Various strategies of privacy preservation in the healthcare digital system: Survey

Yogita Deepak Sinkar[1], C.Rajabhushanam[2]
[1]Ph.D.Scholor, Bharath Institute of Higher Education and Research
[2] Professor, Computer Science & Engineering, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu, India
Email: rajabhushanamc.cse@bharathuniv.ac.in
gtsinkar186@gmail.com

Abstract

Preservation of privacy is greatly important to minimize the disclosure to confidential patient details. Various strategies of privacy preservation are implemented in the digital system, but in the digital world, the security of personal data of the user remains a problem. Here we will see the literature review of to protect the user's medical details, an appropriate privacy protection system is therefore created. The filtering mechanism, The privacy preserved data info storage system, the preserved information is stored within the cloud management system of the cloud setting to render access to the user with higher privacy and utility.

Keywords: privacy preservation, cloud healthcare, cloud management system.

1. Introduction

Preserving privacy in cloud systems requires two aspects: protection in data collection and protection in data storage. Safety of data processing includes the problems of how to preserve consumer privacy in a visualized cloud environment at run time. The dynamic and multi-level technologies allow the cloud storage program more vulnerable to failure.[17]Health cloud is the software system through which users and healthcare professionals interact via software server[12].

Health treatment is specifically appropriate for cloud healthcare because it needs pay as a consumption model and technological capabilities for internet health providers. Moreover, utilizing the cloud technology in the medical care method, owing to the inclusion of sensitive details throughout the patient data, poses big problems. The health care owner subcontract the medical database to the cloud for e-health, whilst the cloud application provider can reveal the data[15]. The healthcare system's main goal is to provide quality treatment from everywhere and all moment, however. Providing health care data with confidentiality is a significant concern in the medical industry, as it protects data access privileges.Private information is the main element in the cloud, and it has the sub-factor as confidentiality that is needed to prevent the release of receptive patient data[10]. Preservation of privacy is a major necessity in the approach to clinical prediagnosis as more sensitive material is found in the medical data. If proper privacy security is not specifically established, the customers discontinue their confidence in utilizing cloud computing[2]. The solution to privacy needs to be flexible and reliable in order to operate toward extreme attacks[13].In comparison, the cloud setting of the healthcare sector greatly offers a flexible and rational software platform, thus dispersing the medical professionals and the patients. Digital service must therefore be allowed to promote collaboration between doctors, clinicians, and patients to address diagnosis, medical problems, and treatments[14][21].

The rest of this paper is structured as follows: Section 2 discusses motivation and survey of different current mechanisms of protecting privacy, along with their benefits and demerits efficiency review.

and section 3 addresses the discussion of Security And Safety E-Health Data Criteria In Cloud Finally, the article ends in section 4.

2. Motivation

This section explains the privacy model's inspiration by utilizing different current cloud-based data protection approaches. Quick access to health data is required for improved healthcare facilities that promote good quality of life, as well as ensuring support when medical emergencies arise. E-healthcare services are highly common nowadays as it dramatically reduces the utilization of hospitals.

2.1 Review of different literature works:

Alphonsa M.A. And Amudhavalli P[1] implemented a updated glowworm algorithm to conduct the process of data recovery and sanitization. It achieved improved results in terms of main responsiveness, and established an appropriate system for reconstruction and sanitization. The link between the key and encrypted data, however, was quite weak.N.P Karlekar And Gomathi N[2] modelled the Kronecker formula and the Bat algorithm to execute the cloud environment privacy protection process. It has successfully collected the data protected for protection, and has accomplished improved DBDR and precision to validate the measure of protection. It failed to reach the required amount of iterations, however. Tong Li et al.[3] also implemented an approach to data publication to build ample documents. It obtained better mechanism of privacy security by maintaining data integrity. It obtained improved efficiency in anonymity without deleting the critical attributes. It was important to complicated publishing method, however. Li J et al.[4] established a multi-party data protection (PMDP) method to secure numerical data and disclose untrusted cloud data. This successfully concurrently accomplished the storage delegation and guarantees protection without complicity. This struggled to satisfy the demands of big data, though. Piao C et al.[5] established a cloud-based computing method for publishing the results. This uses the differential approach to avoid exposure of the data. Nevertheless, it reduced question responsiveness and increased the utility of data publishing. In fact, data exchange at fog layer was not accomplished. Song W et al.[6] implemented the Cloud Paradigm Text Retrieval method. This basically separates the terms in the papers from the pages. It became easier because it maintained protection over cloud records. Nonetheless, risk management has not been addressed about the scenario of the attack.Wu Z et al.[7] developed a cloud-based model of consumer privacy security. The data was encrypted before saving to the cloud utilizing encryption protocol to improve server data protection. Using authenticated data it conducted the queries effectively. Protecting the records, however, was not satisfied with the user actions. Rawal B.S et al.[8] have developed a safe disintegration system for cloud-based privacy protection. It manages the load by supplying cloud storage with high protection. However, it did not allow efficient use of the cryptographic templates. It has shown considerable progress in improving collaboration among various health care providers. Furthermore, the transition of large data from the medical establishment to the cloud liberated the health care industry from the practices of leadership. The e-health cloud framework is inherently highly designed to store and handle vast volumes of health information across providers[9]. In the current Big data age, data abundance allows cloud storage to outsource health-care details. Regardless of the enormous bounces that the cloud offers, it often faces dangerous risks to health care data access and privacy[10][23].

