Research Article

The Security and Privacy of Electronic Health Records in Healthcare Systems: A Systematic Review

Islam Sami Abdulhameed [1], Intisar Al-Mejibli [2], Jolan Rokan Naif [3]

[1] Iraqi Commission for Computers & Informatics, Informatics Institute for Postgraduate Studies, Baghdad, Iraq.
[2] Biomedical Informatics College, University of Information Technology and Communications Baghdad, Iraq.
[3]Iraqi Commission for Computers & Informatics, Informatics Institute for Postgraduate Studies, Baghdad
[1]dr.intisar.almejibli@gmail.com, ms201920528@iips.icci.edu.iq,[2] dr.intisar.almejibli@gmail.com,
[3]newjolan@gmail.com

Article History Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract: Electronic Health Records (EHRs) is used to increase the interoperability between healthcare organizations and patient health information while preserving privacy and confidentiality of patient information. EHR is structured information that may include text, image(s) or both of them; its aims to have the features of decentralization, security, openness, and traceability. This systematic review aims to examine and identify the forms of implemented electronic health records with the available protection and privacy techniques. A number of keywords have been used to scan four reliable databases, which are: PubMed, IEEE, Web of Science, and Science Direct. Where 126 studies have been obtained, based on the phases of filtering and scanning that implemented related to the criteria of inclusion/exclusion processes. This review presented a taxonomy where the concluded 126 studies were classified based on two categories, first includes the applied process of (authentication, authorization and access control), and second includes the applied process of privacy and security in (information, image, and both information with image) of EHR. Then, in this research, a deep review were conducted to highlight the challenges, issues, and critical gaps that outlined in the academic literature of this research subject. The obtained results showed no relevant study that examine and discuss the two aforementioned categories. This concluded that EHR could be enhanced by applying the processes of authentication, authorization, and access control in security, in addition to applying privacy for both information and image included in EHR.

Keywords: Electronic Health Records (EHR), healthcare, privacy, security, authentication, authorization, access control.

1. Introduction

Healthcare systems can be defined as the advantage of technology and automation to reduce high-quality healthcare service costs [1]. In general, healthcare systems are being used increasingly across institutions, across borders, and at the national level [2]. Also, these systems have been defined as a combination of medical and public health informatics and commerce related to health services and information provided or enhanced via the Internet and associated technologies [3]. In other words, the term of healthcare system not only refers to technical development but also to the way of thinking, attitudes, and participation in global network thinking for better healthcare at the local, regional and global level. When we look at all of this, we find that this area is very important in our lives and can save many lives by keeping the patient under constant surveillance in the hospital by tracing or the patient's medical history [4][5][6]. The healthcare field is increasingly dependent on mobile services for multimedia and applications. Among the most important of these applications are electronic health records, which have gained increasing popularity in many countries of the world today, such as the Kingdom of Saudi Arabia [7], Jordan [8], united states [9], united kingdom[10], Nigeria[11], Netherlands[12], Sweden[13], and India[14]. The security and the privacy play an important function in such systems to maintain the availability of health care services efficiently. Therefore, the World Health Organization (WHO) [15][16] has clarified that these systems use critical data and communication technologies in order to keep service providers, patients, and governments in touch [17] to educate and inform health professionals, managers and consumers. In addition to, encourage innovation in the delivery of both care and management related to the healthcare system to improve them. [18][19][20] The human impact of this health system is high, so people who join a medical organization have several questions about online communication. The primary goals of healthcare systems are efficiency, quality, safety, patient empowerment, medical training, ethics, and fairness [3]. In general, figure (1) shows the requirements of healthcare system. Therefore, safety and privacy are essential requirements in healthcare systems. Many different regulations and procedures must be taken into consideration in developing such systems. However, although regulations and procedures differ greatly from country to country, most of them aim to ensure several requirements of them:

- Ensuring the integrity of patient health information throughout its life cycle within the system [21].
- Perform protection against unauthorized access to signs of information, patient health, or use, and any breaches of security, confidentiality, and integrity, should they occur [22].

- Restricting access to sensitive data and applications to authorized personnel. Creating systems that require user identities, such as internal staff [23].

