EAI Endorsed Transactions
on Pervasive Health and Technology
Research Article EAI.EU

A Survey on Secure Cloud-Based E-Health Systems

Dilip Kumar Yadav[1,*], Sephali Behera[2]

[1] Professor & Head, Department of Computer Applications, National Institute of Technology Jamshedpur, India
[2] M.Tech Scholar, Department of Computer Applications, National Institute of Technology Jamshedpur, India

Abstract

Cloud computing is being used in many applications and several aspects for storing and easy sharing of data. Among various trending uses of this technology, the e-health (electronic health) system is one. The health data records are kept in a semi-trusted third-party supplier (i.e., cloud). Therefore, its security has become the main concern. The e-health data on the cloud should be available only to the data owner. This work presents a literature survey on secure cloud-based e-health systems. Seventy-seven research papers related to secure cloud-based e-health systems are collected from different sources till 2019. These papers are divided into three categories (i.e., crypto, non-crypto, and biometric-based). The security mechanism, advantages, and limitations of research papers are presented for all categories which will be helpful to do further researches in this research area.

Keywords: Cloud, E-health, Security, Biometrics, Cryptography, Storage, Data sharing

Received on 29 November 2019, accepted on 13 February 2020, published on 26 February 2020

doi: 10.4108/eai.13-7-2018.163308

*Corresponding author. Email: dkyadav.ca@nitjsr.ac.in

Acronyms

e-health: Electronic Health
SaaS: Software as a Service
IaaS: Infrastructure as a Service
DaaS: Data as a Service
PaaS: Platform as a Service
SSL: Secure Socket Layer
TLS: Transport Layer Service
P-HR: Personal Health Records
E-HR: Electronic Health Records
AES: Advanced Encryption Standard
RSA: Rivest, Shamir, Adleman
ABE: Attribute-Based Encryption
ECC: Elliptic Curve Cryptography
USB: Universal Serial Bus
IBE: Identity-Based Encryption
IBPRE: Identity-Based Proxy Re-Encryption
IND-sID-CPA: Indistinguishability under Identity-Based Chosen-Plaintext Attack
IND-ID-CCA2: Indistinguishability under Identity-Based Chosen-Ciphertext Attack 2
CP-ABE: Ciphertext Policy ABE
KP-ABE: Key Policy ABE
OTP: One-Time Pad Pin
MAABE: Multi-Authority ABE
eMA-ABE: Enhanced MA-ABE
eRSA: Enhanced version of RSA
MITM: Man-in-the-Middle
DOS: Denial-of-Service
SIS: Secure Index Search
CP-ABPRE: Ciphertext Policy Attribute-Based Proxy Re-Encryption
HE: Homo-morphic Encryption
PE: Proxy re-encryption
HSS-EHRS: Hybrid Secure and Scalable Electronic Health Record Sharing
PuD: Public Domain
PsD: Personal Domain
CP: Cloud Provider
PEP: Policy Encryption Point

WEP: Watermarking and Encryption Point
RP: Randomization Point
AAM: Authentication and Access Control
CA: Central Authority
XML: Extensible Mark-up Language
ABAC: Attribute-Based Access Control
XACML: Extensible Access Control Mark-up Language
RBAC: Role-Based access control
CBEKS: Certificate-Based Encryption with Keyword Search
DSEKRSMS: Dynamic Searchable Encryption with Keyword Range Search and Multi-keyword Search
PET: Privacy-preserving Equality Test
FPB: Fully Private Blockchain
CB: Consortium Blockchain
PBEDA: Pseudonym-Based Encryption and Different Authorities
IPFS: Inter-Planetary File System
E-HIS: Electronic Health Information System
ICMetric: Integrated Circuit Metric
MEMS: Micro-Electro-Mechanical Systems
GDC: Geo-Distributed Clouds
TSA: Traffic Shaping Algorithm
CSRF: Cross-Site Request Forgery
XSS: Cross-Site Scripting
3Ps: Patients (1P), Provider (2P), Payer (3P)
ND: National Database
CrA: Certificate Authority
MACSM: Mandatory Access Control Security Model
ACLSM: Access Control List Security Model
HIPAA: Health Insurance Portability and Accountability Act
DP: Data Processor
DC: Data Controller
SNS: Social Network Service
AIC: Availablity, Integrity, Confidentiality
TVD: Trusted Virtual Domains

1. Introduction

In this current world of digitalization, the cloud computing technology is adapted by many institutes and individuals due to its nature of easy sharing and easy distribution of assets. Cloud computing is a type of model or service that aids omnipresent, suitable, on-demand access to the network to a common pool of computing resources such as networks, servers, storage, applications, and services and requires least management work or service provider collaboration [94]. Applications, servers, networks, and storage with a user-oriented platform are the resource sharing services provided by cloud computing. Two of the basic characteristics of the cloud are; storage, a system used to keep data, and the other one is data sharing, the process of transferring data from one person to another.

So basically, the cloud is a type of virtual storage system used on-demand in which its users can store their personal, financial, business data as well as share them with others. The cloud system can be classified into two types; the first one is public cloud system providing offsite solutions with various models like software as a service (SaaS), infrastructure as a service (IaaS), data as a service (DaaS) and platform as a service (PaaS). Windows Azure services platform and Google AppEngine are examples of the public cloud. The second one is a private cloud which is only meant for a particular organization and its servers are either on the organization premises or offsite. It is far more secure and has better customization than the pre-mentioned cloud system. Examples of this cloud system are Dell, IBM, Cisco, HP [1, 2]. Figures of basic public e-health cloud systems and private e-health cloud systems are shown in figure (a) and (b) respectively. Due to the features like, less complex user-interface, easy and location-independent data storage and sharing between companies or individuals globally, utilization of cloud computing has increased from a few users to the users all over the world [3].

Moreover, cloud computing requires resources like software and hardware from the user's side [1]. Cloud has the ability to accommodate multiple applications for a mass of users who can use those applications for accessing and sharing the data with great flexibility, accessibility, and reliability [5]. Cloud computing is applied in many fields like, business applications, data storage services, maintaining e-health records, etc. Even if the cloud is secured with techniques like Secure Socket layer (SSL) and Transport Layer Service (TLS), it is contemplated as semi-trusted. Therefore, it is necessary to achieve security in the cloud as security is the much-needed aspect to protect any kind of data from attacks, threats or vulnerabilities.

The e-health (electronic health) system as the name suggests is a kind of health system which uses computer or electronic systems and cloud technology as its main source of operations for storing and sharing patient's medical data between healthcare service providers and patients [1]. It is different from the pen-paper based traditional health system. As per considering e-health, there exist two kinds of health records; Personal Health Records (P-HR) and Electronic Health Records (E-HR) [48]. P-HR provides mobile health services to the patients that are directly operated by them to upload and share the health records. Microsoft is a type of P-HR cloud provider. E-HR is mainly handled by the healthcare providers and it has a great contribution in making decisions on giving proper health services to the patient, storing and secure the sharing of patient's data like medical history, test results, allergies, medicine details and prescriptions [8]. The e-health service involves an improved and well-founded approach of distribution of

medical data over the networks and the usage of such information can be very beneficial for observing the patient's situation and come with an effective and better health service through actual-time health checking and location transparent distribution of health data with the purpose of studying it [9, 10]. The wide use of cloud and sharing of data through the cloud is increasing along with the time and the risk is also rising to that extent as the owner does not ensure direct control on data and the data is accessed by a virtual machine [12, 13].

To get a secure and reliable cloud environment, the data migrated from source to destination must be exact and safe along with resolving the problems of data confidentiality, integrity, availability, network security, and access control [9, 4]. The objective is to minimize the risk as more as possible to keep the patient's data safe and intact and guarantee the correctness of the data while the data is being shared throughout the network.

Leaving the traditional paper-based healthcare system and adapting the digitalized version in a fast way, caused the situation even tougher to manage the data along with the time and handling such a huge and increasing amount of data is not a simple task [15].

Henceforth, the cloud-based e-health system has to meet all the security necessities along with maintaining availability of data anywhere at any time, reliability of the system and the network, authentication of the users and data backgrounds, integrity of the data and confidentiality of the data in the system while transferring the data over network [16].

To achieve security, the three methods used are: one is crypto methods, it consists of symmetric encryption, asymmetric encryption, attribute-based encryption, and hybrid methods. Another one is non-crypto methods which include access control, role-based policy implementation methods for defining the roles of every single user with their right of access [1]. The third one is the biometric-based methods which use biometric traits of a person for user authentication and authorization purpose. The categorization of the security mechanisms is made based on cryptography and biometrics concepts, where cryptography is the concept used for encryption and decryption of data using any encryption technique implying crypto methods and biometric technology uses a person's physical traits for authentication and authorization to system different from cryptographic techniques implying biometric-based methods. The rest security methods which do not use biometric or cryptographic method are included in the non-crypto method.

The significance of our work is to collect as much knowledge as possible on how to maintain the security requirements of the cloud-based e-health systems so that this system will be capable of storing and transferring the patient health data through a public cloud in a safe and secure manner.

Following the introduction, the section-2 shows the methodology used for this research work. Section-3 is used to point out the security requirements of the e-health system. Section-4 shows some legal perspective of protecting the e-health data on the basis of some security laws. Section-5 consists of some existing security mechanisms in e-health and categorized into crypto, non-crypto, and biometrics-based approaches. After this in section-6, the overall discussion is made on the approaches and a table is shown about the methods used for e-health cloud security and their benefits and limitations for each group. Lastly, in section-7 a conclusion is drawn from this whole work. For acronyms, one can use them from the section mentioned before the introduction section.

