	-	[18]
4	ElGamal PKE, PKI	Resilient against Inside attacks	Expensive computation, Not suitable for dynamic access control policy	✓	✓	✓	✓	-	✓	-	[2]
5	Broadcast ABE, PKE with keyword search	Efficacious user revokement	Obstinate access control	✗	✓	✗	✗	✗	-	-	[16]
6	PKE, Digital signature	Trusted Virtual Domain utilization	Scalability issues	✓	✗	✓	✓	-	-	-	[41]
7	PKE, pseudonymity	Anonymity between user and provider	Service provider may misuse health data contents	✓	✓	✓	✓	✗	✓	✓	[42]
8	Homomorphic encryption, Probablistic algorithm	Security of medical images	Restricted to medical image pocessing	✓	✓	✓	✓	✗	-	-	[43]
9	PKE with keyword search	Address key management problem, Key escrow problem, min computational cost and complexity	Requires a trusted key generation center, Insider attack is possible	✓	✓	✓	✓	✗	-	-	[44]

encrypt data only up to the key size hence the distribution of public keys are troublesome in environments to handle large data sets. While some schemes are designed to protect against insider attacks, other schemes focus on patient centred PHR in which the records are first created by record issuers who knows the content of records, corresponding hash values and signatures. Consequently, inside attacks can happen when an issuer himself misuses health records created by him, forfeits data integrity. Compromising secret keys Sk of the patient and Monitoring by third party loses the data confidentiality. In addition, some other schemes have also discussed that PKE technique has a slightly higher computational cost due to re-encryption of records when updating access policies.

3) Overview Of Alternative Cryptographic Primitive Approaches: This section discusses an overview of alternative cryptographic approaches for securing privacy in e-health clouds. The primitives include ABE, SE, IBE, homomorphic encryption, proxy re-encryption etc.

a) Attribute-based encryption (ABE) Approaches: Attribute based encryption introduced by Sahai and Waters [47] is based on public key encryption to protect cloud data where the encryption and decryption is on the basis of user attributes. In ABE, the encryption is based on the access-structure policy in which the cipher text can be decrypted only when the user attributes match with the ciphertext attributes. The two main types of ABE are Cipher Text Policy Attribute-Based Encryption (CP-ABE) [48] and Key Policy Attribute-Based Encryption (KP-ABE). In KP-ABE, the access policy is enciphered in the user's secret key and decryption of cipher text is possible only when the user attribute matches with the access policy [47], whereas in CP-ABE [49] the private key of each user is tied to a set of attributes and a cipher text is associated with a universal set of attributes which can be decrypted when the user attributes match the access policy. This ABE based approach [50] preserves the confidentiality of EHR by using PKE for

scalable authorization. The smartcard of the patient generates a Transaction Code (TAC) which is the authorization secret, before the medical data is uploaded to the cloud server. PKE is used for authentication and the patients smart card and TAC as authorization. The health professional needs to enter the TAC to encrypt the medical data and the Encryption/Decryption function generates a public key for encryption which is the hash value of the patients identity and TAC. The decryption can be performed using TAC and authentication from a Private Key Generator (PKG). The problem of achieving confidentiality, scalability, and fine-grained access of outsourced data in the cloud are enumerated by Yu et al. [17]. This approach resolves problems, including key distribution and data management issues, by combining techniques such as ABE, KP-ABE, Proxy Re-encryption (PRE), and lazy re-encryption as a hybrid encryption scheme to secure fine-grained access control. The data encrypted by a single user will be shared among different users by key distribution. In this approach re-encryption of data files and updates of secret keys are consigned to cloud servers. A copy of users secret key is kept with the cloud servers for updating of secret key components and re-encryption of data files. Lazy re-encryption is used to reduce computational overhead in cloud servers. It can restrain the revoked users from capturing the updated information once the file contents and keys are modified post user revocation. A patient centered cloud based EHR system that integrates symmetric key cryptography, public key cryptography and an attribute based broadcast cipher text policy Attribute-Based Encryption (bABE) architecture is proposed [16]. This method allows for the encryption of health data using a symmetric key and metadata files that include a description of the file, attribute based access policy. Location based information is encrypted using broadcast CP-ABE by the patient and enables them to store within a cloud platform. This approach also includes a key word search functionality by amalgamating bABE and PKE with Keyword Search (PEKS) [51] to carry out private searches in encrypted data without unveiling the matches to the cloud. Even though this approach facilitates direct revocation without data re-encryption it entails additional computational costs as re-encryption and updating of access policies are borne by the patient. An additional drawback exists with the internal vulnerability of access to encrypted files by the trusted authority without referenced to a permissioned user. The comparison of a few ABE based approaches with its strength and weakness is shown in Table 5.

Efficient and Secure Patient-centric Access Control Scheme (ESPAC) [52] for the cloud using CP-ABE ensures PHI privacy permitting data requesters to access the health data in accordance with role based access privileges. For secure communication between remote patient and e-health cloud provider, IBE is employed, wherein the access control is handled by CP-ABE. A novel technique by Ruj [53] presented an ABE-based access control mechanism that maintains user anonymity for storing PHRs in the cloud. The user identity is unknown to the cloud but the verification of user credentials and communications between users and the cloud are secured by Secure Shell Protocol, SSH. This approach is collision resistant and is resistant to replay attacks and has a decentralized key distribution.To facilitate flexible and effective access control for PHR, this scheme suggests an efficient patient centric framework [48] which employs ABE to encrypt a patient's PHR file before uploading to the cloud.This scheme provides several data owner settings and also categorizes the PHRs into two different sub-domains viz public and private to address key management hurdles. This approach [54] instigates heirarchical attribute based encryption with a keyword search scheme that ensures confidentiality of EHRs in the cloud environment. This scheme encrypts a single access structure in which the trusted authority will issue public and private key pairs.The access policy and time period is set by the information owner before outsourcing the data to the cloud. A proxy re-encryption scheme is also implemented to deny access after the predefined time period defined by the information owner. This work assures fine grained access control, versatile client revocation and lesser storage and encryption time costs compared to other systems.

Even though ABE provides dynamic access control and key management, it still experiences some drawbacks. One of the limitations with ABE is that the data owner needs to use the authenticated users public key for encryption [21]. The drawback with KP-ABE is that the owner of the data cannot decide who can decrypt the encrypted data as the data owner has to trust the key issuer and also suffers with poor scalability issues. Consequently, the Non-repudiation cant be guaranteed. In CP-ABE, attribute management and key distribution are managed by a trusted authority. ABE schemes are most efficient among encryption techniques and provide fine-grained and well-formed access to health records but still infeasible for proper execution on EHRs due to its expensive computation [28] [30], key management complexity and challenge in managing access control policies [25] when attributes in the access structure grows [26]. Another down side is that since most of the ABE schemes use a semi trusted entity who manages the servers and provide cloud services, and for this reason become a threat to data integrity.

b) Searchable Encryption: - Due to the massive growth of big data there exists large scale outsourcing of data into cloud servers. As medical data and EHRs are outsourced to remote cloud servers that are exposed to cloud service providers, this leads to various attacks such as either DoS attacks or adversary attacks that destroys the data confidentiality in the cloud. For protection of data and prevention of information leakage, cloud data will be encrypted. Since the health data is encrypted and stored in third-party Cloud servers, normal searching schemes cannot be applied. It requires some searchable encryption implementation to query the data as shown in Fig. 6. As searching encrypted data is arduous, SSE has been proposed that enable keyword searches