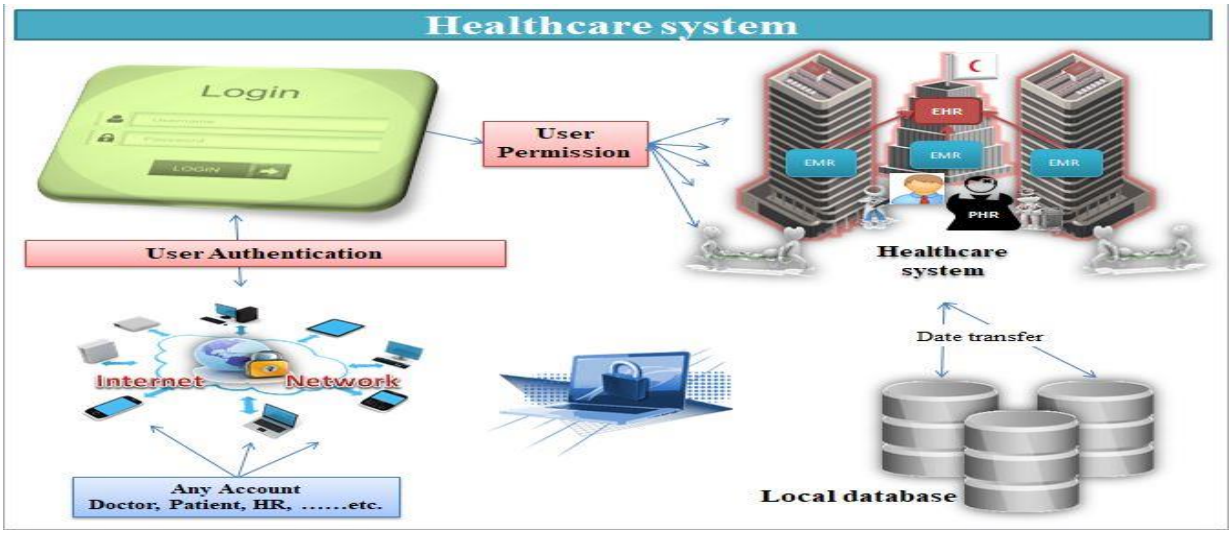


Figure 1: Healthcare System.

Two critical terms must be considered in developing a healthcare system, which is security and privacy. Data security governs the access to data throughout the data lifecycle. In contrast, the data privacy sets this access based on privacy policies and laws that determine, for instance, who can view personal data, financial, medical or confidential information—three paramount of security, which are authentication, authorization and access control. The authentication process verified the identities of the users. In general, the verification process includes a username and a password but other methods can be used instead such as PIN number, fingerprint scan, and smart card. Authorization process is established if the user (who is already authenticated) is allowed to have access to a resource. Access control process enforced the required security for a particular resource. This process actively prevents the user from accessing anything they should not. This review examined these aspects in details throughout the following sections, in order to clarify the state-of-art of applied security and privacy in healthcare systems and identify the gaps in this area. Finally, although figure (1) presents the general context of the security with privacy issues and requirements of the healthcare system, the following sections will go further, focusing on relevant investigated studies.