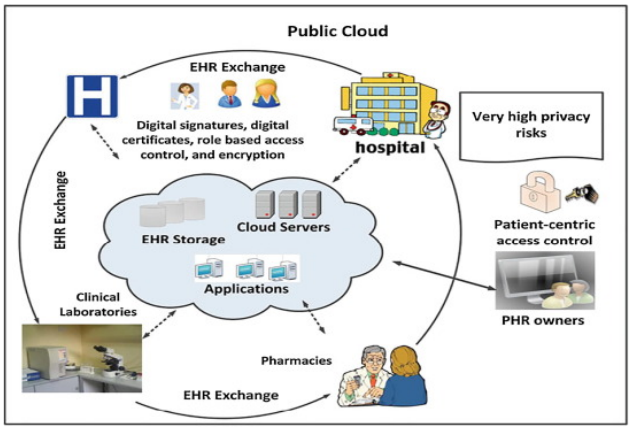

Figure (a). Public e-health cloud system.

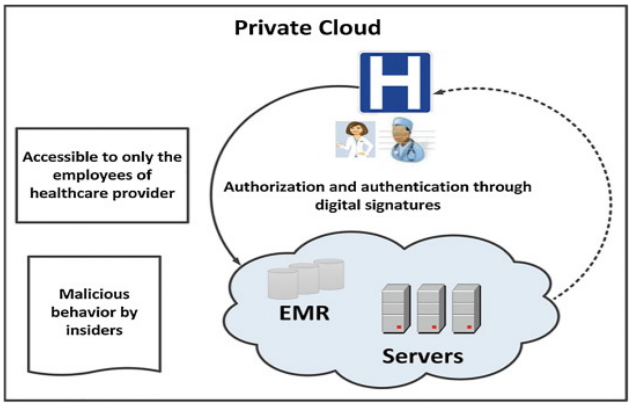

Figure (b). Private e-health cloud system.

2. Research Methodology

A methodical survey always involves thorough and impartial coverage of explored literature. In our literature survey, we have included 85 literatures from various well-recognized journals and conferences. Most of the literature papers are gathered from databases like IEEE Xplore, Science Direct, and Google Scholar. In order to include more information, some open-access journals are

referred on the relevant subject. We gathered the papers by searching the strings:
cloud-based e-health, electronic health security, e-health, e-health security, e-health security law

The review consists of the papers based on maintaining the security criteria of the cloud-based e-health system, what are the security issues and the solutions resolving the issues. The literature used in this review paper is filtered using the following criteria mentioned in table (1) and the number of papers included and excluded from different search engines for the review with respect to the criteria mentioned is given in table (2).

Table (1). Selection and Exclusion criteria to include papers in the review.

Selection criteria	Exclusion criteria
• Directly or indirectly associated with e-health and cloud technology. • Includes cloud computing solutions for various security issues of the e-health system. • Framework designs of Cloud-based e-health. • Privacy and Security mechanisms included electronic health data in the cloud. • Transcribed in English.	• Not related to both cloud technology and e-health. • Not well-known conference papers i.e. not indexed in databases such as IEEE, Scopus, Science Direct, and Cross-Ref. • Papers found not relevant data to any of the terms e-health or cloud or security or combined. • Not written in English.

Table (2). Number of papers included and excluded from different search engines for the review.

Search Engine	Number of papers included	Numbers of papers excluded
IEEE Xplore	44	190
Science Direct	16	347
Google Scholar	91	20009

The 83 papers referenced are from the period of 2010 to 2019 and each of the other 3 papers from 2006, 2007 and 2009, figure (1). No papers are found on the relevant topic in the year 2008.

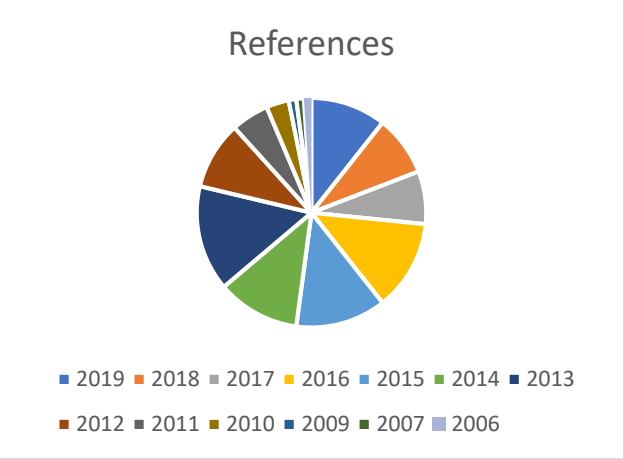

Figure (1). For different years the fractions of references included out of total references.

3. E-health System Security Requirements

The electronic health system is a co-operative computing system that facilitates real-time data flowing via a cloud network which is far better than the classic health system. The e-health system contains different types of sensitive information of the patient which might affect their life directly or put their life at risk. Therefore, to provide good service it is wise to secure the data and transfer it accurately through a fully trusted medium within a certain time to the owner of those data [18]. The actual challenges, in this case, are to manage the security of the location where the data is stored as well as securing the network through which the huge amount of data transmits from source to destination [14].

Many aspects that are to be taken into account for e-health security can be, authentication i.e. checking the validity of the individuals and the data, data confidentiality so that the data will only be accessed by its owner, integrity ensures that the data is safe from any undesirable changes and [16]. It should be taken into consideration that the e-health should be scalable, flexible to any changes and should have a user-friendly interface [18]. The other important feature that could be added is availability of the system whenever and wherever it is needed to process and regulate the patient's data, reliability of the system to avoid any errors while providing services to its users and interoperability where the system should operate according to some standard

communication protocols when communicating between different service providers [14].

To keep both the data and the network fully secured it gets very tricky to manage as the data is transferred to various destinations such as patients, health centres, insurance organizations, and cloud service providers [19]. However, the e-health system has a mechanism to assign different access privileges to different users to access and view the E-HR. As an example, a doctor can view a lot of information about the patient whereas an insurance company can see a limited part of the patient's data. In this manner, it is challenging to handle the verification and validation of diverse users with different access rights [21].

By using cryptography, E-HR files security can be obtained by changing the meaning of original files to an unknown meaning which only can be decrypted by using cryptographic keys of the actual owner. Cryptography can be used to protect the E-HR files while it is stored and also while streaming the data [22].

Many security techniques are used for e-health systems such as secret-key or symmetric key cryptography in which encryption and decryption key are identical, for example, Advanced Encryption Standard (AES), public-key or asymmetric key method uses a couple of different keys for encryption and decryption like RSA (Rivest, Shamir, Adleman) and the attribute-based encryption (ABE) [23] and biometrics which uses the users' traits for authentication.

Although, cryptography is extremely useful in e-health security handling the crypto keys is tough as particular users are assigned with only a particular key and those must be kept secret. For any emergency cases, the system needs to keep the backup of the keys. As the data in the system are sensitive and its exposure might affect people's lives, the data must be maintained correctly also taking the emergency into considerations [20].

4. Legal Perspective Relevant to Cloud-Based E-health

As this paper presents brief knowledge of the security mechanisms used for the cloud-based e-health system, some security laws related to the topic are mentioned in table(3).

Table (3). Security Laws.

Reference	Law	Origin and Time	Description
[87]	Health Insurance Portability and Accountability Act (HIPAA)	United States Congress, 1996	It was introduced by the United States Congress as federal law and used in the US healthcare industry. HIPAA suggested some privacy and security requisites for developing a better e-health system, such as a patient's understanding of the operations performed on his health data, patient allowing access on his data, data confidentiality, data integrity, non-repudiation, auditing, consent exception.
[89]	Federal Privacy Act of 1998	Australia, 1998	It states the principal measures relating to information privacy. But this act lacks in addressing issues such as information ownership, access, and control, data breach warning. Later with a modification data breach warning was made mandatory in this act.
[89]	Personally Controlled Electronic Health Records Act 2012	Australia, 2012	This act was legislated to operate in combination with the Heath Identifiers Act 2010 to address the issues faced in the Federal Privacy Act 1998, by creating an electronic information warehouse of health records arranged by reference to distinct health identifiers assigned to the Australian citizens.
[90]	Article 8 (Data Protection Directive Or Directive 95/46/EC)	European Parliament, 24 Oct 1995	The is no specific category for 'sensitive data' in the law so it is considered under 'special categories of data' under article 8 which includes data associated with health or sex life.
[90]	Article 6 (Directive 95/46/EC)	European Parliament, 24 Oct 1995	The personal data need to be, • Processed impartially and legitimately. • Collected for particular, clear and legitimate motives. • Satisfactory, relevant and not too much concerning the purposes due to which they are gathered and/or further processed.