3. SECURITY AND SAFETY E-HEALTH DATA CRITERIA IN CLOUD

Many of the potential attacks involve leakage of details, Cyber-attack (DoS), cloud malware intrusion assault, man-in-the-middle cryptographic assault[18].Spoofing[19], conspiracy attacks[20]. Cloud service companies and other government departments have recommended a range of protection initiatives and recommendations to ensure and improve customer and corporate trust. The first such regulatory initiative brought out for the US healthcare sector by the United States Congress in 1996 was the (HIPAA)[11]. There are basically three cloud service categories: trustworthy servers, semi-trusted servers, and untrusted servers. A secure server is one that can be completely secure without any leakage of details, and the risks to the stored health data may be attributed to internal opponents[16].

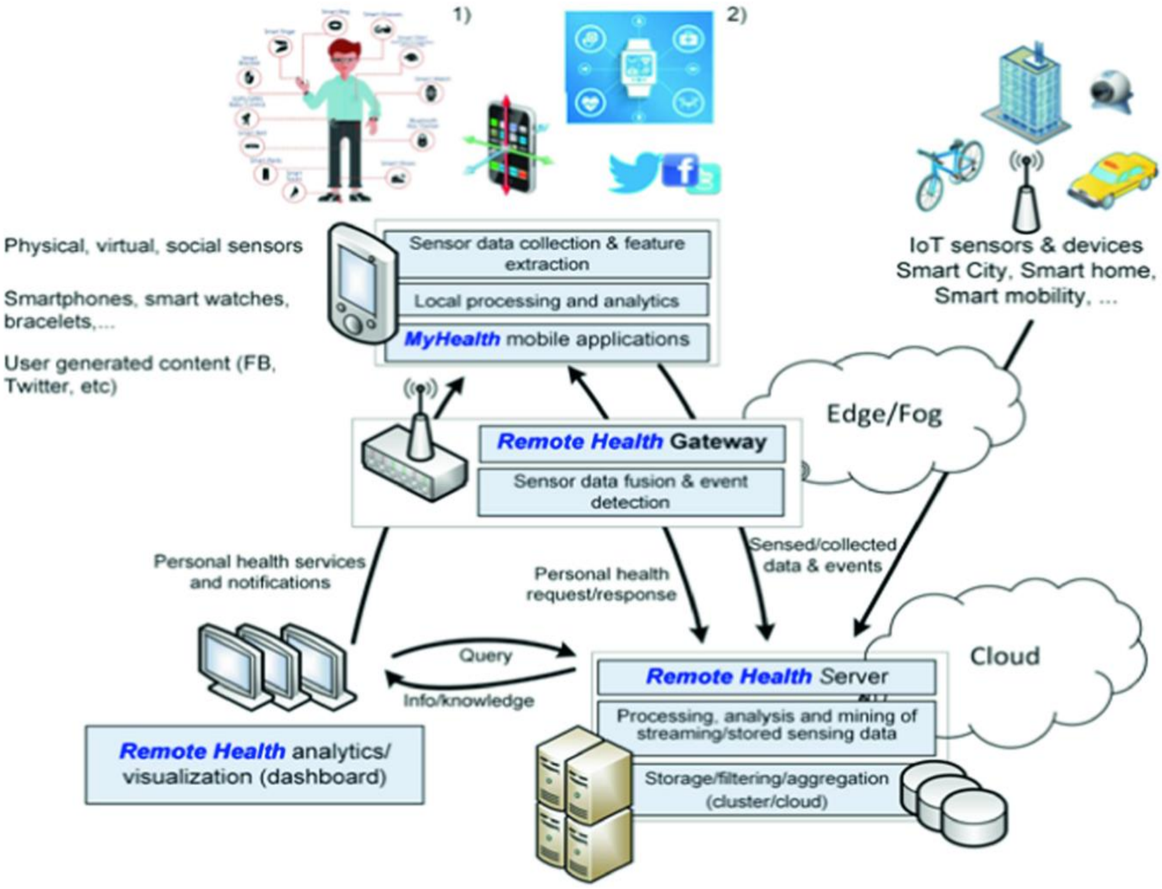
1)
2)
Physical, virtual, social sensors
Smartphones, smart watches, bracelets,...
User generated content (FB, Twitter, etc)
Sensor data collection & feature extraction
Local processing and analytics
MyHealth mobile applications
IoT sensors & devices
Smart City, Smart home, Smart mobility, ...
Edge/Fog
Remote Health Gateway
Sensor data fusion & event detection
Personal health services and notifications
Personal health request/response
Sensed/collected data & events
Query
Info/knowledge
Remote Health Server
Cloud
Processing, analysis and mining of streaming/stored sensing data
Storage/filtering/aggregation (cluster/cloud)
Remote Health analytics/ visualization (dashboard)