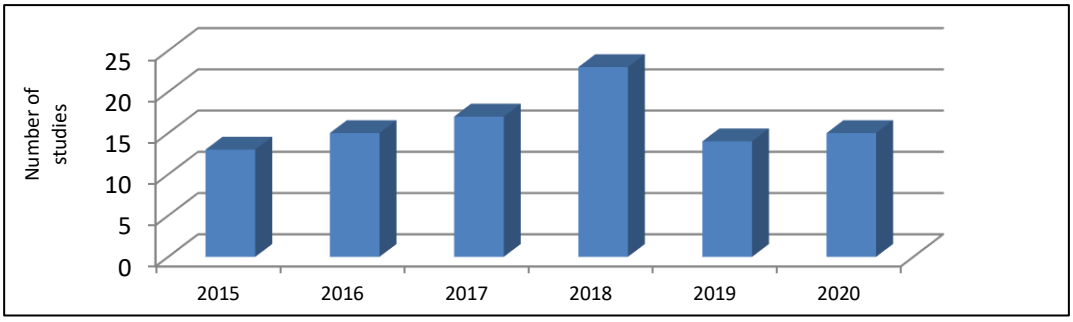
2. Methodology

This research adopted the systematic review approach based on four academic databases: PubMed, IEEE, Web of Science (WoS), and Science Direct. PubMed is the ultimate scientific and scientific engineering science database. IEEE Explore includes updated research papers in information science, electronic technical, engineering applications, and computer technology in medical applications. WoS is a widely trusted platform in the fields of social sciences, engineering, science, the arts, humanities but this type of database dose not available in Iraq. Science Direct includes different scientific literature covers all disciplinary sciences. All scholarly facets of the healthcare system are covered by these four databases. These databases are regarded sufficient to include the recent and most reliable literature for the security and privacy of electronic patient record. The extracted studies from these databases are relevant and reliable to investigate the significance of security and privacy in electronic patient record and their impact on healthcare systems. The obtained studies have been extracted from the four major databases in latest 5 years between 2015 and 2020, where all of them are in English language. The type of selected studies is could be journal, conference or book chapter. The conclusions of this literature review will help save lives by offering in-depth observations that lead to the safety of medical care processes, as well as suggested strategies for the development and making them reliable for patients.

3. Results

A basic search query using databases, specifically Google Scholar in English and without specifying the years of "security and privacy in the Healthcare System" without quotes, yielded more than 912,000 search results. After identifying the past six years, the results yielded 123,000 search results. The dataset was revised for the third time for comprehensive inclusion in the literature in the four citations of the databases above, published from 2015 to

2020. The selection of these indicators results from their adequate coverage of studies related to this research that hierarchically addressed data security and privacy, which requires excellent attention to the risks of tampering with these data on the health of patients. This study was presented based on four logical research strategies. The first strategy was conducted using several keywords related to healthcare systems, for example ("electronic health records" or "electronic health records" or "healthcare system")—the keywords related to information security (including authentication, authorization, and access control) and privacy. The results were trimmed dataset of 1756 articles in second strategy, after which we made a third pruning after reading the abstract and titles. This led to 226 research papers, followed by reading the entire research papers, in fourth reduction, and resulting in 126 research papers shown in figure (2) distributed over the years of its publication. Figure (3) shows the methodology result of research.



We used these inquiry techniques to develop research for different healthcare systems and their application studies; with all of the above, the alerts have been activated in search engines for permanent communication with any new studies.