			• Precise and updated when needed. • Kept in the format permitting the data subject identification until they serve the purpose for which they were assembled.
[90]	Article 16 (Directive 95/46/EC)	European Parliament, 24 Oct 1995	This article deals with data confidentiality by restricting the processing of data if there no instructions from the controller or no requirement by law.
[90]	Article 17 (Directive 95/46/EC)	European Parliament, 24 Oct 1995	This article deals with data integrity and data confidentiality where the data controller (DC) i.e hospital will be held responsible, • To the data subjects for implementing proper technical and organizational precautions ensuring a level of security relevant to the risks associated with the data handling and essence of data. • For confirming that the sub-providers allotted by the cloud-based e-health service do not process personal data without the controller's directions. • For the selection of data processors (DP) providing enough guarantee with respect to organizational and technical security steps associated with data processing.
[91]	Article 2(d) (Directive 95/46/EC)	European Parliament, 24 Oct 1995	It is not always the situation that a single organization having the data controller role and single-handedly authorized to define the processing of data.
[91]	Article 6 (Directive 95/46/EC)	European Parliament, 24 Oct 1995	The DC must make sure that the reason for data processing is legal, not processed for non-specified purposes, the data is thorough and precise and not kept longer than required.
[91]	Article 7 (Directive 95/46/EC)	European Parliament, 24 Oct 1995	The private data may be handled only if one or more predetermined necessities are fulfilled. The member states of EU directives are eligible for deciding the situations and use cases for usage and sharing of an individual's private data with a third party.
[91]	Article 10-14 (Directive 95/46/EC)	European Parliament, 24 Oct 1995	These outline the rights that are retained by the social network service (SNS) users.
[91]	Article 11 (Directive 95/46/EC)	European Parliament, 24 Oct 1995	The patients must be notified about the gathering and processing of their private data involving circumstances such as DC identity, data classifications, data processing purposes.
[91]	Article 12 (Directive 95/46/EC)	European Parliament, 24 Oct 1995	The data subject has the right to know about the processed data, the logic behind processing, and should be eligible to require re-citification, blocking or removal to imprecise and incomplete nature of data.
[91]	Article 18 (Directive 95/46/EC)	European Parliament, 24 Oct 1995	The DC needs to inform the administrative authority about the processing of an individual's data before performing it.
[91]	Section VIII (Directive 95/46/EC)	European Parliament, 24 Oct 1995	The DC and DP should make sure that by planning and executing systematic measures they can maintain satisfactory data security concerning confidentiality, integrity, and accessibility.
[92]	Article 44 (French Project of Law for a Digital Society)	France	This article of French law aims at improving the Internet access service for the disabled.
[92]	Article L311-4 (French Social Action and Families Code)	France	There is a possibility for the collection of the consent of the patient and the aforesaid third after a primary analysis of disease concerning the forward probability of disorders of cerebral functions.
[92]	Article 4 (Directive 95/46/EC)	European Parliament, 24 Oct 1995	This highlights the right to privacy and accommodates an active electronic communication service provider to consider suitable measures for the protection of the security of its services.

[92]	Article 8 (European Charter of Fundamental Rights)	Europe	An individual has the right to protect their data. These data must be processed legally on the basis of the person's consent or on the basis of law.
[92]	Article 5-1-f (Directive 95/46/EC)	European Parliament, 24 Oct 1995	Data must be processed in a way ensuring proper security of private data, protecting the data from unauthorized or illegal access, accidental loss, destruction or damage by utilizing correct technical or organizational measures.
[92]	Article 25 (European Regulation 2016-679)	Europe, 27 Apr 2016	It states that the European or EU Regulation on the safety of regular persons regarding the individual data processing offers a legal foundation for the protection of data by design and by default.
[92]	Article 5-2 (European Regulation 2016-679)	Europe, 27 Apr 2016	EU Regulation enforces heavy legal responsibility on the DC who meant to be in authority for demonstrating agreement with the Regulation basic principles.
[92]	Article 35-7-c (European Regulation 2016-679)	Europe, 27 Apr 2016	When the technology is expected to give a high risk to the privileges and liberties of regular persons, the DC should activate an influence valuation before processing, including the risks to the privileges and liberties of data subjects.
[92]	Article 83-5 (European Regulation 2016-679)	Europe, 27 Apr 2016	Data defense authorities have the power to enact administrative penalties up to € 20,000,000 or 4% of global gross revenue for data protection breach principles.
[92]	Article 83-4 (European Regulation 2016-679)	Europe, 27 Apr 2016	Data protection by design and by default, security, and privacy influence valuation breaches are also bound by penalties up to €10,000,000 or 2% of global gross revenue.
[93]	Article 2(d) (Directive 95/46/EC)	European Parliament, 24 Oct 1995	The DC is an entity determining the need for dealing out private data. The DP is an entity dealing with private data on behalf of DC.
[93]	Article 17 (Directive 95/46/EC)	European Parliament, 24 Oct 1995	The DP is answerable to an investigation by DC.

5. Existing Security Mechanisms used in e-health

As per the requirements of the security of E-HRs, it is necessary to discuss the existing security techniques that are used in achieving e-health cloud security. The three types of techniques used are; crypto techniques, non-crypto techniques, and biometric-based techniques.

5.1. Crypto Techniques

Cryptography is defined as a technique of altering a meaningful data to a pointless format by using a key and recovering the original format also by using a key. Several techniques use many ways to encrypt and decrypt the data for instance; asymmetric, symmetric and attribute-based encryption. It facilitates data confidentiality, user and data authentication, user authorization and non-repudiation [24]. Although each of these methods has their different attributes and uses many techniques to achieve data security, those techniques and their usage in the research area of e-health are expressed below.

First of all, the symmetric key or secret-key encryption uses the identical secret key for both encryption and decryption of the data. There are some specific perquisites like policy enforcement, assigning role and access privileges to each user and management of keys where the particularly authorized persons are provided with the keys and access rights, all of these should be met while using the secret-key encryption algorithm [16]. In e-health, the most popular secret-key algorithm is the Advanced Encryption Standard (AES) [1, 27]. According to NIST, AES is considered the fast and secure symmetric algorithm for e-health [28]. In [29], authors proposed an idea of using a selective encryption process utilizing the AES technique in which different keys are used to partially encrypt the file and each user according to their role is provided with different keys by the file owner. The authors of [30] have also suggested using a selective AES which is the improved version and better than original AES in terms of security as well as speed. Here, the suggestion says that before the encryption using AES the data is compressed and the key size is set by the user's

choice which varies within (128,192,256). David et al. recommended the usage AES with big data in e-health application by using a customized AES in DaaS, one of the cloud services, which makes it faster and more effective ever when used with big data [31]. Using secret-key key encryption is much effective for protection of the e-health data, however, to satisfy the requirements for the e-health role-based decryption there will be a need for customization to have selective encryption or the use of a mechanism to control the access with it [1].

Next, the asymmetric key encryption or public-key encryption algorithms use a couple of keys where the key known as a public key is utilized for encryption and the other key is utilized for decryption known as the private key. The most popular among this encryption technique used in e-health are RSA and Elliptic Curve Cryptography (ECC) [20]. One of the security techniques using RSA includes dividing users into varying modules like admin, patient, doctor, and hospital and then to achieve fine-grained file encryption, particular data related to each user of that module are encrypted using RSA [32]. According to [33], using RSA in the medical database the encrypted files are stored in a multilevel database along with the private key. In this concept, as per the user's level in the database, each user has access to his profile where he can get the private key and decrypt the files. Dhanabagyam et al. mentioned that another asymmetric encryption algorithm, ECC has a computational improvement than other linear algorithms because of which ECC was taken into consideration for securing the e-health system [34]. In [35], the authors used ECC techniques for the concerned system and compared its performance with RSA and the study implied that ECC has faster performance because it uses a smaller size key than RSA and maintains an appropriately good security level. So in [36], ECC was used with an integration unit that is dedicated to the encryption and decryption of data. That integration unit consists of a chip to identify the users and a smart card reader, USB (Universal Serial Bus) controller and wireless transmitter where the USB is linked to a wireless device by using a USB protocol that transfers utilizing the wireless transmitter, architecture is shown in figure (2). Liu et al. [50] used an identity-based encryption system (IBE) for the access control of P-HR, the use of this mechanism is able to reduce key management complexity and also able to resist external attack, equation attack, reverse attack in the cloud computing background. In [77], the authors described an advanced IBE and advanced Identity-based proxy re-encryption (IBPRE) schemes to be used in e-health systems, proved their security, analyzed their performance which resulted that the IBE is IND-sID-CPA (indistinguishability under identity-based chosen-plaintext attack) secure, IBPRE is IND-ID-CCA2 (indistinguishability under identity-based chosen-ciphertext attack 2) secure. They also expressed that the IBPRE scheme is better in performing re-encryption which leads to the protection of e-health data and cost-effective for cloud-based e-health users.

The third type of crypto technique is the attribute-based encryption (ABE) in which the data gets encrypted based on a particular attribute that must be matched the users for the decryption of files. ABE is an addition to the public key cryptography that have two methods; one is ciphertext policy ABE (CP-ABE) where every ciphertext is bounded with the strategy that deciphers it and another one is key policy ABE (KP-ABE)in which the association between the key and the ciphertext is reversed [37, 38].

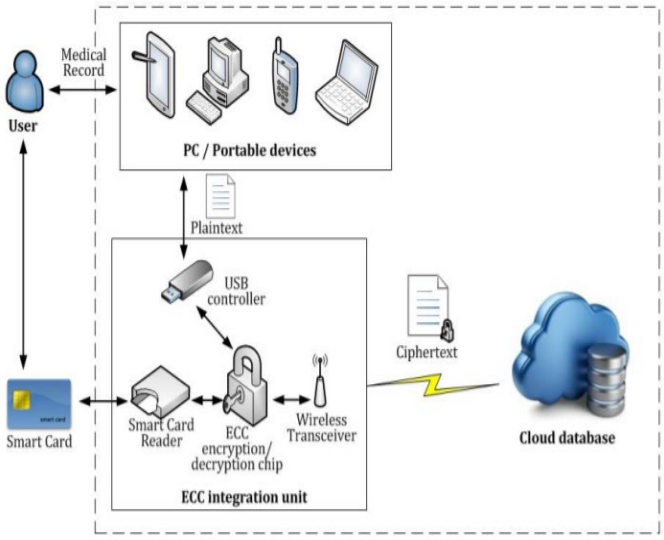

Figure (2). An ECC based e-health system architecture [36].