Figure 2: “ Remote health services”

The critical criteria for protection and privacy of e-health systems are 1) data integrity-assurance that no unauthorized party has altered the health records. 2) Confidentiality of records-assures the personal patient information is not entering unauthorized people. The most important solution to maintaining personal protection is the device encryption.3) Authenticity-guarantees that confidential health details can only be available to the approved and legitimate authority.4) Responsibility- an duty to be accountable and to explain persons or organization’s acts and decisions The most important 5) Audit- is a prerequisite that guarantees that the safety records are tracked and secured by maintaining control of the operation record and ensuring data protection and confidentiality for the relevant consumers. 6) Non-repudiation- applies to non-denial of sender and receiver legitimacy. For e.g., after malfunctioning of health records, patients or doctors cannot repudiate method for maintaining security of data is computer encryption. 7) Privacy- guarantees that the subject's identification will be anonymized and that cloud providers may not have access to the information of the health details collected.

4. Analysis Concerns and future direct Technology advancement benefits and difficulties :

This segment addresses research concerns and potential developments in EHR concerning privacy and protection. Because EHR data is private, secret, and stored in third-party repositories, there are significant data privacy and security risks involved [22].

1. How can I monitor and maintain the confidentiality of data held in the cloud?
2. How to incorporate data protection maintained for the safety of the health care?
3. What method of access control would be more effective for safe EHR transfer?
4. Whose encryption scheme should be used to safeguard data security?
5. How will patient details be exchanged easily with different health-care providers?
6. How do I preserve health records with integrity?

7. Who will be able to access the patient data during an emergency situation with healthcare providers?
8. What kind of access should the Administrative workers be provided to counter attacks inside?
9. How will account revocation be done when an authorised consumer leaves the system?
10. How to manage the complexities of key management when exchanging healthcare data among disparate healthcare providers?

This analysis outlined numerous research problems related to e-health data privacy and protection. We therefore noticed that there is an urgent need to improve the technology architecture in e-health systems targeted at patients to maintain data protection and security, thus maintaining confidentiality and sovereignty of patients. The great breakthroughs in emerging technology represented by social networking, IoT, Big Data Analytics, and cloud computing call for the urgent attention of all stakeholders to maintain better levels of privacy and protection for big data. The integration of data mining and artificial intelligence would also be a stronger subject of study to assess, investigate and avoid threats in healthcare. A fusion of encryption technologies and access management systems to protect big data protection and privacy may also be seen as a potential course of study to ensure a foolproof e-healthcare security system.

This technological development profits from a substantial reduction in cost of usage, web management, information collection as well as distribution, and hence the term slowly emerges further in other sectors that have abused the healthcare field. In these situations, more difficult is the effective processing and retrieval of data from a cloud system. In fact, the derived data must be conserved.