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access

Table 5: ABE based approaches

Sl No.	Technique(s) used	Strength	Weakness	Privacy Requirements							Ref.
				IN	CO	AU	NR	AC	AN	UN	
1	PKE, ABE	Flexible Access control	Linkability among Electronic Health records	✗	✓	✗	✓	✓	-	-	[16]
2	Broadcast ABE, PKE with keyword search	Effective user revokement	Rigid access control	✗	✓	✗	✓	✗	-	-	[49]
3	KP-ABE,PRE,Lazy re-encryption	Scalable access control	Computational overhead	✗	✓	-	✗	✓	-	-	[17]
4	CP-ABE, IBE, digital signatures	patient-centrical access policies	Communica-tion delays	✓	✓	✓	✗	✗	✗	✗	[50]
5	ABE	Maintains user anonymity of data storing entities	Cloud is aware about health record access policy	✗	✗	✓	✗	✓	✓	-	[51]
6	MA-ABE	Efficient user revocation	Restricted access policy specification	✗	✓	✓	✗	✓	-	-	[46]
7	Hierarchical-ABE with Keyword Search, Proxy re-encryption	Fine grained access control, versatile client revocation	Single keyword search is possible	✓	✓	✓	✗	✓	-	-	[52]

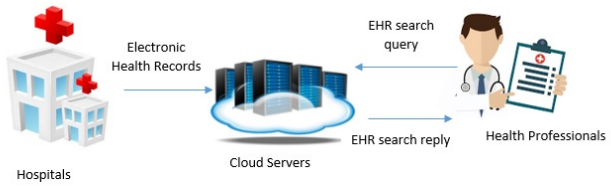


Figure 6: Searchable Encryption

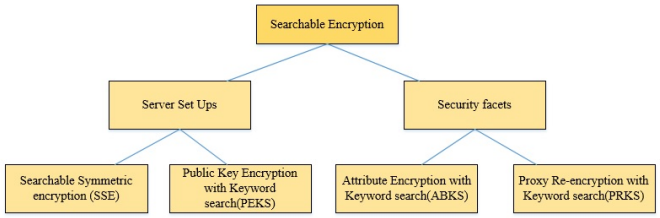


Figure 7: Classification of SE techniques

across encrypted cloud data. This poses challenges such as (1) How the data owner permits search permissions to the data user? (2)How the authenticated data users search the encrypted stored data? One of the solutions is SE. SE is a cryptographic primitive that permits search operations over encrypted data without disclosing the information to untrusted servers. These search operations are performed on encrypted ciphertext with the support of a trapdoor function from user. The main two types are symmetric searchable encryption and asymmetric searchable encryption [55]. This approach is initially introduced based on symmetric cryptography [56] that facilitates controlled searching where the untrusted server is unable to retrieve the original plaintext.

Here we discuss SE and categorize its use cases into four schemes viz Searchable Symmetric Encryption (SSE), Public Key Encryption with Keyword Search (PEKS), Attribute-based Encryption with Keyword Search (ABKS), Proxy Re-encryption with Keyword Search (PRKS) as shown in Fig. 7 and their comparison is presented in Table 6 and Table 7. A searchable encryption service contains three types of entities: a data owner, a data user (data users), and the untrusted cloud [57]. The data owner is a cloud service user who outsourced the original data to a third-party cloud. Different healthcare application scenarios require different searchable encryption schemes. We can characterize existing healthcare application scenarios into four categories: (1) When the outsourced data are searched only by the data

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access

owner, where the data owner is the only authorized data user to search the encrypted data, SSE schemes can be applied in this scenario. (2) When the outsourced data are shared with another user, i.e. there is only one authorized data user who can create the search tokens and search the encrypted data, PEKS schemes are suitable for this one-to-one scenario. (3) When the outsourced data are shared with several users, i.e. more than one authorized user have the permission to search the encrypted data, ABKS schemes can be used in this one-to-many scenario. (4) When the data owner is unavailable and cannot directly grant the search authorization upon emergency, it needs an authorized delegate user to re-authorize the search permission to other user(s) on behalf of the data owner. PRES schemes are applicable to this authorization-delegation scenario [57].

• **Searchable Symmetric Encryption (SSE)** SSE is a symmetric key encryption technique which outsources the data confidentially from one party to another by providing selective search capabilities. This model uses proxy re-encryption [58] that shares medical data in the cloud with end-to-end data encryption that confines data access only to authenticated recipients. This approach [59] preserves the privacy and security in e-Health systems with a new cryptographic technique named as a conjunctive keyword search with designated tester and timing dependent SE schemes named proxy rencryption function (Re-dtPECK).The EHR documents are encoded by symmetric encryption algorithms and a symmetric key is encapsulated with the patients public key by key encapsulation. This makes use of a delegation function θ to perform operations and uses a conjunctive keyword search mechanism. This approach proposes a novel SSE scheme [60] which provides searching according to the unique keywords stored on the server. The search time is logarithmic and the client can search and update the document whenever required. This makes use of two variant schemes in which the first one is an interactive scheme and the second one is non-interactive in which the former needs two rounds of communication for the index generation, updates, and search whereas the latter can be deployed using a hash chain. This method [61] states an SSE procedure which supports conjunctive search and boolean queries on stored data which is symmetrically encrypted and focus on a single keyword search mechanism. This model provides higher security and scales to very large databases. By preserving keyword privacy, this approach [62] validates and resolves the issue regarding fuzzy keyword searches across encrypted data in the cloud. Fuzzy keyword searches enrich system utility by providing matching files or nearest possible matching files for the user input with the predefined keywords based on keyword similarity semantics, otherwise. This solution precomputes fuzzy keyword sets with edit distance to evaluate keyword similarity and also minimizes the storage and representation overheads by developing an advanced mechanism on constructing fuzzy keyword sets.

• **Public Key Encryption with Keyword Search (PEKS)** PEKS is a cryptographic approach that uses a public key system to search across encrypted data. Boneh et al. [63] proposed PEKS as an initial scheme which does not uncover any information pertaining to users searching in the public-key setting and with lesser communication complexity. This technique [64] proposes a weak key unlinkability that provides a broader view on trapdoor privacy in asymmetric searchable encryption for IBE. The main purpose of this scheme is to build an anonymous IBE scheme that fulfils both key unlinkability and enhanced functional privacy. This approach [65] addresses three main issues of a PEKS scheme viz removal of secure channel, refreshing keywords, and processing multiple keywords. The idea of PKE with registered keyword search (PERKS) has been presented by Tang and Chen [66]. This scheme provides flexibility in such a way that the sender is able to register a keyword with the receiver prior to the sender generating a tag to build searchable content. This makes the scheme more efficient and secure against offline keyword-guessing attacks.