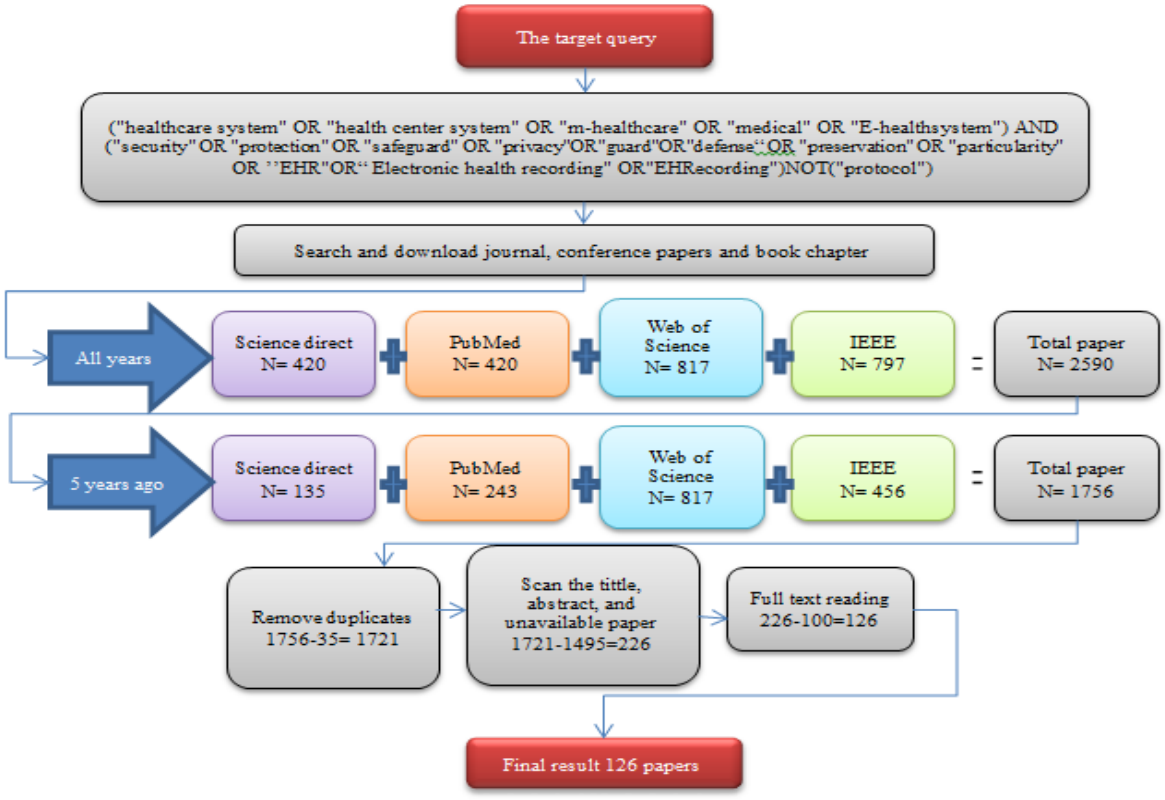


Figure 3: Methodology Result of Research.

4. 4. Criteria for eligibility

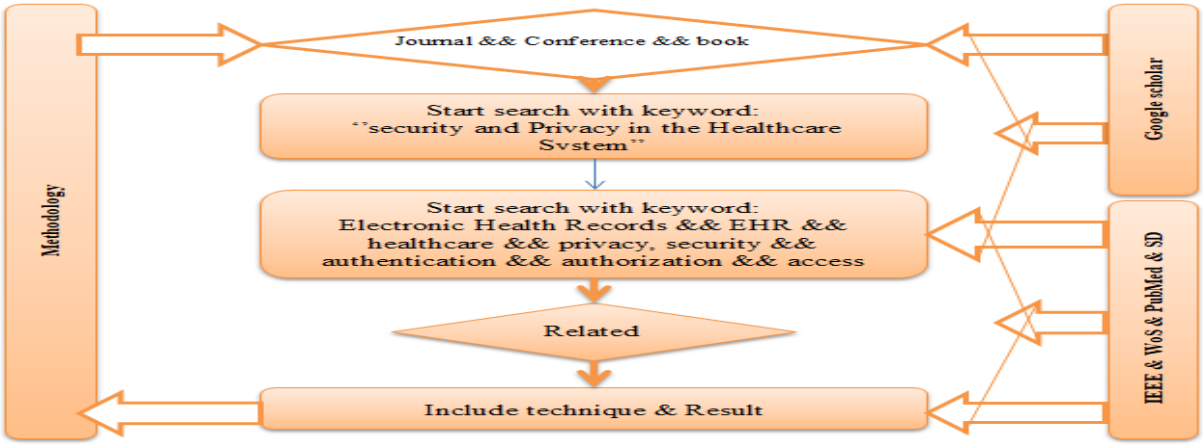
In this research, articles that met our requirements is shown in figure (4). The initial objective was to map the search range into a general and speciality classification consisting of two categories taken without constraints from a previous literature sample (we used Google Scholar to identify literature trends). After extracting redundant

papers between databases, where we found no connection to the subject of concern, just the medical part, we removed articles through a series of iterations of filtering and sorting.

Reports were omitted if they were:

A. Not written in English.
B. Artificial intelligence and data mining systems are their targets.
C. Protocols in the field of health systems.
D. They are just based on the medical side.
E. Any papers that did not explicitly discuss the protection and privacy of the health system, as with any documents that did not provide accurate information on these topics.

This research focuses on health care services, patient identity security priorities, the safety of their data from



misuse, and high-quality healthcare management and cost reduction.

Figure 4: Methodology Method of Research.

5. Data collection methods

The papers are included in the latest trimming, where they have been read, revised, and summarized according to their basic categories. The papers are stored as Microsoft Word and Excel files to improve the filtering process according to their years of authorship and the techniques and algorithms used in healthcare systems. The proposed classification is made possible by numerous highlights and notes on works surveyed and the continuous classification of scientific papers. Comments were recorded electronically or on papers. This method was preceded by another method for describing, defining, tabulating, and inferring essential findings. These results are presented as a complete guide in the supplementary materials for the results described in the next section.