The limitations of the privacy paradigm are discussed here;

- Digital healthcare is gaining growing traction across the field to promote the distribution and storing of Big Data through e-health. At the cloud provider[9], though, maintaining the safety and confidentiality of healthcare data across the network results in major issues.
- Due to the presence of sensitive data in the medical information, adopting the cloud computing framework in the medical diagnosis system causes a significant complex in the cloud environment [15].
- Balancing the proper utility and privacy of cloud-related cloud data faces a challenging task in the health care system[2].
- Due to the difficulty of performance, protection and usability, the implementation of a model for privacy conservation utilizing a three-factor protocol remains a challenging problem in the difficult issue[9].
- Ressource stressful while protecting the confidential medical records of the patient is a daunting activity in a resource-constrained setting.

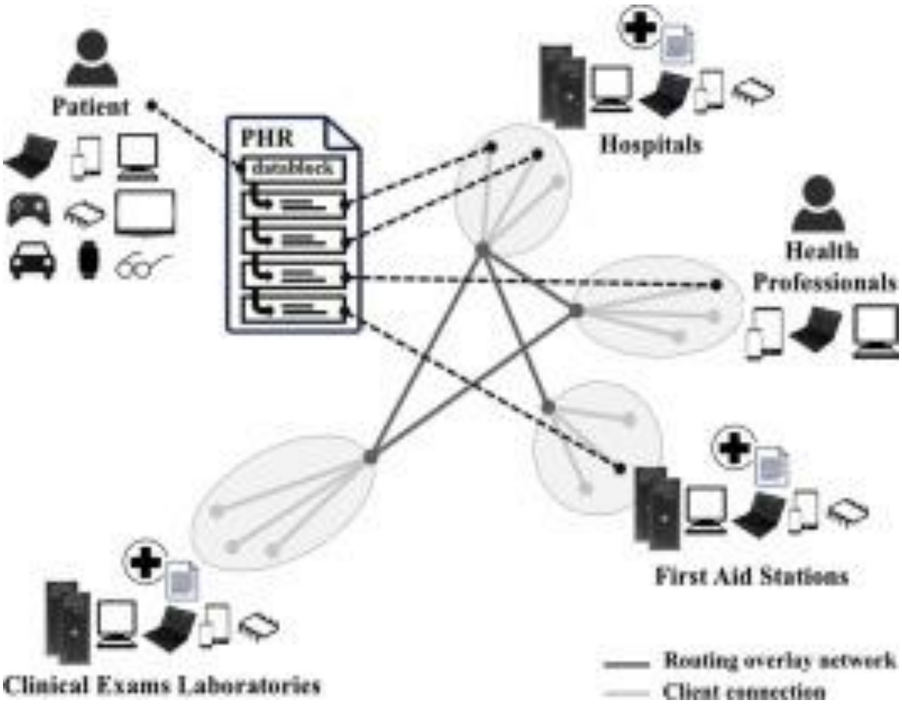

Figure 2: “Safety Architecture for Electronic Health using cloud”

A mixture of encryption mechanisms and access management mechanisms to protect the protection and privacy of analytics may also be seen as a potential research path for preserving a covert security system in e-healthcare .

5. Discussion:

Intelligent healthcare systems are a huge asset and are mainly utilized by doctors, clinicians and other healthcare professionals. Chenthara et al.: Safety and privacy-Preserving e-Health Applications issues nowadays in cloud service providers. Since most data are housed in cloud storage, which are particularly vulnerable to attacks and breaches, The need to shield them from unwanted entry is inevitable. Existing smart health systems have a degree of protection but not a system that is foolproof. In this sense, a significant scientific advancement to preserve patient trust and reputation is important for the wide-ranging application and progress of digital healthcare.

6. References

[1] Alphonsa M.A. and Amudhavalli P, “Genetically modified glowworm swarm optimization based privacy preservation in cloud computing for healthcare sector”, Evolutionary Intelligence, vol. 11, no. 1-2, pp.101-116, 2018.

[2] Karlekar N.P. and Gomathi N., “Kronecker product and bat algorithm-based coefficient generation for privacy protection on cloud”, International Journal of Modeling, Simulation, and Scientific Computing, vol. 8, no. 03, pp.1750021, 2017.

[3] Tong Li, Zheli Liu, Jin Li, Chunfu Jia and Kuan-Ching Li, ”CDPS: A cryptographic data publishing system”, Journal of Computer and System Sciences, nol. 89, pp.80-91, 2017.

[4] Li J., Wei J., Liu W and Hu X., “PMDP: A Framework for Preserving Multiparty Data Privacy in Cloud Computing”, Security and Communication Networks, 2017.

[5] Piao C., Shi Y., Yan J., Zhang C. and Liu L., “Privacy-preserving governmental data publishing: A fog-computing-based differential privacy approach”, Future Generation Computer Systems, vol. 90, pp.158-174, 2019.