• **Attribute Encryption with Keyword Search (ABKS)** ABKS is a cryptographic searching approach which uses attribute-based encryption for data encryption. This searching technique permits keyword searches over encoded EHR data by authorised users whose attributes fulfill the access policy. Yang [67] proposed a multi sender and user scenario that enhances fine grained access control and supports flexible user revocation using a flexible keyword searching technique and attribute based encryption. This scheme introduced a novel fundamental named as Attribute Based Searchable Encryption with Synonym Keyword search function (SK-ABSE). An ABE scheme described by Li et al. [68] implements keyword search functions with outsourcing key-issuing and outsourcing decryption (KSFOABE). In this scheme, the cloud service provider undertakes partial decryption tasks assigned by data user without having any information regarding the plaintext which is secure and robust against chosen plaintext attack. Verifiable Attribute-Based Keyword Search (VABKS) [69] solution permits a data user to only search over the data owners outsourced encrypted data whose credentials match with the data owners access control policy . Liu et al. [70] presented a new approach called Key Policy Attribute-Based Keyword Search(KP-ABKS) that removes secure channel for validation of the searched result from the cloud that reduces the computation complexity on VABKS.

• **Proxy Re-Encryption with keyword Search (PRKS)** PRKS is a cryptographic fundamental that uses a proxy re-encryption system for searching encrypted data. It permits an authenticated data user who permissions the search capability to other users by re-encrypting the outsourced data [57]. The proxy re-encryption with keyword search functions (PRKS) as the union of two schemes, Proxy Re-Encryption (PRE) and PEKS. This approach [71] provides two security concepts for bidirectional PRES (Proxy Re-encryption Scheme) : privacy

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access

Table 6: Comparison of SE techniques (SSE and PEKS)based on Server Set Ups

Scheme	Set Ups	Main Operations	Query Type	Performance
Re-dtPECK Scheme [56]	Multiple server	Time dependent Search,Symmetric Encryption,Proxy Re-encryption	Conjunctive Keyword	Higher Security and Confidentiality, Overcomes Keyword Guessing Attack (KGA)
SSE for Boolean queries [58]	Cloud Server	Symmetric Encryption, Diffie Hellman	Single keyword	Higher Security, Scales to very large databases, Moderate data leakage
Fuzzy keyword search [59]	Cloud server	Symmetric Encryption, Edit distance	Fuzzy Keyword Search	Privacy preserving system
PKE with Keyword Search [60]	Single Server	Public Key Encryption, Homomorphic Encryption	Multiple keywords	Preserves privacy, Less communication complexity
Trapdoor Privacy in PKE [61]	cloud server	Asymmetric Searchable Encryption, PEKS, IBE	Multiple keywords	Enhanced Trapdoor privacy,Key Unlinkability
PKE with registered Keyword Search [63]	single server	PEKS, Bilinear pairing	single keyword	Secure against Offline KGA attacks, less computational complexity

for keyword and privacy for message. In keyword privacy, the opponent is permitted to obtain the plaintext of any ciphertext, and nearly all trapdoors, excluding those which are connected to the two specific keywords. Nevertheless, it cannot determine which keyword matches to a given ciphertext. This security idea ensures that the test can only be done by the person who has the trapdoor or token. For message privacy, the opponent is permitted to obtain the plaintexts of nearly all ciphertexts, excluding one and all the trapdoors, but it cannot determine which message matches with the particular plaintext. This security concept ensures that the one who holds the private key can decrypt the ciphertexts. A new cryptographic approach described by Fang et al. [72] called Conditional Proxy Re-Encryption with Keyword Search (C-PRES) is an association of C-PRE and PEKS. This approach offers various benefits over previous schemes, such as chosen-ciphertext security, non-interactivity keyword-anonymity, unidirectionality, and collusion-resistance. Shi et al. [73] presented an approach in which the encrypted data will be outsourced to the cloud by the data owner to perform the keyword search on encrypted data with the specified search token. The idea is to combine ABE and PRE in which the data owner permits keyword searches over encrypted data to authenticated users in accordance with access control policies.

We have discussed a survey of Searchable encryption techniques for healthcare applications. However, all existing multi-user SE schemes are not practical with respect to the performance required by critical real-world applications and do not scale well for extensive databases. We categorize and compare the different SE schemes in terms of their security, efciency, and functionality. However, SSE is not a preferred method [65] for querying the search in EHR due to key management issues. Nevertheless, PEKS and PRKS exhibit better performance in terms of security and privacy and are commonly adopted to EHR that supports search functionality.

c) Proxy Re-Encryption: Proxy Re-encryption is a cryptographic approach that permits a semitrusted proxy server to re-encrypt the ciphertext, which is encrypted by one user's public key, into another ciphertext i.e. encrypted by the public key of another user [74]. For example, Alice sends a message (M) to Bob through a semi-trusted proxy server, Without sharing Alices private key to either the proxy or Bob, and without disclosing the secret message to the proxy shown in Fig. 8. Yang [59] introduced a novel cryptographic approach called as Conjunctive Keyword Search with a designated tester and a timing enabled proxy re-encryption function, Re-dtPECK, that uses a delegation indicator θ to perform operations and uses conjunctive keyword for searching mechanism. This scheme proposes a proxy re-encryption mechanism [75] for on the road emergencies that permits an emergency medical center to decrypt a patient's health records wth the aid of cloud servers and user credentials without disclosing the secret key.

Timing enabled proxy re-encryption systems over conjunctive keyword search have been proposed [76] that allow users to access the patient records under a predefined time interval, T. This technique achieves objectives such as Efficient Access Control, User revocation, Efficiency, and Time based revocation.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access

Table 7: Comparison of ABKS and PRKS techniques based on Security facets

Technique	Security facets	Query Model	User revocation
Yang [64]	Effective Data Security	Synonym	Yes
Li[65]	Secure against Chosen Plaintext Attack	Single	No
Zheng [66]	Secure against Chosen Keyword attack, keyword secrecy	Single	No
Liu[67]	Secure against Offline guessing attack, keyword secrecy	Single	No
Shao[69]	Keyword privacy,message privacy	Single	No
Fang[70]	Cipher text security	Single	No
Shi[71]	Selective chosen keyword security	Single	No

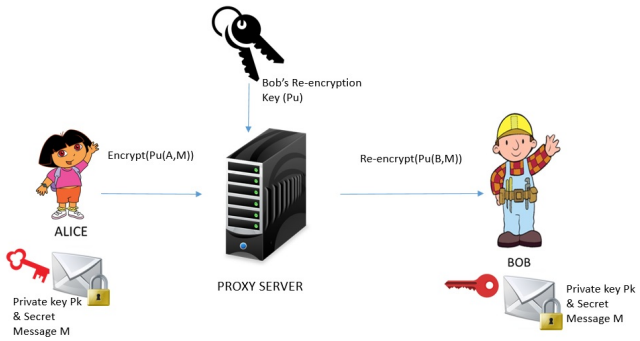


Figure 8: Proxy Re-encryption

d) Homomorphic Encryption: Homomorphic encryption is a type of encryption which performs computation on ciphertexts in which the data is acquired in an encrypted format, when decrypted returns the result of operations if they had been performed on the plaintext. A simple example for homomorphic encryption is shown in Fig. 9.