Due to these reasons, ABE is used in e-health systems so that it can provide fine-grained access control and role-based decryption of publicly shared files which implies that even though a person has access to a particular data only the authorized user who fulfils the required set of traits for constructing the key will be capable of decrypting and reading the files. These characteristics make it appropriate for e-health requirements [39]. In addition to this, the authors of [41] used CP-ABE as the encryption mechanism and solved the problem of reconstruction of keys due to any policy change by relating a proxy re-encryption method with one time pad pin (OTP), so that it can be more secure and will be accessed by only the authorized personnel. In [38], the authors have created a software library that has both CP-ABE and KP-ABE and built a policy generator that is used for generating ABE policies utilizing which the encryption key can be created and data can be encrypted. In [40], the authors have utilized multi-authority ABE (MAABE) where ABE is implemented with the division of users into domains, each domain having similar privileges that lead to reduce the difficulty with the key management. In [70], the authors used a fine-grained and enhanced MA-ABE (eMA-ABE) for the secure data sharing of P-HRs. this model ensures data confidentiality and user revocation on demand.

Lastly, from the previously mentioned algorithms, the combination of different types can be used in a hybrid

environment. These types of hybrid systems get benefitted by more than one encryption technique, e.g. proxy re-encryption with asymmetric key encryption method. One type of fusion cryptography includes RSA and AES; RSA is used for creating a digital signature that provides user authentication and AES used for data encryption which ensures data integrity as well as security [43]. In [60], Percarina et al. presented an architecture known as SAPPHIRE to maintain the privacy of users by providing anonymity and enhancing the policy administration for the primary data owner. It is a hybrid of RSA and AES.

For providing a secure environment for storage of E-HRs authors of [69] proposed a hybrid technique composed of a symmetric block cipher algorithm, Blowfish to encrypt the data and RSA to encrypt the keys. This mechanism uses an enhanced version of RSA (eRSA) which has better speed than the original RSA. This hybrid method provides better security than any single encryption method.

Another usage of the hybrid system includes using ABE combined with image steganography to insert an encrypted prescription and transmit from the physician to the druggist [27]. Another hybrid technique has AES and ABE used together in e-health, where AES is used for encrypting the files and uploading it to the e-health cloud and ABE i.e. KP-ABE is used for providing the users access privileges related to their attributes [42]. In [63], the authors proposed a hybrid model using the combination of AES and MA-ABE to provide enhanced security, privacy and access control services to the existing e-health system. It also enhances the scalability of the system and protects the system from attacks like Man-in-the-Middle (MITM) attack, eavesdropping, and Denial-of-service (DOS) attack. The security mechanism used in [64], is ABE with a binary search tree method. Using the effectiveness of CP-ABE this technique ensures that the privacy and security of E-HRs are properly maintained even during data sharing and fuzzy keyword searches. In [51], the proposed framework uses a combined mechanism of IBE and ABE which provides security through data privacy, fine-grained access control, and prevention of inappropriate access of E-HR by the users with numerous roles. In [52], the combination of IBE and ABE decreases the overhead occurs due to management as well as the encryption-decryption time. This mechanism uses AES to encrypt the data files and ABE to encrypt the AES key. By using IBE, ABE and threshold signing the proposed model in [53] provide access control and auditability of the authorized users. The authors of [57] provided an improvement of an existing secure index search (SIS) algorithm to increase the proficiency of information control and flow in an E-HR cloud using a key management scheme. Both in [71], [72] the authors proposed models for mobile health application using ABE and IBE schemes, those are, IBBE and CP-ABPRE (cipher-text policy attribute-based proxy re-encryption). The patient's data can be shared between patients and medicals securely and patients can discover other persons suffering from similar health conditions using a private data –matching method and ensure to keep the privacy and integrity of data intact. Patients' can choose their doctors, encrypt and upload data and the authorized doctors decrypt it. CP-ABPRE provides fine-grained access control. Doctors have to generate only the re-encryption key and the re-encryption is accomplished by a proxy. In [61], the authors proposed a mobile solution for e-health using IBE to protect the credentials of the client, homo-morphic encryption (HE) of medical archives and proxy re-encryption (PE) for protecting the privacy of each entity in e-health. In [65], the authors suggested a hybrid system of MA-ABE and KP-ABE i.e., Hybrid Secure and Scalable Electronic Health Record Sharing (HSS-EHRS) system, which is further divided into two security domains, known as, Public domain (PuD), where the professionals of healthcare can access the E-HRs whereas Personal domain (PsD) is for the persons who are related to the patient. MA-ABE is used for multiple attribute authorities in PuD who can provide secret keys to the PuD users and KP-ABE is specifically used for encryption and management of the secret keys for PsD.

Among other type of hybrid system, one is an hybrid mechanism proposed the authors of [48], to deal with the problem of link-ability, where it is the situation when the trusted cloud provider (CP) tries to access and look into the patient's health records hampering the privacy of patient's data and able to track a patient and identify him, CP is able to do so as he has the responsibility of indexing the medical images and logging the uploads made by healthcare provider hospital and consumer hospital. So this approach considers a trusted third-party as the medium for secure communication and the correct policy is applied to the data by policy encryption point (PEP), and then transferred to the watermarking and encryption point (WEP) where it marks the image, then encrypt and handovers the image to the randomization point (RP). RP is responsible for computing random image index and cache time which makes it difficult for CP to know about the correct order of data received from the provider hospital. When the consumer hospital wants the data it enquires the third-party for the medical image index, then the PEP ensures the access rights of the consumer party to that data, sends indexes and an access ticket for data at the CP. To get access to the right medical image the consumer hospital executes oblivious transfer protocol. In [62], Haas et al. proposed a public cloud solution to prevent link-ability in which before sending a record to public CP it is made anonymous using a component called data pseudo-anonymity service. This service consists of PEP and a local cache that randomizes the order of transfer of the record to CP.

Overall, the use of the hybrid system is quite advantageous as it gets profits from the features of more than one set of rules where those features can be extended security, fast computing with a lesser amount of overhead, use of digital signature, provision of access rights [1].

5.2. Non-Crypto Techniques

As already explained, cryptography has a great impact on the security of the e-health system. However, there also exist some methods other than cryptographic methods which can also provide security. But, these are not commonly used as it gives partial security to e-health cloud which is less than the security provided by crypto methods. Thus these systems are used with crypto approaches in a hybrid system, some those are pointed out below.

One of these approaches is a prototype of authentication and access control manager (AAM) where the users use tokens to access their records warehoused in the cloud, then the server identifies the users and determines their access privileges through AAM server. This model relies on the cloud in case of complex computations [21]. In another approach, several facilities are provided to the users like accessing, sharing and management of files by putting a central authority (CA) where the individuals are divided into security classes like; patients, doctors, nurses, family, and insurance companies. In order to achieve user access rights and user authentication, the security classes here give different access privileges to each user and this model is responsible for encryption key distribution [44]. The authors of [45] used a combination for an extensible mark-up language (XML) and attribute-based access control (ABAC), which is extensible access control mark-up language (XACML), to get advantages like role-based access control (RBAC) and policy implementation along with e-health data representation by XML. In [46], Shuo et al. proposed a two-level access control mechanism which includes role-based access control in the first layer with an enhanced RBAC in the second layer, due to the weak features of RBAC. The second tier is time-centred which stores the patient's meeting time, unique for each person; so, the RBAC determines who can see the requested service whereas the extended RBAC regulates the value for each one. A cloud-based privacy-aware role-based access control model was proposed by the authors of [54], which can be utilized for controlling and tracking the data and the authorized accesses to the healthcare system resources. Another noticeable work is by the authors of [47] who presented a fresh technique as certificate-based encryption with keyword search (CBEKS). This technique is performed by using an asymmetric encryption technique. To set the correct access rights, the data receiver has to send a keyword that describes the desired data file and then a certificate, which expresses the access rights, provided to that receiver. In [84], dynamic searchable encryption with keyword range search and multi-keyword search (DSEKRSMS) using a privacy-preserving equality test (PET) was used to give a searchable and privacy-preserving approach for data sharing in cloud-based e-health systems.

A combined blockchain model of the fully private blockchain (FPB) and consortium blockchain (CB) was proposed to upgrade the time taken for data validation. Here, FPB is used as the classical database for the healthcare institute and CB is used for storing the medical data from all participating medicals. It provides tamper-resistant and reliable storage [68]. In [56], the Watermarking approach used can mitigate insider threats to the e-health system. Chenthara et al. [78] considered a patient-oriented e-health system model i.e. personally controlled E-HR system using blockchain technology where blockchain can be used for verifying the ownership of the patient's data, giving access permissions and ensuring the data integrity. In [81], to satisfy the criteria of distribution architecture a protocol named pseudonym-based encryption and different authorities (PBEDA) was proposed along with multi-tier blockchain technology in an e-health system. In [82], blockchain is used to protect the outsourced E-HRs from the illegal alteration as every operation on the outsourcing E-HRs is summed up to a transaction. Nguyen et al. [85] proposed an approach using blockchain and peer-to-peer inter-planetary file system (IPFS) storage which provides an efficient access control scheme for secure and decentralized data storage and sharing, shown in figure (3).

To secure the e-health information system (E-HIS) the authors of [49] proposed a framework which consists of the entities, to generate and manage the e-health information are; patients (1P): the healthcare receivers, provider (2P): the health service providers, payer (3P): the insurance companies, national database (ND): cloud used to store data and certificate authority (CrA): a third-party who certifies the 3P's legitimacy in the E-HIS framework.

The authors of [55] proposed a dynamic access control mechanism implemented with the e-health cloud known as risk aware task-based control which ensures that the access is granted based on the AIC (Availability, Integrity, Confidentiality) principle. Lohr et al. [19] proposed an approach provides client platform security using trusted virtual domains (TVD). In [58], the authors used a secret sharing scheme to maintain privacy and high security in the e-health cloud. In [67], a secure and simple framework was proposed in which the e-health data is portioned into multiple segments, each of those segments are enciphered by a secret key method and then stored in a permuted manner by anther CP. The order of data and decryption process is known to the user. This approach can adapt any type of security measure implemented by CP and along with that the framework still manages the secrecy and security of data.