[6] Song W., Wang B., Wang Q., Peng Z., Lou W. and Cui Y., “A privacy-preserved full-text retrieval algorithm over encrypted data for cloud storage applications”, Journal of Parallel and Distributed Computing, vol. 99, pp.14-27, 2017.

[7] Wu Z., Xu G., Lu C., Chen E., Jiang F. and Li G., “An effective approach for the protection of privacy text data in the Cloud DB”, World Wide Web, vol. 21, no. 4, pp.915-938, 2018.
[8] Rawal B.S., Vijayakumar V., Manogaran G., Varatharajan R. and Chilamkurti N., “Secure disintegration protocol for privacy preserving cloud storage”, Wireless Personal Communications, pp.1-17, 2018.
[9] Jiang Q., Khan M.K., Lu X., Ma J. and He D., “A privacy preserving three-factor authentication protocol for e-Health clouds”, The Journal of Supercomputing, vol. 72, no. 10, pp.3826-3849, 2016.
[10] Shrestha N.M., Alsadoon A., Prasad P.W.C., Hourany L. and Elchouemi A., “Enhanced e-health framework for security and privacy in healthcare system”, Sixth International Conference in Digital Information Processing and Communications (ICDIPC), IEEE, pp. 75-79, April 2016.
[11] Rahman S.M.M., Masud M.M., Hossain M.A., Alelaiwi A., Hassan M.M. and Alamri,A., “Privacy preserving secure data exchange in mobile P2P cloud healthcare environment”, Peer-to-Peer Networking and Applications, vol. 9, no. 5, pp.894-909, 2016.
[12] AL Hamid H.A., Rahman S.M.M., Hossain M.S., Almogren A. and Alamri A., “A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography”, IEEE Access, vol. 5, pp.22313-22328, 2017.
[13] Zhou J., Cao Z., Dong X. and Lin X., “PPDM: privacy-preserving protocol for dynamic medical text mining and image feature extraction from secure data aggregation in cloud-assisted e-healthcare systems”, IEEE, Journal of Selected Topics in Signal Processing, vol. 9, no. 7, pp.1332-1344, 2015.
[14] Sreedhar K.C. and Suresh Kumar N., “An optimal cloud-based e-healthcare system using k-centroid MVS clustering scheme”, Journal of Intelligent & Fuzzy Systems, vol. 34, no. 3, pp.1595-1607, 2018.
[15] Park J. and Lee D.H., “Privacy Preserving k-Nearest Neighbor for Medical Diagnosis in e-Health Cloud”, Journal of healthcare engineering, 2018.
[16] Karlekar N.P. and Gomathi N., “OW-SVM: Ontology and whale optimization-based support vector machine for privacy preserved medical data classification in cloud”, International Journal of Communication Systems, p.e3700, 2018.
[17] https://www.sciencedirect.com/science/article/pii/S1110866517302797
[18] N. Asokan, V. Niemi, and K. Nyberg, ‘‘Man-in-the-middle in tunnelled authentication protocols,’’ in Proc. Int. Workshop Secur. Protocols. New York, NY, USA: Springer, 2003, pp. 28–41.
[19] Y. Chen, W. Trappe, and R. P. Martin, ‘‘Detecting and localizing wireless spoofing attacks,’’ in Proc. 4th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Netw., Jun. 2007, pp. 193–202.
[20] C. Meadows, R. Poovendran, D. Pavlovic, L. Chang, and P. Syverson, ‘‘Distance bounding protocols: Authentication logic analysis and collusion attacks,’’ in Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks, New York, NY, USA: Springer, 2007, pp. 279–298.
[21] Lu, R., Liang, X., Li, X., Lin, X. and Shen, X., “Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications”, IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp.1621-1631, 2012.
[22]”Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing”, SHEKHA CHENTHARA , KHANDAKAR AHMED, (Member, IEEE), HUA WANG , AND FRANK WHITTAKER, Received April 19, 2019, accepted May 20, 2019, date of publication May 30, 2019, date of current version June 19, 2019.Digital Object Identifier 10.1109/ACCESS.2019.2919982.
[23] N. Dong, H. Jonker, and J. Pang, ‘‘Challenges in ehealth: From enablingto enforcing privacy,’’ in Proc. Int. Symp. Found. Health Inform. Eng. Syst.Berlin, Germany: Springer, 2011, pp. 195–206