Barni et al. [77] introduced a multiparty approach for processing the encrypted Electrocardiogram (ECG) using homomorphic encryption to preserve patient privacy. Privacy Preserving Attribute based authentication systems have been introduced [78] for e-health networks which contribute users' verifiable attributes to authenticate users in an e-health system. The proposed scheme relies on homomorphic encryption to guarantee data security, which preserves the privacy of attributes but the computation cost is extremely high. Gentry [79] proposed the idea of fully homomorphic encryption which permits a random number of additions and multiplications over the encrypted data, whereas, Somewhat Homomorphic Encryption(SwHE) executes restricted numbers of homomorphic operations by evaluating circuits of specified depth. Fully homomorphic encryption based approaches are impractical because of their inefficacy. Lauter et al. [80] presented SwHE to perform computations over the encrypted data. This approach [81] implements a hybrid architecture that uses homomorphic encryption and RSA (Rivest-Shamir-Adleman) to enhance e-health data security in private cloud OpenStack platforms. This architecture enables cloud clients to take control of their cryptographic operations and key management rather than the cloud provider. Sergiu et al. [82] designed a privacy preserving diagnosis model using homomorphic encryption which processes data without allowing any information breach to the cloud provider. Data will be encrypted with the private key of the user before uploading to cloud servers and data evaluation will be done on encrypted data in which the results are oblivious to the cloud. This approach integrates state-of-the art components such as, transciphering, automatic compilation, parallelisation, and message packing, to preserve user privacy.

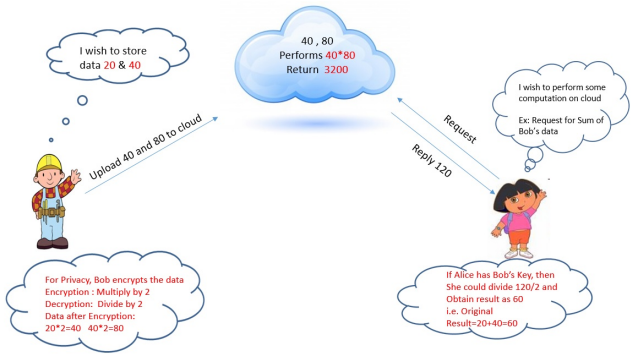


Figure 9: Example of homomorphic encryption

B. Non-cryptographic Approaches

Non-cryptographic approaches mainly use policy-based authorization infrastructure such as, access control policies, to enforce privacy control to the data. In EHR systems where data access is of a highly confidential nature and data is housed on third party severs. Access control mechanisms are inevitable and vital as encryption approaches. In a health care information system access control offers fundamental security barriers to data privacy whereby it limits the access and operation of documents in the EHR system. Some of the main access control techniques are depicted in Fig. 10. Comparison of a few privacy preserving Non-cryptographic mechanisms is shown in Table 8.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access

Discretionary Access Control (DAC) is a form of access control in which the object's owner has whole control over the programs. DAC is based on giving access to objects based on the subject's identity [83]. In MAC, access policy decisions are not made by the individual owners of an object but by a central authority and also the owner cannot change access rights [84]. RBAC defines access decisions on basis of their job functions in which roles have been allocated to subjects, and the roles are associated with permissions that defines which actions can be operated over which objects. ABAC is an authentication based access control in which the decisions for access are performed according to the set of user defined attributes and requesters will be given object access according to attributes that satisfy the policy rules. IBAC is an approach to regulate access based upon the authenticated identity of an individual.

Khan and Ken [85] proposed a context sensitive fine-grained access control mechanism of personal health information by means of discretionary access control and RBAC models. This approach uses eTRON architecture in which authentication is performed using public key cryptography and secure key sharing is established through the Diffie-Hellman algorithm. Harsha et al [86] presented a patient-centric attribute based method in which each PHR file is encrypted and stored along with an attribute based access policy in an e-health cloud that controls the access to the particular resource and also utilizes a proxy re-encryption technique that aids the authenticated users to decrypt the appropriate PHR files. This scheme can resist attacks mounted via attribute collusion and is also capable of provisioning on-demand user revocation. Suhair and Rajendra [87] presented a framework which eliminates the limitations of RBAC and ABAC. This work proposed a BiLayer Access Control (BLAC) in which attributes are integrated with roles and an access request is examined against pseudo-roles before checking the rules within the policy. R.Sandhu et al [88] proposed RBAC in which the roles have been assigned to subjects and roles are also associated with permissions that define which actions can be operated over which objects. This scheme has several drawbacks. It is an expensive process to define and structure the roles, and it only supports policies that are static and defined in advance. Furthermore it cannot support dynamically changing environments [89], and also RBACs coarse-granularity causes internal attacks [90] . Yuan and Tong [20] proposed ABAC in which specific attributes of each subject are used to explain access policies for access permission. ABAC resolves issues of RBAC but it has two problems. Initially, ABAC is arduous because of the large number of rules that are required to be examined for access decisions, and secondly for n attributes ABAC may require 2^n rules [20].

A secure attribute based access control technique for EHR has been presented by Harsha et al. [91] using selective disclosure of the attributes in which the access decisions are made in such a way that the user must acquire the same attribute set that satisfies the defined access policy to the requested resource. This approach employed a Public Key Infrastructure(PKI) for establishing a secure channel to authenticate with the health center. This model [92] integrates several mechanisms such as RBAC and ABAC to provide confidentiality for Electronic health records. A framework that introduces the concept of a provenance based access control combines with RBAC with a distributed rule-based mechanism is proposed [93] to enhance the security of cloud data. Bahga et al. [94] proposed an EHR architecture that attains semantic interoperability between stakeholders. This framework adopts a two level modelling that provides better security and addresses the key requirements of HIPAA and HITECH (Health Information Technology for Economic and Clinical Health act). For secure data storage and secure access a cryptographic model for EHR systems has been proposed [95]. Location awareness and biometric authentication techniques are used for user authentication and steganography techniques are used to conceal EHR data in the cloud by embedding in ECG signals.

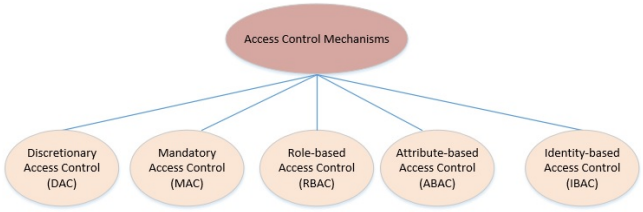


Figure 10: Classification of Access Control Mechanism

Gajanayake et al. [96] presented a new access control technique to preserve patient privacy and confidentiality for EHR by combining three prevalent techniques such as MAC, DAC, RBAC along with a purpose based access control. This work [97] adopted an XACML (Extensible Access Control Markup Language) ABAC mechanism for the protection of EHR against unauthorized intruder access, which supports interoperability. This approach makes use of semantic technologies and an inference engine which uses attributes as classes and rule based policies for decision making. Seol et al. [98] proposed an EHR model that combines ABAC using XACML to preserve patient privacy and ensure security in the cloud environment. This work makes use of partial encryption based on XML and XML digital signature technology for authentication purposes. An attribute based access control scheme [99] for an e-health environment, integrated with controlled access delegation, has been proposed. This approach also performs multilevel access delegation with on-demand attribute revocation mechanisms. An authentication algorithm and RBAC to preserve patient privacy in smart health systems [100] has been proposed. It makes use of three parties, namely Health Authority, Healthcare Professionals, and the Information Consumer. Liu et al [101] introduced an RBAC scheme for EHR on the basis of two roles. One for