In [66], the authors offered a framework to deliver security to IoT healthcare wearable devices along with Integrated Circuit Metric (ICMetric). Here, the sensor of the wearable uses MEMS (Micro-Electro-Mechanical Systems) bias and creates device ICMetric. This model provides security services like privacy, confidentiality, availability, the authenticity of the user's device, data integrity, secure access control, protection from attacks like device-capture attack, brute force attack, dictionary attacks, and rainbow table attacks.

In [87], an architecture is presented using Mandatory Access Control Security Model (MACSM) and Access

Control List Security Model (ACLSM). It is estimated to provide high reliability, efficiency and dependability to protect the patient's information.

Patra et al. proposed a security architecture for the e-health system to avoid the problems related to the central web-based system i.e, link failure and low or no fault tolerance. So, they presented a decentralized e-health system named iMedikD which facilitates both local and centralized access [88].

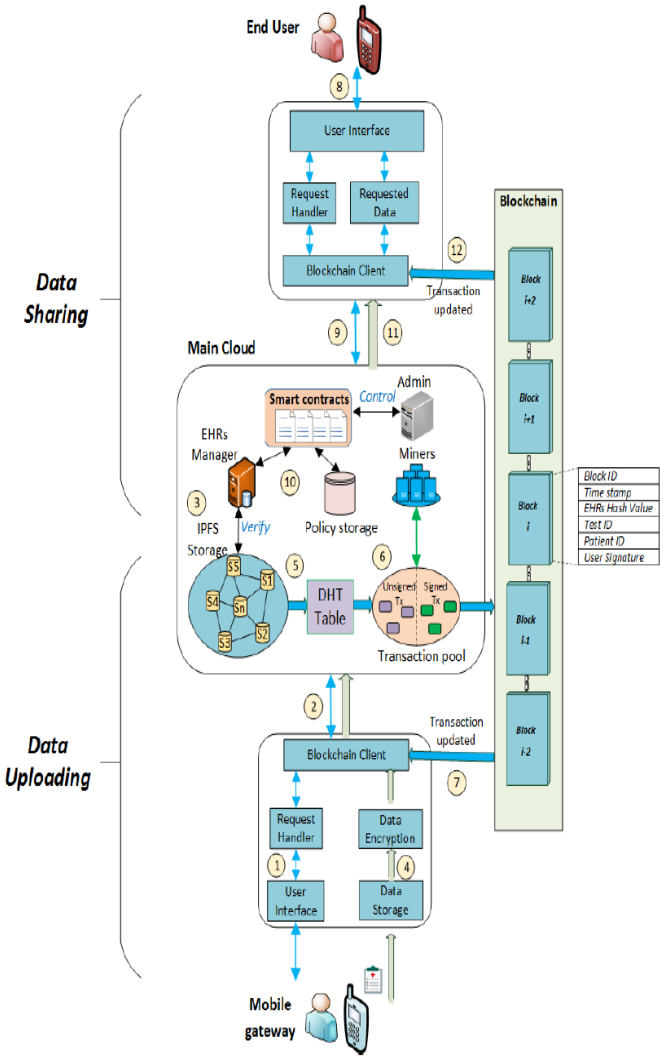

Figure (3). Multi-tier blockchain framework [85].

To preserve privacy in public e-health cloud, Zhang and Liu in [59] introduced a reference model that depends on group signatures to guarantee the unlink-ability of health data to a particular doctor. The authors also proposed that the health record indexes of patients must not reveal their information and should facilitate an effective search. Wang et al. [79] proposed a secure scheme for data sharing by maintaining the anonymity and confidentiality of data while sharing it through public clouds using a bilinear pairing mechanism that provides speed and efficiency along with low expansion rate. Shen et al. [83] proposed an e-health monitoring system using geo-distributed clouds (GDC) and a traffic shaping algorithm (TSA) which together helps in minimizing the service delay and preserving the privacy of health data.

5.3. Biometric-based Techniques

Nowadays biometric is adapted by most institutions as it provides a unique identity for each person. Biometric mechanisms provide facilities like user identification and user authentication [73]. One of the approaches for the security of e-health using biometric utilizes Minutiae map algorithm authentication of the user concerning his fingerprint biometrics, as it is shown to be the more secure one and needs less time for feature extraction of fingerprint than Gabor feature, orientation maps, and orientation co-linearity algorithms. For the storage services, the approach proposed splits the files of the user and then stores them in two cloud storage, Cloud Me and Dropbox. For encryption of the files, the RC4 algorithm is used. Some of the prevention techniques for Cross-site request forgery (CSRF) and Cross-site scripting (XSS) attacks considered are the use of web-application firewalls, protection of cookie details and checking of the validation of user input [74]. The proposed biometric-based architecture of paper [74] is shown in figure (4). The biometric methodology used by the authors of [75] provides security to the e-health data, easy and secure data access and sharing, either by using a given unique identification number or thumb impression of the patient. In [76], the authors provided a framework for security of health monitoring application using biosensor data of the patient where it provides secured access to the data and self-protects the data, for all the times while the data is stored and shared through the cloud. Ibrahim et al. [80] proposed a robust and secure multi-factor remote user protocol that can assure secure communication between patient and doctor even through a public-insecure channel. To protect the user identity the mechanism uses a combination of passwords, smart devices, and biometric authentication.

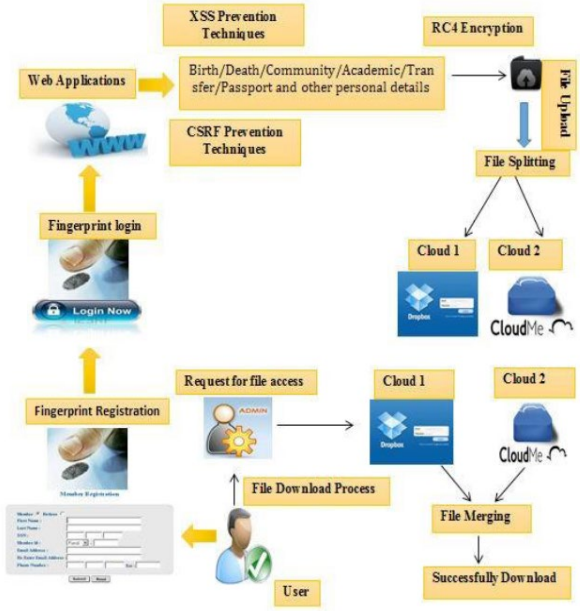

Figure (4). Biometric-based proposed architecture [74].

6. Discussion

Several security mechanisms used for cloud-based e-health system security are already explored in this paper; in this section, we are going to mention some advantages and limitations of the mechanisms mentioned above and those limitations can be taken into consideration for future researches. To keep the e-health data free from unwanted exposure as it could disturb the patient's life directly, some features to be taken into consideration are real-time data access, availability of data, and transfer of data from source to endpoint in an unaffected and correct manner. The cryptographic cloud serves well according to these criteria. But there are some of the problems which are pointed out on crypto techniques used in e-health.

At first, the symmetric encryption is secure and fast and is very much capable of giving proper security. But the problem with this encryption method is that it does not provide role-based access privileges, because of which an extra method for controlling the data access of users or two-step encryption causing overhead, can be used with it. A solution to this problem can be either to customize this technique to meet the e-health requirement or increase its computation speed. The public-key encryption has the same difficulty as secret-key encryption. However, it is able to be utilized as a digital signature solution as well as for sharing keys among multi-users. Even if the ABE system has the facility of giving role-based privileges, the main problem arises once a user is withdrawn from the e-health system due to which the whole access policies in the system must be modified. Non-crypto methods do not use cryptographic methods and are faster. Biometric methods are good in user authentication and authorization using physical traits.

Overall, crypto methods are slower than non-crypto methods even if earlier one is more secure than later. It is more preferred to use non-crypto methods than crypto methods if used individually. As a solution to this problem, a hybrid system using any of crypto, non-crypto, and biometric-based approach can be used for providing a desirable security system.

According to our opinion with respect to the papers referenced, the ideal methods for securing the cloud-based e-health system could be, an advanced AES having different types of users with multiple access privileges and low overhead, ABE with an efficient user revocation method, RSA with proper access control and modified application of Biometric compatible with mobile devices, hybrid of any non-crypto methods and biometric-based method, blockchain-oriented methods.

After all the findings for cloud-based e-health system security we would like to recommend to consider the papers ([68], [78], [81], [82], [85]) on blockchain-based mechanism as it is more trending in recent days, the papers ([74], [75], [76], [80]) on biometric-based mechanism for mobile devices. If anyone considering cryptographic methods for securing cloud-based e-health system then they should consider the papers ([27], [30], [31], [42], [43], [63], [64] for AES based), ([43], [64], [69] for RSA based) and ([38], [42], [51], [53], [63], [65] for ABE based) hybrid system.

Along with all these, the advantages and limitations of some security mechanisms are shown in the table (4.a), table (4.b) and table (4.c) for crypto, non-crypto and biometric-based security mechanisms respectively. Some of the open problems in e-health security which can be taken into account while developing a security system are user revocation with updating access policy of the e-health system, efficient key distribution, and management in emergencies. Further researches for the e-health cloud can be done in these fields in the future.

This study is different from other review papers related to the secure cloud-based e-health system because we have considered all possible relevant literature. The security mechanisms are divided into 3 categories by considering a new part as biometric-based along with the previously known cryptographic and non-cryptographic mechanisms.