6. Literature review

With the development of information technology, the expansion of the Internet, and the interconnectedness of health care systems. This has increased data exposure to threats, and new security holes have been discovered in these medical systems and equipment's cybersecurity. This led to making it a target for cybercrime for two reasons: First, these systems are rich sources of essential data. Second: It does not contain high-performance protection, and these crimes include theft of this information in addition to ransomware attacks on health systems and sometimes on the patient's mobile medical devices. Therefore, the patient's confidence in this type of system may be undermined, and this may damage health systems resulting in tampering with the patient's sensitive information, thus endangering his life, so security and privacy should always be the priority [24][25]. Many other security specifications must be included in the electronic health records infrastructure of healthcare systems, such as security, privacy, authentication, authorization, confidentiality, and access control. With the electronic health record, several experts recommended ensuring that information is shared to make most healthcare facilities. Many of them tried to meet the challenges facing healthcare and tried to reduce the security vulnerabilities associated with data processing, but they reduced their flexibility during delivery. In our review of many scientific articles dealing with the security and privacy of health care facilities, we found that many of them used the critical points to build a stable infrastructure effectively. With the variance ratios between those studies, its classification has been shown in figure (5). Further, we discovered that many of them did not discuss other priorities such as identification, permission, and access control despite studies dealing with one or two of them.

Although, studies of [24][26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44] [45]–[49] address the issue of authentication, other aspects are neglected. The authors of [50] [51]–[57] were only interested in authorization. Also [58] [59] [60] [61] [62] [63] [64] [20] [65] dealt only with the issue of access control. In all of the above; we did not find a study that included all objectives or solutions related to security and privacy issues, which led to continuous research on the subject.

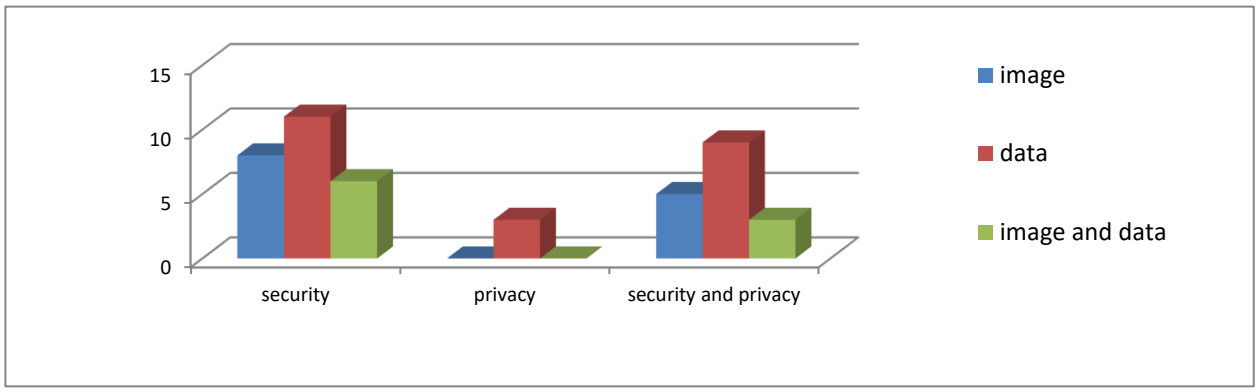
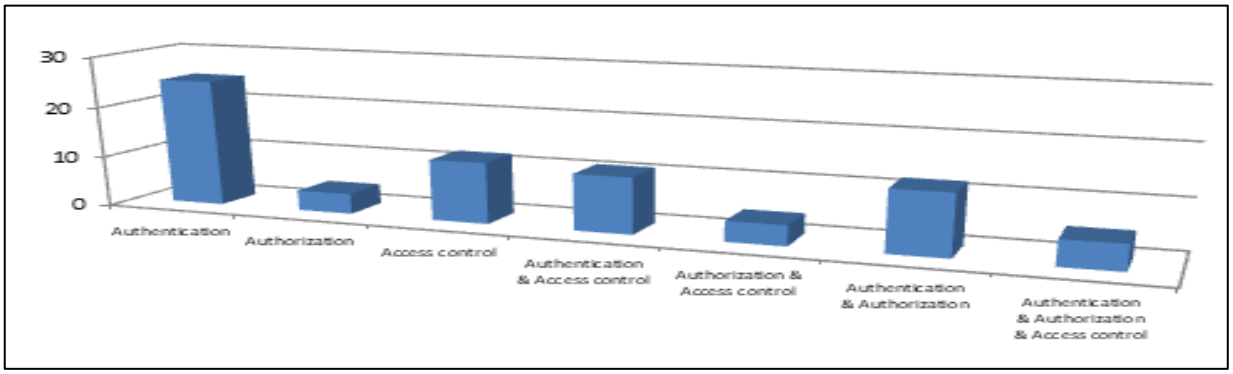