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access

Table 8: Comparison of Privacy Preserving Non-Cryptographic Mechanisms

Sl No.	Technique(s)	Strength	Weakness	Privacy Requirements							Ref.
				IN	CO	AU	NR	AC	AN	UN	
1	RBAC	Simpler access administration	Expensive process to define roles	✗	✗	✓	-	-	-	-	[84]
2	ABAC	Dynamic access control policy	Requires large no: of rules	✗	✓	✓	-	-	-	-	[18]
3	BLAC	Combines advantages of RBAC and ABAC	Security threats	✗	✓	✓	-	✓	-	-	[85]
4	RBAC, AES, SSL, MAC	Semantic Interoperability, Scalability	Inflexible access control	✓	✓	✓	✗	✓	-	-	[86]
5	RBAC, PKI	Context and location awareness	Key exchange problem	✓	✗	✓	✗	✓	-	-	[89]
6	MAC,DAC, RBAC, PBAC	Combines three access control models	-	✗	✗	✓	✗	✓	-	-	[90]
7	ABAC (XACML)	Flexible access control	Lack of Confidentiality and Integrity	✗	✗	✓	✗	✓	-	-	[95]
8	ABAC(XACML), XML Encryption	preserves privacy and security	-	✓	✓	✓	✓	✓	-	-	[96]

patients and another for medical staff. Patients are identified by their identity whereas medical staff will be recognized by their roles and access will be given per access policies. This approach also supports user revocation mechanisms.

V. Research Issues and Future Directions

This section discusses the research issues and future directions related to privacy and security in EHR. Since EHR data is sensitive, confidential, and housed in third party servers entails serious risks in terms of data privacy and security. Higher levels of security is utmost needed to prevent, detect, and act on unauthorized access to healthcare system and is required to mitigate social, economic, political and cultural conflicts. Some of the main research issues include :

1. How to secure and safeguard security of stored data in the cloud?
2. How to implement privacy preserved health care data storage?
3. Which access control mechanism will be more efficient for the secure transfer of EHR?
4. Which encryption scheme can be used for preserving data security?
5. How the health data can be effectively shared against multiple healthcare providers?
6. How to maintain integrity of health records?
7. Who will be able to access the patient data with healthcare providers during an emergency situation?
8. What kind of access can be given to Administrative staff to offset inside attacks?
9. How to handle user revocation when an authorized user leaves the system?
10.How to handle key management complexity while sharing healthcare data between disparate healthcare providers?

This review highlighted various research issues pertaining to the privacy and security of e-health data. Therefore we found that there is an imminent need to strengthen the security infrastructure in e-health systems aiming towards patients' to ensure the privacy and security of data thereby securing patient confidentiality and sovereignity. Thus, we bring forth some future research directions as follows:

• From the discussion, we have examined several cryptographic and non-cryptographic mechanisms. Eventhough ABE is most efficient among encryption schemes, Yi et al. [2] investigated and proved that even though ABE is most efficient among encryption schemes , it still suffers from expensive computation and complexity in bi-linear pairing operations. Therefore, recognizing new techniques for reducing the complexity of bi-linear operations or finding ways to outsourcing computations will be an interesting research direction.

• we have observed several access control mechanisms that ensure privacy in which ABAC is the most flexible and convenient providing fine grained access. So, ABAC will be efficient to introduce more flexibility into authorizations which can also be considered as a research direction.

• Introducing secure Provenance for tracking information flow

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access

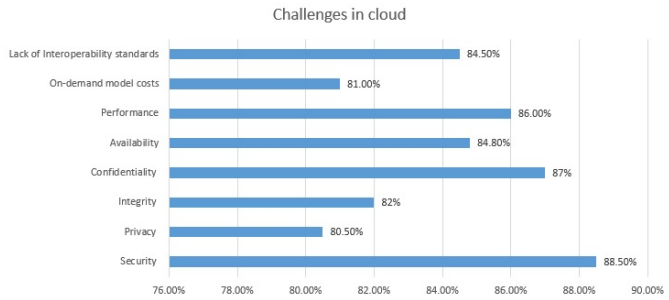


Figure 11: Challenges in cloud

for e-health data would be another interesting area to work on.
• Integrity of health data in the cloud can be another interesting research direction.
• Privacy is a crucial aspect in healthcare. Maintaining privacy and tracking privacy violations by means of accountability mechanisms in healthcare records is essential for fraud detection and prevention. Keeping track of provenance for both data and programs is advisable.
• The great leaps in digital technologies characterised by Social networking, IoT, Big Data Analytics and Cloud computing calls for the immediate attention of all stakeholders to ensure stricter norms of privacy and security with respect to big data. Therefore, combinations of Data Analytics and Artificial Intelligence will be a better research focus to analyze, examine, and prevent threats in healthcare.
• A combination of encryption mechanisms and access control mechanisms to preserve big data security and privacy can also be considered as a future research direction for maintaining a foolproof security mechanism in e-healthcare.

VI. Discussion

From the comparitive review of existing cryptographic and non-cryptographic approaches, we have discussed how several privacy and security mechanisms can be applied to e-health data efficiently. For the comparison, we have examined several crucial factors including the strengths and weakness of existing techniques and characterized each method using several privacy preserving requirements such as IN(Integrity), CO(Confidentiality), AU(Authenticity), NR(Non-repudiation), AC(Accountability), AN(Anonymity), UN(Unlinkability).

The comparison results are indexed in Table 1 to Table 6 in which the symbols "✓","✗" denotes whether the specific privacy preserving requirement is accomplished or not and "-" denotes that a specific requirement is not discussed. From the detailed survey it is evident that most of the techniques are adhere to the privacy preserving requirements but none adhere completely.

From the discussion, it is apparent that most of the existing cryptographic approaches suffer from higher computational cost, complexity in key management and distribution, in addition to vulnerability to a wide range of intruder attacks due to the nature of design, portability and scalability.The review provides a detailed study of cryptographic approaches such as SKE, PKE, ABE, SSE, Proxy Re-encryption and Homomorphic Encryption in which the SKE suffers from inflexible access control which further entails user presence for every smart card access. SKE schemes are unable to operate in a dynamically changing cloud environment because of its inability to manage multiple user roles. It is evident that PKE schemes are computationally inefficient due to larger key sizes. Eventhough existing ABE based mechanisms have the advantage of defining access structures and are superior in preserving privacy levels, the computation of bilinear pairing in ABE is very expensive. One of the main limitations found in the existing techniques is that they are administered and controlled by a central trusted entity. Moreover, among the access control mechanisms, RBAC is inflexible in dynamically changing environments and the task of defining structure and roles in RBAC is quite expensive too. ABAC is significantly efficient in handling access control, but it requires a large number of rules for decision making.The non-cryptographic approaches have several limitations on their expensive processes to define and structure roles, policies, and are inefficient operating with in a dynamic environment. From the review, it is also evident that SE schemes are not extensively used for handling healthcare data in the cloud environment due to computational limitations and an inability to withstand intruder attacks. The majority of the approaches described are incapable to withstand internal and external attacks due to the lack of proper privacy preserving mechanisms. However, we have discussed several mechanisms and pointed out the advantages and disadvantages, but these existing techniques still fail to achieve security, privacy and integrity of health data in an e-health deployment. From Fig. 11 it is obvious that security is a crucial concern in the cloud environment as cyber threats are increasing exponentially. Therefore, there is an imminent need to preserve security of EHRs against security breaches and to stregthen the security infrastructure in healthcare to ensure patient confidentiality.