7. Conclusion

In this paper, 94 relevant research papers are surveyed for the safekeeping of cloud-based e-health systems from various sources till 2019. The various security techniques are summarized that are used in cloud-based e-health systems to achieve security when storing and sharing the e-health record on the cloud. These techniques are crypto methods, non-crypto methods, and biometric methods. Some hybrid systems with the features of more than one technique are also considered. A brief review of the advantages and limitations are provided for some of the security techniques used. The limitations can be

considered as existing open problems on the techniques in the tables and can be used for future studies for providing an improved security facility than the previous version of the technique. Along with these, some mechanisms are recommended such as Blockchain, Biometrics-based mechanisms, ABE, AES, RSA and a list of reference papers to be helpful for other researchers in developing security standards for the e-health system used in the cloud.

In this research paper, six papers are related to e-health cloud security laws. However, in this paper, there is only one research paper which includes both security mechanism and security laws.

Our future research scope includes implementation of a hybrid model using blockchain, biometrics-based security mechanism and if needed using any of the cryptographic security mechanisms and involving security laws in the model for making the security of the cloud-based e-health system better.

Table (4.a). The advantages and limitations of the crypto security mechanisms.

Reference	Security mechanism	Advantages	Limitations
[29]	AES	Role-oriented distribution of keys with high security	Growth in the number of keys and key management difficulty
[30]	AES	Role-based encipherment with better security and speed	Before encryption data compression is necessary
[31]	AES-DaaS	Better than MS default encryption, efficient and faster	Scalability is limited due to the use of big data
[32]	RSA	Fine-grained file encryption	Management of access model is required
[33]	RSA	Security improvement	Multiple level access control is required
[35]	ECC	Smaller key size and faster performance as compared to RSA	Access privileges not present
[36]	ECC	Private key distribution in relation to access privileges	An integration unit is a must
[40]	MAABE	Fine-grained accessing within a lesser amount of time and a lesser amount of complexity	The server is responsible for securing the files and secret keys
[41]	CP-ABE	Users are revoked and keys are updated efficiently	Use of re-encryption creates an overhead
[77]	IBE, IBPRE	IBE is IND-sID-CPA secure IBPRE is IND-ID-CCA2 secure IBPRE achieves master secret security IBPRE is cost-effective IBPRE is better for re-encryption	IBE is not CCA-secure
[38]	CP-ABE + KP-ABE	Policy-based encipherment	The policy engine is needed
[65]	MA-ABE + KP-ABE	Eliminates user revocation problem, Increases scalability, provides fine-grained access regulation, confidentiality towards the E-HRs, Key generation and revocation, Encryption-decryption period and cost of production are linear to the magnitude of attributes	-
[27]	AES + steganography	Provides high security	Causes computational overhead
[42]	AES + KP-ABE	Provides access privileges and better security	Difficult to modify the access privileges
[43]	RSA + AES	Offers user authentication with more security	Problem in scalability
[63]	AES + MA-ABE	Provides enhanced security, privacy and access control Scalability of the system is enhanced	-

		Protects from MITM attack, eavesdropping, DOS attack	
[51]	IBE + ABE	Offers data privacy, fine-grained access regulation, stoppage of incorrect access to E-HRs by multi-role users	Does not have a grant for write privileges to the entities and have no provisions for updating of files and keys
[53]	IBE + ABE	Provides access control and auditability for the authorized users	No provision for identifying possible sources of data leakage and illegal distribution of E-HRs
[57]	SIS + key management	Provides reliability, flexibility, quick access to health records, enhancement of efficiency and security without any need of third-party	Absence of access control model for E-HRs
[64]	SAPPHIRE (AES + RSA)	Offers auditing, anonymity provision, access revocation and access control by data owner only, local policy administration, emergency access	Absence of a collaborative toolkit, no confidential auditing and usage control
[69]	Blowfish + eRSA	Provides better security than any single encryption technique Fast encryption and decryption than AES and Blowfish Generates large prime numbers for the generation of keys and manages the keys efficiently	-
[61]	IBE + HE + PE	Provides identity protection of users, proper encryption of records, protection of privacy	Cannot completely avoid timing attacks, the link-ability problem not solved
[48]	PEP + WEP + RP	Link-ability problem is solved	Use of OT creates overhead, management of third-party and security of RP is crucial

Table (4.b). The advantages and limitations of the non-crypto security mechanisms.

Reference	Security mechanism	Advantages	Limitations
[21]	AAM	Takes a lesser amount of online time of the user	All computations are performed on a semi-trusted cloud server
[44]	CA	User access rights and authentication is ensured	Central authority management is a must
[45]	XML-ABAC	Provides an attribute-centered access regulation	An increase in security is needed
[46]	RBAC	Improved role-based access regulation	Computational overhead
[47]	CBEKS	Sets right access privileges to the users	Use of public-key encryption causes an overhead
[19]	TVD	Offers platform security for the clients	Patient's absence, patient unable to authenticate himself, unable to keep the existence of the patient's health records confidential, could not maintain the anonymity of the client, unable to maintain non-repudiation of emergency cases
[68]	Blockchain	Provides a tamper-proof and reliable	Need for updating the proposed

		storage Reduces data validation time	technology in e-health according to the advanced technologies Cost of deployment of the model
[78]	Blockchain	Tamperproof approach Ensure integrity, privacy, availability, confidentiality, and security	No detailed practical information provided
[81]	Multi-tier Blockchain + PBEDA	Anonymously accessing, checking and updating of sensitive data of E-HRs by patients	Not specific about each blockchain layer in e-health platform for IoT security solutions meant for some vulnerabilities
[82]	Blockchain	Method is tamperproof No need for a central authority Using a transaction user can check the integrity Provides strong security with high efficiency	More research on blockchain technology needed to improve the security
[85]	Blockchain + IPFS	Highly flexible and reliable High availability of medical data in the cloud No single point of failure Maintains data integrity and privacy	-
[56]	Watermarking	Able to mitigate the insider threats of the system	Unable to assess the resilience of watermark against a modification or removal attack, The method proposed cannot mitigate the risk of an insider attack on an original un-watermarked health record
[49]	3Ps + ND + CA	Security achieved along with user authentication	Theoretical approach, not a practical one
[66]	ICMetric	Provides data confidentiality, integrity, availability, privacy, authentication of user's device, secure access control Able to protect from attacks like a dictionary attack, rainbow-table attack, brute-force attack, device-capture attack.	It is only a theoretical approach, no practical
[63]	Group signatures	Maintain anonymity of signer	No practical solution for the efficient searching, link-ability problem not solved
[79]	Bilinear pairing	Fast and efficient Low expansion rate	-
[83]	GDC + TSA	Service delay minimization Privacy preservation Capable of reducing traffic analysis attacks	Not suitable for more complicated circumstances dealing with different requirements for privacy preservation and arbitrary medical requests
[86]	MACSM + ACLSM	Offers high dependability, effectiveness, trustworthiness Gives flexible authentication to patient's e-health data Information controlled by stakeholders and provides mechanisms for critical and difficult circumstances.	Architecture is not implemented, only a theoretical approach.
[88]	iMedikD architecture	Enhanced system performance Reduced operational errors System and data security are enhanced	Not resolved the problem of making the system fail-safe Data pushing technique, required for false download elimination, is not incorporated

Table (4.c). The advantages and limitations of the biometric-based security mechanisms.

Reference	Security mechanism	Advantages	Limitations
[74]	Biometric (Fingerprint)	Provides user identification and authentication, secure data access and storage Prevents from CRSF and XSS attacks	May be prone to other security threats and attacks Not compatible with mobile devices
[75]	Biometric (Thumb impression)	Ensures data security, easy and secure accessing of data and data sharing	Not compatible with mobile devices
[76]	Biometric (Fingerprint)	Provides self-preservation of data and secured access to data	No practical implementation has done yet
[80]	Biometrics + Password	Privacy level increased Communication cost minimized	-

('-' sign denotes no limitations found yet)

References

[1] Kamoona, M. A., & Altamimi, A. M. (2018, July). Cloud E-health Systems: A Survay on Security Challenges and Solutions. In *proceedings of 2018 8th International Conference on Computer Science and Information Technology (CSIT),* (IEEE) :pp. 189-194.

[2] Selvam, S., & Kannan, S. T. (2015). Analysis of the major issues in Cloud Computing Environments. *IARS' International Research Journal* **5**(2).

[3] Balasooriya, P. N., Wibowo, S., & Wells, M. (2016). Green cloud computing and economics of the cloud: Moving towards sustainable future. *GSTF Journal on Computing (JoC)* **5**(1): 15.

[4] Chowdhury, R. R., Mahato, S., Agrawal, S., & Mishra, R. G. (2015). Cloud Computing: A Review of Security Related Issues. *In Book Chapter of Cloud Computing: Reviews, Surveys, Tools, Techniques and Applications-An Open-Access eBook published by HCTL Open*.

[5] Apostu, A., Puican, F., Ularu, G. E. A. N. I. N. A., Suciu, G., & Todoran, G. (2013). Study on advantages and disadvantages of Cloud Computing–the advantages of Telemetry Applications in the Cloud. *Recent Advances in Applied Computer Science and Digital Services* :2103.

[6] Adler-Milstein, J., DesRoches, C. M., Kralovec, P., Foster, G., Worzala, C., Charles, D., Jha, A. K. et al. (2015). Electronic health record adoption in US hospitals: progress continues, but challenges persist. *Health affairs*, *34*(12), 2174-2180.

[7] Xue, C. T. S., & Xin, F. T. W. (2016). Benefits and challenges of the adoption of cloud computing in business. *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*, *6*(6).

[8] Cyganek, B., Graña, M., Krawczyk, B., Kasprzak, A., Porwik, P., Walkowiak, K., & Woźniak, M. (2016). A survey of big data issues in electronic health record analysis. *Applied Artificial Intelligence* **30**(6): 497-520.