Figure 5: Classification and Variance between Security and Privacy Studies

We found that some studies [66] [67] [68] [69] [70] [71] [72] [73] [74] [75] [76] [77] with only two goals which are authentication and access control. Likewise, the authors of [78] [79] [80] [81] [82] included only their studies authorization and access control. In addition to everything we covered in previous studies, the authors of [3][83] [84] [85] [86] [87] [88] [89] [90] [91] [92] [93] dealt with authentication and authorization only. While The authors of [54][94] [95] [96] [97] [98] have comprehensively included all the above-mentioned goals as they are illustrated in figure (6).

Figure 6: Classification of the Security



On the other hand, [99] expected an improvement in the digitization of health and patient data in clinical, technical and commercial models shortly and generally in the economic climate. This change is related to demographic distribution and lifestyle improvement, in addition to the rapid development of digital applications and devices, prioritization and focus on quality and care that subsequently led to innovative treatments based on evidence rather than discretionary practices.

Thus providing clinical decision-making and increasing the efficiency of systems in the scope and approach of Health care. Technically, despite all these advantages, some decision-makers did not focus on the essential aspect of this type of system: the security aspect and were content with an in-depth definition of protection and privacy standards to protect the company and its customers. Several studies were confirmed this view, which is [75][97][100] [101] [102] [103] [104] [105] illustrated the importance of using an electronic patient record in healthcare systems and have been busy developing and updating this record in addition to obtaining better features such as lower costs and higher response speed [53][72][106] and did not address one of the biggest problems facing the healthcare sector in different places and multiple forms [1][4][54][75][99][107][108].

The authors of [45][71][109][110][111] proposed a health care system through which medical images are stored and shared between many doctors and patients securely. Their proposals were limited to dealing with

medical images only, without pay attention to patient's information. Likewise, the authors of [54][57][77][99][104][112][113][114] have also suggested a health system in which the sensitive patient information are shared in safe channels in addition to preserving its privacy. These systems were providing security to shared patient information only, without securing medical images. By the same logic, the authors of [20][113][115] proposed privacy-preserving health systems through which the medical information was exchanged among the doctors themselves besides sharing it with their patients. These systems were concerned with introducing a system that preserves the privacy of the patient and his/her information but did not address the security of these data. While the authors of [1] [48][75][76] [116][117][118][119][120][121] suggested another systems that sharing sensitive patient information between doctors and patients. These systems dealt with the security of information and did not give importance to privacy. Although the authors of [122][123][124][125][126] suggested systems for sharing images only through a secure channel, they did not address sensitive patient information and privacy in their proposals. At the same time, the authors of [3] [53][56][73][97] proposed safe systems for sharing medical images and sensitive patient information that can be accessible by the patients themselves. Also, they did not pay any attention to the privacy of this data.

The previously mentioned studies did not include a study investigating the safety and privacy of patient data for both medical image and medical information. However, the study of [47] affiliated to a proposed system where the author proposed an integrated security system in terms of security and privacy of images and medical information, but he used algorithms, not of the required level.

Figure (7) shows the classification of investigated studies according to the terms of authentication, authorization and access control.