One of the solutions to overcome all these limitations in the existing system is to introduce patient centered electronic health system namely, Personally Controlled Electronic Health Record System, in which the patient will be the universal consent provider of their data (except in emergency situations) to all stakeholders viz doctors, pharmacists, nurses, scientists etc. Blockchain technology [102] can be used as an underlying access control tool to support this distributed ledger mechanism in the cloud. A secure Blockchain based EHR system in cloud is depicted in Fig. 12. Smart contracts are intelligent permission contracts or codes that are written which verifies data ownership, permissions and integrity of data [103]. This approach will be a tamper proof mechanism as every health transaction information will be stored as hash values in the blockchain. It has immense potential to ensure security, privacy, confidentiality, availability and integrity of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2919982, IEEE Access

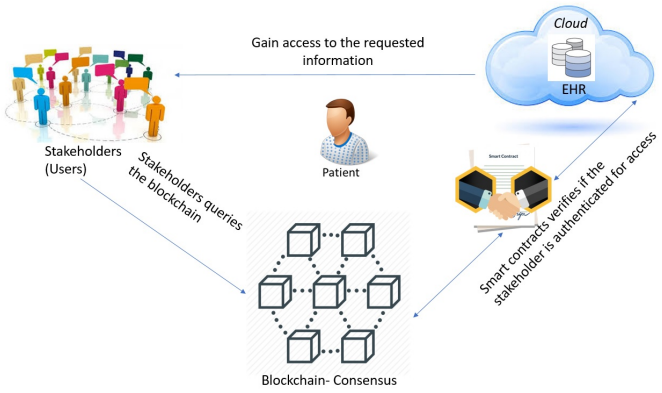


Figure 12: Secure Blockchain based EHR System in Cloud

the e-health information. The introduction of this technological advancement that integrates cryptographical aspects provides a secure and efficient framework for efficient storage, transfer and access of electronic health records in the cloud environment.

VII. Conclusion

Smart health care services are a great boon and are dominantly used by patients, doctors and other healthcare providers nowadays. Since the majority of data is stored in cloud servers, which is highly susceptible to threats and breaches, there is an imminent need to safeguard them from unauthorized access. Existing smart health solutions provide a certain level of immunity but not a foolproof mechanism. In this context a major breakthrough in research to sustain the confidence and credibility of patients is essential for the wide scale usage and success of the digital health care. This review highlights a comprehensive study of existing e-health cloud preserving cryptographic and non-cryptographic mechanisms to secure privacy aspects in cloud and their vulnerabilities in fast changing digital era. More over, our work also provides and identifies key research areas with diverse aspects viz architecture, encryption techniques, access control mechanisms and has also identified some remarkable research issues and future research directions to bring deliberate action for ensuring foolproof privacy in smart health solutions. The evolution of a holistic security mechanism as suggested by this work can make health care data more secure and sustainable.

VIII. Conflict of Interest

None.

IX. Acknowledgment

The authors would like to thank Prof. Yuan Miao and Dr. Hui Cui for their valuable comments, suggestions and reviews.

References

[1] N. Dong, H. Jonker, and J. Pang, "Challenges in ehealth: From enabling to enforcing privacy," in *International Symposium on Foundations of Health Informatics Engineering and Systems*, pp. 195–206, Springer, 2011.

[2] X. Yi, Y. Miao, E. Bertino, and J. Willemson, "Multiparty privacy protection for electronic health records," in *Global Communications Conference (GLOBECOM), 2013 IEEE*, pp. 2730–2735, IEEE, 2013.

[3] C. S. Kruse, M. Mileski, A. G. Vijaykumar, S. V. Viswanathan, U. Suskandla, and Y. Chidambaram, "Impact of electronic health records on long-term care facilities: Systematic review," *JMIR medical informatics*, vol. 5, no. 3, 2017.

[4] L. Griebel, H.-U. Prokosch, F. Köpcke, D. Toddenroth, J. Christoph, I. Leb, I. Engel, and M. Sedlmayr, "A scoping review of cloud computing in healthcare," *BMC medical informatics and decision making*, vol. 15, no. 1, p. 17, 2015.

[5] P. Li, S. Guo, T. Miyazaki, M. Xie, J. Hu, and W. Zhuang, "Privacy-preserving access to big data in the cloud," *IEEE Cloud Computing*, vol. 3, no. 5, pp. 34–42, 2016.

[6] A. Abbas and S. U. Khan, "A review on the state-of-the-art privacy-preserving approaches in the e-health clouds," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 4, pp. 1431–1441, 2014.

[7] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, pp. 268–275, IEEE, 2010.

[8] M. Ahmed and A. S. B. Ullah, "False data injection attacks in healthcare," 2017.

[9] M. R. Fuentes, "Cybercrime and other threats faced by the healthcare industry," *Trend Micro*, 2017.

[10] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, "e-health cloud: opportunities and challenges," *Future Internet*, vol. 4, no. 3, pp. 621–645, 2012.

[11] D. McGraw, "Building public trust in uses of health insurance portability and accountability act de-identified data," *Journal of the American Medical Informatics Association*, vol. 20, no. 1, pp. 29–34, 2013.

[12] B. Edwards, S. Hofmeyr, and S. Forrest, "Hype and heavy tails: A closer look at data breaches," *Journal of Cybersecurity*, vol. 2, no. 1, pp. 3–14, 2016.

[13] N. Asokan, V. Niemi, and K. Nyberg, "Man-in-the-middle in tunnelled authentication protocols," in *International Workshop on Security Protocols*, pp. 28–41, Springer, 2003.

[14] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07. 4th Annual IEEE Communications Society Conference on*, pp. 193–202, IEEE, 2007.

[15] 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*, pp. 279–298, Springer, 2007.

[16] S. Narayan, M. Gagné, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, pp. 47–52, ACM, 2010.

[17] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Infocom, 2010 proceedings IEEE*, pp. 1–9, Ieee, 2010.

[18] D. Mashima and M. Ahamad, "Enhancing accountability of electronic health record usage via patient-centric monitoring," in *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium*, pp. 409–418, ACM, 2012.

[19] 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.

[20] E. Yuan and J. Tong, "Attributed based access control (abac) for web services," in *Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference on*, IEEE, 2005.

[21] R. Charanya and M. Aramudhan, "Survey on access control issues in cloud computing," in *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, pp. 1–4, IEEE, 2016.

[22] L. Zhu, C. Zhang, C. Xu, X. Liu, and C. Huang, "An efficient and privacy-preserving biometric identification scheme in cloud computing," *IEEE Access*, vol. 6, pp. 19025–19033, 2018.

[23] W. Li, K. Xue, Y. Xue, and J. Hong, "Tmacs: A robust and verifiable threshold multi-authority access control system in public cloud storage," *IEEE Transactions on parallel and distributed systems*, vol. 27, no. 5, pp. 1484–1496, 2016.

[24] K. Xue, Y. Xue, 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 Transactions on information Forensics and Security*, vol. 12, no. 4, pp. 953–967, 2017.