[9] De Moor, G., Sundgren, M., Kalra, D., Schmidt, A., Dugas, M., Claerhout, B., Karakoyun, T., Kush, R. et al. (2015). Using electronic health records for clinical research: the case of the EHR4CR project. *Journal of biomedical informatics* **53**: 162-173.

[10] Hanauer, D. A., Mei, Q., Law, J., Khanna, R., & Zheng, K. (2015). Supporting information retrieval from electronic health records: A report of University of Michigan's nine-year experience in developing and using the Electronic Medical Record Search Engine (EMERSE). *Journal of biomedical informatics* **55**: 290-300.

[11] Silva, B. M., Rodrigues, J. J., de la Torre Díez, I., López-Coronado, M., & Saleem, K. (2015). Mobile-health: A review of current state in 2015. *Journal of biomedical informatics* **56**: 265-272.

[12] Shahzad, F. (2014). State-of-the-art survey on cloud computing security Challenges,

approaches and solutions. *Procedia Computer Science* **37**: 357-362.

[13] Bhadauria, R., Chaki, R., Chaki, N., Sanyal, S. (2014). Security issues in cloud computing. *Acta Technica Corvininesis-Bulletin of Engineering* **7**(4): 159.

[14] Asija, R., & Nallusamy, R. (2014, July). A Survey on Security and Privacy of Healthcare Data.

[15] Ahuja, S. P., Mani, S., & Zambrano, J. (2012). A survey of the state of cloud computing in healthcare. *Network and Communication Technologies* **1**(2): 12.

[16] Sumathi, R., & Kirubakaran, E. (2013). SCEHSS: Secured Cloud Based Electronic Health Record Storage System with Re-Encryption at Cloud Service Provider. *International Journal of Computer and Communication Engineering* **2**(2): 162.

[17] Wang, X., Bai, L., Yang, Q., Wang, L., & Jiang, F. (2019). A dual privacy-preservation scheme for cloud-based eHealth systems. *Journal of Information Security and Applications* ***47*:** 132-138.

[18] AbuKhousa, E., Mohamed, N., & Al-Jaroodi, J. (2012). e-Health cloud: opportunities and challenges. *Future internet* **4**(3): 621-645.

[19] Löhr, H., Sadeghi, A. R., & Winandy, M. (2010, November). Securing the e-health cloud. In *Proceedings of the 1st acm international health informatics symposium* (ACM), pp. 220-229

[20] Abbas, A., & Khan, S. U. (2014). A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. *IEEE Journal of Biomedical and Health Informatics*, *18*(4), 1431-1441.

[21] Kahani, N., Elgazzar, K., & Cordy, J. R. (2016, April). Authentication and access control in e-health systems in the cloud. In *proceedings of 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)* (IEEE), pp. 13-23.

[22] Sahama, T., Simpson, L., & Lane, B. (2013, October). Security and Privacy in eHealth: Is it possible?. In *proceedings of 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)* (IEEE), pp. 249-253.

[23] Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of biomedical informatics* **46**(3): 541-562.

[24] Rezaeibagha, F., Win, K. T., & Susilo, W. (2015). A systematic literature review on security and privacy of electronic health record systems: technical perspectives. *Health Information Management Journal* **44**(3): 23-38.

[25] Meingast, M., Roosta, T., & Sastry, S. (2006, August). Security and privacy issues with health care information technology. In *proceedings of 2006 International Conference of the IEEE Engineering in Medicine and Biology Society* (IEEE), pp. 5453-5458.

[26] Hu, Y., & Bai, G. (2014). A systematic literature review of cloud computing in eHealth. *arXiv preprint arXiv:1412.2494. Health Informatics-An International Journal (HIIJ)* **3**(4): 11-20.

[27] Omotosho, A., Adegbola, O., Mikail, O. O., & Emuoyibofarhe, J. (2015). A secure electronic prescription system using steganography with encryption key implementation. *arXiv preprint arXiv:1502.01264*.

[28] Omotosho, A., & Emuoyibofarhe, J. (2015). A criticism of the current security, privacy and accountability issues in electronic health records. *arXiv preprint arXiv:1501.07865*.

[29] Varsha, B. S., & Suryateja, P. S. (2014). Using Advanced Encryption Standard for Secure and Scalable Sharing of Personal Health Records in Cloud. *International Journal of Computer Science and Information Technologies (IJCSIT)* **5**(6): 7745-7747.

[30] Oh, J. Y., Yang, D. I., & Chon, K. H. (2010). A selective encryption algorithm based on AES for medical information. *Healthcare informatics research* **16**(1): 22-29.

[31] Shin, D., Sahama, T., & Gajanayake, R. (2013, October). Secured e-health data retrieval in DaaS and Big Data. In *roceedings of 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)* (IEEE), pp. 255-259.

[32] Ramakrishnan, N., & Sreerekha, B. (2013). Enhancing Security of Personal Health Records in Cloud Computing by Encryption. In *International Journal of Science and Research (IJSR)*.

[33] Pooja, Batra, N. (2014). Secure Mechanism for Medical Database Using RSA. *International Journal of Application or Innovation in Engineering & Management* **3**(7): 320-327.

[34] Dhanabagyam, S. N., and G. R. Karpagam. (2017) Secure Communications for e-Health in Mobile Cloud Computing Using Provable Security. *International Journal of Pure and Applied Mathematics* **114**(7): 325-335.

[35] Sridevi, R., & Nithiya, C. (2016). E-Health Security using ECC algorithm. *International*

Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST), **2**(19): 114-117.

[36] Tsai, K. L., Leu, F. Y., Wu, T. H., Chiou, S. S., Liu, Y. W., & Liu, H. Y. (2014). A Secure ECC-based Electronic Medical Record System. *J. Internet Serv. Inf. Secur.* ***4***(1): 47-57.

[37] Zheng, Y. (2011). Privacy-preserving personal health record system using attribute-based encryption, *Masters Thesis*, (Publisher: Worcester Polytechnic Institute). *https://digitalcommons.wpi.edu/etd-theses/902*

[38] Akinyele, J. A., Pagano, M. W., Green, M. D., Lehmann, C. U., Peterson, Z. N., & Rubin, A. D. (2011, October). Securing electronic medical records using attribute-based encryption on mobile devices. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices* (ACM), pp. 75-86.

[39] Rezaeibagha, F., Win, K. T., & Susilo, W. (2015). A systematic literature review on security and privacy of electronic health record systems: technical perspectives. *Health Information Management Journal* **44**(3): 23-38.

[40] Kulkarni, K., & Dixit, A. M. (2014). Privacy Preserving System Using Attribute Based Encryption for e-health Cloud.

[41] Charanya, R., Nithya, S., & Manikandan, N. (2017, November). Attribute based encryption for secure sharing of E-health data. In *Materials Science and Engineering Conference Series* **263**(4): 042030.

[42] Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2012). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE transactions on parallel and distributed systems* **24**(1): 131-143.

[43] Sadikin, M. A., & Wardhani, R. W. (2016, July). Implementation of RSA 2048-bit and AES 256-bit with digital signature for secure electronic health record application. In *proceedings of 2016 International Seminar on Intelligent Technology and Its Applications (ISITIA)* (IEEE), pp. 387-392.

[44] Liu, C.H., Chen, T.L., Lin, H.Y., Lin, F.Q., Liu, C.M., Wu, E.P., Chen. T.S. (2013) Secure PHR Access Control Scheme in Cloud Computing. *International Journal of Information and Electronics Engineering* **3**(3): 329.

[45] Drozdowicz, M., Ganzha, M., & Paprzycki, M. (2016). Semantically enriched data access policies in eHealth. *Journal of medical systems* **40**(11): 238.

[46] Lu, S., Hong, Y., Liu, Q., Wang, L., & Dssouli, R. (2007, November). Access control in e-health portal systems. In *proceedings of 2007 Innovations in Information Technologies (IIT)* (IEEE), pp. 88-92.

[47] Gritti, C., Susilo, W. & Plantard, T. (2016). Certificate-based encryption with keyword search enabling secure authorization in electronic health record. *Journal of Internet Services and Information Security*, **6** (4): 1-34.

[48] Vincent, J., Pan, W., Coatrieux, G., (2016) Privacy protection and security in eHealth cloud platform for medical image sharing. In *proceedings of 2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, (IEEE), pp. 93-96.

[49] Kim, D. H., & Kwak, J. (2018, January). The Framework of 3P-Based Secure eHealth-Information System. In *proceedings of 2018 International Conference on Platform Technology and Service (PlatCon)* (IEEE), pp. 1-6.

[50] Liu, C.H., Lin, F.Q., Chiang, D.L., Chen, T.L., Chen, C.S., Lin, H.Y., Chung, Y.F., and Chen, T.S., (2013) Secure PHR access control scheme for healthcare application clouds. In *proceedings of 2013 42nd International Conference on Parallel Processing*, (IEEE) ,pp. 1067-1076.

[51] Huang, J., Sharaf, M., Huang, T.S., (2012) A hierarchical framework for secure and scalable ehr sharing and access control in multi-cloud. In *proceedings of 2012 41st International Conference on Parallel Processing Workshops,* 10-13 Sept. 2012 (IEEE), pp. 279-287.

[52] Lounis, A., Hadjidj, A., Bouabdallah, A., Challal, Y., (2012). Secure and scalable cloud-based architecture for e-health wireless sensor networks. In *proceedings of 2012 21st International Conference on Computer Communications and Networks (ICCCN),* July 30, 2012 - August 2, 2012 (IEEE: IEEE Communication Society; U.S. National Science Foundation (NSF); City Mayor of Munich), pp. 1-7.

[53] Tong, Y., Sun, J., Chow, S.S.M., Li, P., (2013). Towards auditable cloud-assisted access of encrypted health data. In *proceedings of 2013 IEEE Conference on Communications and Network Security (CNS)*, 14-16 Oct. 2013 (IEEE), pp. 514-519.

