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

INTRODUCTION: The e-health (electronic health) system is one of many cloud services 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. The health data records are kept in a semi-trusted third-party supplier (i.e., cloud). Therefore, its security has become the main concern as the data should not be accessible to unauthorized person.
OBJECTIVES: To provide a brief knowledge on the security aspects of cloud-based e-health systems for further improvement in the field of e-health system security.
METHODS: This paper presents a literature survey on secure cloud-based e-health systems including ninety-four research papers related to secure cloud-based e-health systems collected from different sources till 2019.
RESULTS: The security mechanisms used to secure cloud-based e-health systems are divided into three categories (i.e., crypto, non-crypto, and biometric-based). Also some health related security laws, security mechanisms, advantages and limitations of security mechanisms for all categories are presented.
CONCLUSION: This paper will be helpful to do further researches in the research area of e-health system as it consists of the analysis of security mechanisms, security laws, advantages and limitations of the security mechanisms.

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/_____

*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
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
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
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.

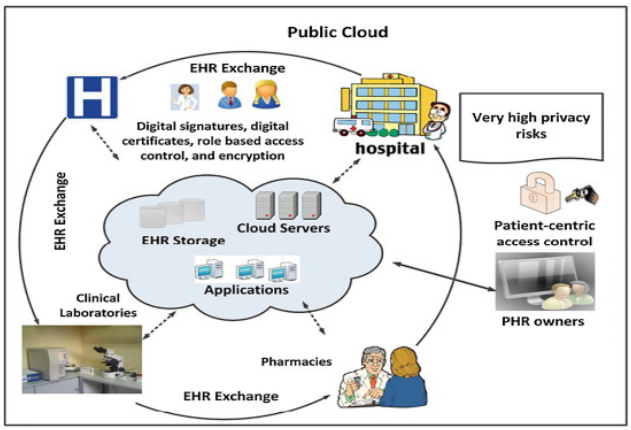

Figure (a). Public e-health cloud system.

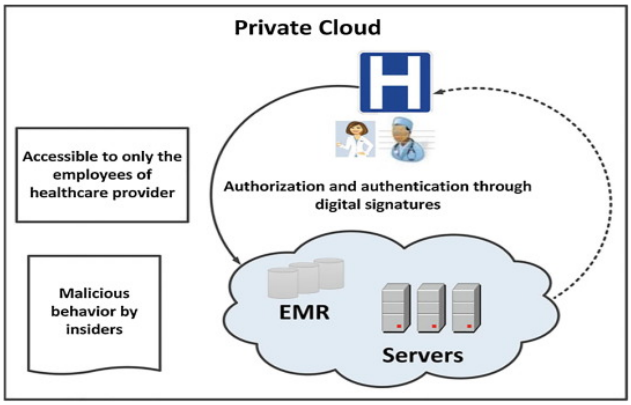

Figure (b). Private e-health cloud system.

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.

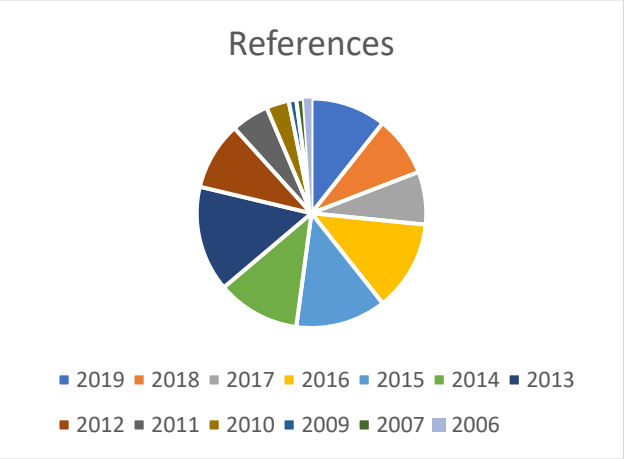

Figure (1). For different years the fractions of references included out of total references.

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	European Parliament,	The personal data need to be, • Processed impartially and legitimately.

[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.