[25] P.-W. Chi and C.-L. Lei, "Audit-free cloud storage via deniable attribute-based encryption," *IEEE Transactions on Cloud Computing*, vol. 6, no. 2, pp. 414–427, 2018.

[26] 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 journal of biomedical and health informatics*, 2018.

[27] C. Zhang, L. Zhu, C. Xu, and R. Lu, "Ppdp: An efficient and privacy-preserving disease prediction scheme in cloud-based e-healthcare system," *Future Generation Computer Systems*, vol. 79, pp. 16–25, 2018.

[28] 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 *2017 International Conference on Progress in Informatics and Computing (PIC)*, pp. 266–270, IEEE, 2017.

[29] J. Wei, W. Liu, and X. Hu, "Secure data sharing in cloud computing using revocable-storage identity-based encryption," *IEEE Transactions on Cloud Computing*, 2016.

[30] H. Cui, R. H. Deng, and Y. Li, "Attribute-based cloud storage with secure provenance over encrypted data," *Future Generation Computer Systems*, vol. 79, pp. 461–472, 2018.

[31] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, "Information security conscious care behaviour formation in organizations," *Computers & Security*, vol. 53, pp. 65–78, 2015.

[32] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, "Security techniques for the electronic health records," *Journal of medical systems*, vol. 41, no. 8, p. 127, 2017.

[33] W.-B. Lee and C.-D. Lee, "A cryptographic key management solution for hipaa privacy/security regulations," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no. 1, pp. 34–41, 2008.

[34] 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 *Consumer Electronics (ISCE), 2011 IEEE 15th International Symposium on*, pp. 98–103, IEEE, 2011.

[35] Y.-Y. Chen, J.-C. Lu, and J.-K. Jan, "A secure ehr system based on hybrid clouds," *Journal of medical systems*, vol. 36, no. 5, pp. 3375–3384, 2012.

[36] T.-S. Chen, C.-H. Liu, T.-L. Chen, C.-S. Chen, J.-G. Bau, and T.-C. Lin, "Secure dynamic access control scheme of phr in cloud computing," *Journal of medical systems*, vol. 36, no. 6, pp. 4005–4020, 2012.

[37] R. Zhang, L. Liu, and R. Xue, "Role-based and time-bound access and management of ehr data," *Security and Communication Networks*, vol. 7, no. 6, pp. 994–1015, 2014.

[38] 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 Transactions on Cloud Computing*, 2017.

[39] A. Ibrahim, B. Mahmood, and M. Singhal, "A secure framework for sharing electronic health records over clouds," in *Serious Games and Applications for Health (SeGAH), 2016 IEEE International Conference on*, pp. 1–8, IEEE, 2016.

[40] A. Kaletsch and A. Sunyaev, "Privacy engineering: personal health records in cloud computing environments," 2011.

[41] X. Sun, M. Li, H. Wang, and A. Plank, "An efficient hash-based algorithm for minimal k-anonymity," in *Proceedings of the thirty-first Australasian conference on Computer science-Volume 74*, pp. 101–107, Australian Computer Society, Inc., 2008.

[42] H. Löhr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in *Proceedings of the 1st ACM International Health Informatics Symposium*, pp. 220–229, ACM, 2010.

[43] J. Pecarina, S. Pu, and J.-C. Liu, "Sapphire: Anonymity for enhanced control and private collaboration in healthcare clouds," in *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*, pp. 99–106, IEEE, 2012.

[44] X. Sun, H. Wang, J. Li, and Y. Zhang, "Satisfying privacy requirements before data anonymization," *The Computer Journal*, vol. 55, no. 4, pp. 422–437, 2012.

[45] A. Vengadapurvaja, G. Nisha, R. Aarthy, and N. Sasikaladevi, "An efficient homomorphic medical image encryption algorithm for cloud storage security," *Procedia Computer Science*, vol. 115, pp. 643–650, 2017.

[46] M. Ma, D. He, M. K. Khan, and J. Chen, "Certificateless searchable public key encryption scheme for mobile healthcare system," *Computers & Electrical Engineering*, 2017.

[47] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 457–473, Springer, 2005.

[48] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE transactions on parallel and distributed systems*, vol. 24, no. 1, pp. 131–143, 2013.

[49] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pp. 321–334, IEEE, 2007.

[50] T. Hupperich, H. Löhr, A.-R. Sadeghi, and M. Winandy, "Flexible patient-controlled security for electronic health records," in *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium*, pp. 727–732, ACM, 2012.

[51] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *International conference on the theory and applications of cryptographic techniques*, pp. 506–522, Springer, 2004.

[52] M. Barua, X. Liang, R. Lu, and X. Shen, "Espac: Enabling security and patient-centric access control for ehealth in cloud computing," *International Journal of Security and Networks*, vol. 6, no. 2-3, pp. 67–76, 2011.

[53] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy preserving access control with authentication for securing data in clouds," in *Cluster, Cloud and Grid Computing (CCGrid), 2012 12th IEEE/ACM International Symposium on*, pp. 556–563, IEEE, 2012.

[54] B. K. Gowda and R. Sumathi, "Hierarchy attribute-based encryption with timing enabled privacy preserving keyword search mechanism for e-health clouds," in *Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on*, pp. 425–429, IEEE, 2017.

[55] N. Pramanick and S. T. Ali, "A comparative survey of searchable encryption schemes," in *Computing, Communication and Networking Technologies (ICCCNT), 2017 8th International Conference on*, pp. 1–5, IEEE, 2017.

[56] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*, pp. 44–55, IEEE, 2000.

[57] R. Zhang, R. Xue, and L. Liu, "Searchable encryption for healthcare clouds: A survey," *IEEE Transactions on Services Computing*, 2017.

[58] A. D. Gupta, Y. Polyakov, K. Rohloff, and G. Ryan, "Securely sharing encrypted medical information," in *Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2016 IEEE First International Conference on*, pp. 330–331, IEEE, 2016.

[59] Y. Yang and M. Ma, "Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 746–759, 2016.

[60] P. Van Liesdonk, S. Sedghi, J. Doumen, P. Hartel, and W. Jonker, "Computationally efficient searchable symmetric encryption," in *Workshop on Secure Data Management*, pp. 87–100, Springer, 2010.

[61] D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Roşu, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for boolean queries," in *Advances in Cryptology–CRYPTO 2013*, pp. 353–373, Springer, 2013.

[62] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *INFOCOM, 2010 Proceedings IEEE*, pp. 1–5, IEEE, 2010.

[63] D. Boneh, E. Kushilevitz, R. Ostrovsky, and W. E. Skeith, "Public key encryption that allows pir queries," in *Annual International Cryptology Conference*, pp. 50–67, Springer, 2007.

[64] A. Arriaga, Q. Tang, and P. Ryan, "Trapdoor privacy in asymmetric searchable encryption schemes," in *International Conference on Cryptology in Africa*, pp. 31–50, Springer, 2014.

[65] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in *International conference on Computational Science and Its Applications*, pp. 1249–1259, Springer, 2008.

[66] Q. Tang and L. Chen, "Public-key encryption with registered keyword search," in *European Public Key Infrastructure Workshop*, pp. 163–178, Springer, 2009.

[67] Y. Yang, "Attribute-based data retrieval with semantic keyword search for e-health cloud," *Journal of Cloud Computing*, vol. 4, no. 1, p. 10, 2015.