[54] Chen, L., & Hoang, D. B. (2011, September). Novel data protection model in healthcare cloud. In *proceedings of 13th IEEE International Workshop on FTDCS 2011, the 8th International Conference on ATC 2011, the 8th International Conference on UIC 2011 and the 13th IEEE International Conference on HPCC 2011*, September 2, 2011 - September 4, 2011 (IEEE), pp. 550–555.

[55] Sharma, M., Bai, Y., Chung, S., & Dai, L. (2012, June). Using risk in access control for cloud-assisted ehealth. In *proceedings of 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems* (IEEE), pp. 1047-1052.

[56] Yu, Z., Thomborson, C., Wang, C., Wang, J., & Li, R. (2012, July). A cloud-based watermarking method for health data security. In *proceedings of 2012 International Conference on High Performance Computing & Simulation (HPCS)*, 2-6 July 2012 (IEEE), pp. 642-647.

[57] Alabdulatif, A., Khalil, I., & Mai, V. (2013, July). Protection of electronic health records (EHRs) in cloud. In *proceedings of 2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 3-7 July 2013 (IEEE), pp. 4191-4194

[58] Ermakova, T., & Fabian, B. (2013, July). Secret sharing for health data in multi-provider clouds. In *proceedings of 2013 IEEE 15th Conference on Business Informatics (CBI),* 15-18 July 2013 (IEEE), pp. 93–100.

[59] Zhang, R., & Liu, L. (2010, July). Security models and requirements for healthcare application clouds. In *proceedings of 2010 IEEE 3rd International Conference on cloud Computing* (IEEE), pp. 268-275.

[60] Pecarina, J., Pu, S., & Liu, J. C. (2012, December). SAPPHIRE: Anonymity for enhanced control and private collaboration in healthcare clouds. In *proceedings of 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings* (IEEE), pp. 99-106.

[61] Lin, H., Shao, J., Zhang, C., & Fang, Y. (2013). CAM: cloud-assisted privacy preserving mobile health monitoring. *IEEE Transactions on Information Forensics and Security* **8**(6): 985-997.

[62] Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N., & Müller, G. (2011). Aspects of privacy for electronic health records. *International journal of medical informatics* **80**(2): e26-e31.

[63] Shrestha, N. M., Alsadoon, A., Prasad, P. W. C., Hourany, L., & Elchouemi, A. (2016, April). Enhanced e-health framework for security and privacy in healthcare system. In *proceedings of 2016 Sixth International Conference on Digital Information Processing and Communications (ICDIPC)* (IEEE), pp. 75-79.

[64] Liu, Z., Weng, J., Li, J., Yang, J., Fu, C., & Jia, C. (2016). Cloud-based electronic health record system supporting fuzzy keyword search. *Soft Computing* **20**(8): 3243-3255.

[65] Manoj, R., Alsadoon, A., Prasad, P. C., Costadopoulos, N., & Ali, S. (2017, April). Hybrid secure and scalable electronic health record sharing in hybrid cloud. In *proceedings of 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)* (IEEE), pp. 185-190.

[66] Tahir, R., Tahir, H., Sajjad, A., & McDonald-Maier, K. (2017, March). A secure cloud framework for ICMetric based IoT health devices. In *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing* (ACM), p. 171.

[67] Sakr, A., Yaacoub, E., Noura, H., Al-Husseini, M., Abualsaud, K., Khattab, T., Guizani, M., (2018) A secure client-side framework for protecting the privacy of health data stored on the cloud. In *proceedings of 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)* (IEEE), pp. 1-6.

[68] Han, H., Huang, M., Zhang, Y., & Bhatti, U. A. (2018, June). An architecture of secure health information storage system based on blockchain technology. In *proceedings of International Conference on Cloud Computing and Security* (Springer, Cham), pp. 578-588.

[69] Chinnasamy, P., & Deepalakshmi, P. (2018, April). Design of Secure Storage for Health-care Cloud using Hybrid Cryptography. In *proceedings of 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)* (IEEE), pp. 1717-1720.

[70] Selvam, L., & Arokia, R. J. (2018, March). Secure Data Sharing of Personal Health Records in Cloud Using Fine-Grained and Enhanced Attribute-Based Encryption. In *proceedings of 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)* (IEEE), pp. 1-6.

[71] Maganti, P. K., & Chouragade, P. M. (2019, February). Secure Health Record Sharing for Mobile Healthcare in Privacy Preserving Cloud Environment. In *proceedings of 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)* (IEEE), pp. 1-4.

[72] Maganti, P. K., & Chouragade, P. M. (2019). Secure Application for Sharing Health Records using Identity and Attribute based Cryptosystems in Cloud Environment. In *proceedings of 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*(IEEE), pp. 220-223.

[73] Choi, M., and Paderes, R.E.O., (2015) Biometric application for healthcare records using cloud technology. In *proceedings of 2015 8th International Conference on Bio-Science and Bio-Technology (BSBT)* (IEEE), pp. 27-30.

[74] Vinodhini, A. N., & Ayyasamy, S. (2017, March). Prevention of personal data in cloud computing using bio-metric. In *proceedings of 2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT)* (IEEE), pp. 1-6.

[75] Gopal, G.V., and Saiphani, K.V., (2017). Providing security with biometric system to the health data using cloud storage. *International Journal of Recent Trends in Engineering & Research, National Conference on Convergence of Emerging technologies in computer science and Engineering (CETCSE-2k17*), pp. 266-272.

[76] Sharma, S., & Balasubramanian, V. (2014, November). A biometric based authentication and encryption framework for sensor health data in cloud. In *Proceedings of the 6th International Conference on Information Technology and Multimedia* (IEEE), pp. 49-54.

[77] Wang, X. A., Ma, J., Xhafa, F., Zhang, M., & Luo, X. (2017). Cost-effective secure E-health cloud system using identity based cryptographic techniques. *Future Generation Computer Systems* **67**: 242-254.

[78] Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and Privacy-preserving Challenges of e-Health Solutions in Cloud Computing. *IEEE Access*, **7**: 74361-74382.

[79] Wang, H. (2018). Anonymous Data Sharing Scheme in Public Cloud and Its Application in E-Health Record. *IEEE Access*, **6**: 27818-27826.

[80] Albarki, I., Rasslan, M., Bahaa-Eldin, A. M., & Sobh, M. (2019). Robust Hybrid-Security Protocol for HealthCare Systems. *Procedia Computer Science*, **160**: 843-848.

[81] Badr, S., Gomaa, I., & Abd-Elrahman, E. (2018). Multi-tier blockchain framework for IoT-EHRs systems. *Procedia Computer Science*, **141**: 159-166.

[82] Cao, S., Zhang, G., Liu, P., Zhang, X., & Neri, F. (2019). Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. *Information Sciences*, ***485*:** 427-440.

[83] Shen, Q., Liang, X., Shen, X. S., Lin, X., & Luo, H. Y. (2013). Exploiting geo-distributed clouds for a e-health monitoring system with minimum service delay and privacy preservation. *IEEE journal of biomedical and health informatics*, **18**(2): 430-439.

[84] Xu, C., Wang, N., Zhu, L., Sharif, K., & Zhang, C. (2019). Achieving Searchable and Privacy-Preserving Data Sharing for Cloud-Assisted E-healthcare System. *IEEE Internet of Things Journal,* **6**(5): 8345-8356.

[85] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for Secure EHRs Sharing of Mobile Cloud based E-health Systems. *IEEE Access*, **7**: 66792-66806.

[86] Jangiti, S., Swathi, G., Ravi, L., Vijayakumar, V., & Subramaniyaswamy, V. (2019). Automated question extraction and tagging for cloud-based online communities. *International Journal of Web Based Communities*, **15**(3): 212-224.

[87] Azeez, N. A., & Van der Vyver, C. (2019). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. *Egyptian Informatics Journal*, **20**(2): 97-108.

[88] Patra, D., Ray, S., Mukhopadhyay, J., Majumdar, B., & Majumdar, A. K. (2009, December). Achieving e-health care in a distributed EHR system. In *proceedings of 2009 11th International Conference on e-Health Networking, Applications and Services (Healthcom 2009)* (IEEE), pp. 101-107.

[89] Sahama, T., Simpson, L., & Lane, B. (2013, October). Security and Privacy in eHealth: Is it possible?. In *proceedings of 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)* (IEEE), pp. 249-253.

[90] Bernsmed, K., Hon, W. K., & Millard, C. (2014, June). Deploying Medical Sensor Networks in the Cloud-Accountability Obligations from a European Perspective. In *proceedings of 2014 IEEE 7th International Conference on Cloud Computing* (IEEE), pp. 898-905.

[91] Mirkovic, J., Skipenes, E., Christiansen, E. K., & Bryhni, H. (2015, April). Security and privacy legislation guidelines for developing personal health records. In *proceedings of 2015 Second International Conference on eDemocracy & eGovernment (ICEDEG)* (IEEE), pp. 77-84.

[92] Devillier, N. (2016, November). Ageing, well-being and technology: From quality of life improvement to digital rights management a French perspective. In *proceedings of 2016 ITU Kaleidoscope: ICTs for a Sustainable World (ITU WT)* (IEEE), pp. 1-7.

[93] Balboni, P., & Iafelice, B. (2011, October). Mobile cloud for enabling the EU eHealth sector regulatory issues and opportunities. In *proceedings of 2011 Technical Symposium at ITU Telecom World (ITU WT)* (IEEE), pp. 51-56.

[94] Paul, P. K., & Ghose, M. K. (2012). Cloud Computing: possibilities, challenges and opportunities with special reference to its emerging need in the academic and working area of Information Science. *Procedia engineering*, **38**, 2222-2227.