[68] J. Li, X. Lin, Y. Zhang, and J. Han, "Ksf-oabe: outsourced attribute-based encryption with keyword search function for cloud storage," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 715–725, 2017.

[69] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: verifiable attribute-based keyword search over outsourced encrypted data," in *Infocom, 2014 proceedings IEEE*, pp. 522–530, IEEE, 2014.

[70] P. Liu, J. Wang, H. Ma, and H. Nie, "Efficient verifiable public key encryption with keyword search based on kp-abe," in *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2014 Ninth International Conference on*, pp. 584–589, IEEE, 2014.

[71] J. Shao, Z. Cao, X. Liang, and H. Lin, "Proxy re-encryption with keyword search," *Information Sciences*, vol. 180, no. 13, pp. 2576–2587, 2010.

[72] L. Fang, W. Susilo, C. Ge, and J. Wang, "Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search," *Theoretical Computer Science*, vol. 462, pp. 39–58, 2012.

[73] Y. Shi, J. Liu, Z. Han, Q. Zheng, R. Zhang, and S. Qiu, "Attribute-based proxy re-encryption with keyword search," *PloS one*, vol. 9, no. 12, p. e116325, 2014.

[74] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 127–144, Springer, 1998.

[75] K. Rabieh, K. Akkaya, U. Karabiyik, and J. Qamruddin, "A secure and cloud-based medical records access scheme for on-road emergencies," in *Consumer Communications & Networking Conference (CCNC), 2018 15th IEEE Annual*, pp. 1–8, IEEE, 2018.

[76] R. Bhateja, D. P. Acharjya, and N. Saxena, "Enhanced timing enabled proxy re-encryption model for e-health data in the public cloud," in *Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on*, pp. 2040–2044, IEEE, 2017.

[77] M. Barni, P. Failla, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider, "Privacy-preserving ecg classification with branching programs and neural networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 452–468, 2011.

[78] L. Guo, C. Zhang, J. Sun, and Y. Fang, "Paas: A privacy-preserving attribute-based authentication system for ehealth networks," in *Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference on*, pp. 224–233, IEEE, 2012.

[79] C. Gentry and S. Halevi, "Implementing gentrys fully-homomorphic encryption scheme," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 129–148, Springer, 2011.

[80] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?," in *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*, pp. 113–124, ACM, 2011.

[81] A. El Bouchti, S. Bahsani, and T. Nahhal, "Encryption as a service for data healthcare cloud security," in *Future Generation Communication Technologies (FGCT), 2016 Fifth International Conference on*, pp. 48–54, IEEE, 2016.

[82] S. Carpov, T. H. Nguyen, R. Sirdey, G. Constantino, and F. Martinelli, "Practical privacy-preserving medical diagnosis using homomorphic encryption," in *Cloud Computing (CLOUD), 2016 IEEE 9th International Conference on*, pp. 593–599, IEEE, 2016.

[83] K. Punithasurya and S. Jeba Priya, "Analysis of different access control mechanism in cloud," *International Journal of Applied Information Systems (IJAIS), Foundation of Computer Science FCS*, vol. 4, no. 2, 2012.

[84] V. C. Hu, D. Ferraiolo, and D. R. Kuhn, *Assessment of access control systems*. US Department of Commerce, National Institute of Standards and Technology, 2006.

[85] M. F. F. Khan and K. Sakamura, "Fine-grained access control to medical records in digital healthcare enterprises," in *Networks, Computers and Communications (ISNCC), 2015 International Symposium on*, pp. 1–6, IEEE, 2015.

[86] 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 *Collaboration and Internet Computing (CIC), 2016 IEEE 2nd International Conference on*, pp. 46–53, IEEE, 2016.

[87] S. Alshehri and R. K. Raj, "Secure access control for health information sharing systems," in *Healthcare Informatics (ICHI), 2013 IEEE International Conference on*, pp. 277–286, IEEE, 2013.

[88] R. Sandhu, D. Ferraiolo, R. Kuhn, *et al.*, "The nist model for role-based access control: towards a unified standard," in *ACM workshop on Role-based access control*, vol. 2000, pp. 1–11, 2000.

[89] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," *Computer*, vol. 43, no. 6, pp. 79–81, 2010.

[90] E. Chickowski, "Healthcare unable to keep up with insider threats," *Dark Reading (May 2012)*, 2012.

[91] H. S. G. Pussewalage and V. A. Oleshchuk, "An attribute based access control scheme for secure sharing of electronic health records," in *e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on*, pp. 1–6, IEEE, 2016.

[92] M. Sicuranza and A. Esposito, "An access control model for easy management of patient privacy in ehr systems," in *Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for*, pp. 463–470, IEEE, 2013.

[93] J. Lacroix and O. Boucelma, "Trusting the cloud: A prov+ rbac approach," in *Cloud Computing (CLOUD), 2014 IEEE 7th International Conference on*, pp. 652–658, IEEE, 2014.

[94] A. Bahga and V. K. Madisetti, "A cloud-based approach for interoperable electronic health records (ehrs)," *IEEE Journal of Biomedical and Health Informatics*, vol. 17, no. 5, pp. 894–906, 2013.

[95] U. Premarathne, A. Abuadbba, A. Alabdulatif, I. Khalil, Z. Tari, A. Zomaya, and R. Buyya, "Hybrid cryptographic access control for cloud-based ehr systems," *IEEE Cloud Computing*, vol. 3, no. 4, pp. 58–64, 2016.

[96] R. Gajanayake, R. Iannella, and T. Sahama, "Privacy oriented access control for electronic health records," *electronic Journal of Health Informatics*, vol. 8, no. 2, p. 15, 2014.

[97] J. Calvillo-Arbizu, I. Roman-Martinez, and L. M. Roa-Romero, "Standardized access control mechanisms for protecting iso 13606-based electronic health record systems," in *Biomedical and Health Informatics (BHI), 2014 IEEE-EMBS International Conference on*, pp. 539–542, IEEE, 2014.

[98] K. Seol, Y.-G. Kim, E. Lee, Y.-D. Seo, and D.-K. Baik, "Privacy-preserving attribute-based access control model for xml-based electronic health record system," *IEEE Access*, vol. 6, pp. 9114–9128, 2018.

[99] H. S. G. Pussewalage and V. A. Oleshchuk, "Attribute based access control scheme with controlled access delegation for collaborative e-health environments," *Journal of Information Security and Applications*, vol. 37, pp. 50–64, 2017.

[100] P. Tasatanattakool and C. Techapanupreeda, "User authentication algorithm with role-based access control for electronic health systems to prevent abuse of patient privacy," in *Computer and Communications (ICCC), 2017 3rd IEEE International Conference on*, pp. 1019–1024, IEEE, 2017.

[101] W. Liu, X. Liu, J. Liu, Q. Wu, J. Zhang, and Y. Li, "Auditing and revocation enabled role-based access control over outsourced private ehrs," in *High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on*, pp. 336–341, IEEE, 2015.

[102] M. Zhang and Y. Ji, "Blockchain for healthcare records: A data perspective," *PeerJ Preprints*, vol. 6, p. e26942v1, 2018.

[103] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare:medrec prototype for electronic health records and medical research data," in *Proceedings of IEEE open & big data conference*, vol. 13, p. 13, 2016.