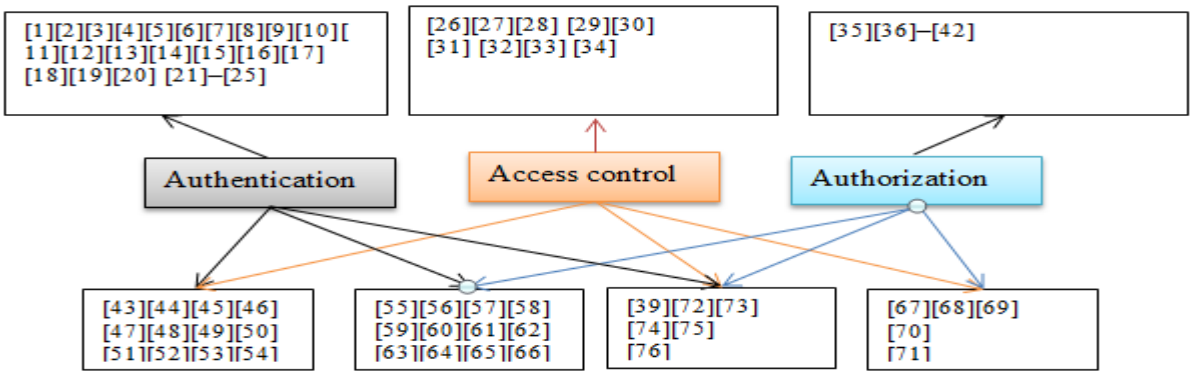


Figure 7: Component of Security Studies

Table 1: Some technique and data used

Author	Year	Technique	Types of Data
Dagadu [122]	2016	Comparison technique in DWT	Medical image
Bhopi [123]	2016	Chaotic maps	Medical image
Bouchti [118]	2016	Cass (cryptography as a service) included RSA & homomorphic algorithm	Healthcare Data
Kadhim [4]	2016	RSA & ElGamal algorithm	medical image
Sridevi [3]	2016	ECC algorithm	Healthcare Data
Ravichandran[113]	2017	DNA chaos blend	medical image
Dahiya [114]	2017	Parallel partial method IAES , mECC	Healthcare Data
Kiran [124]	2017	Dual DNA & Chaotic map	Medical image
Boussif [125]	2017	Matrix product and exclusive addition security	Medical image

Chauhan [56]	2017	Watermarking technique	Medical image
Yang [68]	2017	decisional bilinear Diffie-Hellman (DBDH) assumption	Health IOT data
Kumar [109]	2017	RSA, AES	Medical image
Kamble [21]	2018	DNA cryptography	Medical data
Winnie [117]	2018	AES algorithm	health care data
Brindha [45]	2018	AES-GCM (Galois counter mode) & whirlpool hush function	medical data
Singh[104]	2018	Stemming & lemmatization algorithms	EHR
Basnet [64]	2018	"Role-based access control" (RBAC)	EHR & PHR
Lim [47]	2018	SHA-2 & MAC algorithm	healthcare Data
Chinnasamy [53]	2018	Blowfish algorithm	EHR data
Shahzadi [111]	2019	Chaos based on Rc5	Medical data
Khandge [116]	2019	Decoy Technique	EMR
Cheng [46]	2019	ECC algorithm & session key symmetric encryption	Medical IOT device
Hussein [74]	2019	ECC+AES algorithm	Medical image
Kaw [93]	2019	Optimal Pixel Repetition (OPR)	Medical image and
Bindhu [112]	2020	Blowfish,SHA3 , Diffehelman	Cloud storage
Kumari [108]	2020	HECC SHA-2DWT	data in cloud
Kumar [119]	2020	R2E algorithm	PHR Data
Zhang [75]	2020	Huffman compression & RC4	EHR
Boussif [126]	2020	Arnold transform and Vigenere Cipher [126]	Medical image
Jenveja [83]	2020	AES	ECG signal
J.Zhang [67]	2020	ECC algorithm	EHR data
Olakanmi [100]	2020	symmetric key and modified ciphertext-policy attribute-based encryption	e-health system data
Gull [48]	2020	Huffman encoding strategy	IoMT data

7. Conclusion

As a conclusion, we note in all investigated studies, after examining and allaying them, some of these systems provided security channels for sharing data between doctors and patients, and the other preserving their privacy in the system itself. In this study, we dealt with several aspects according to the proposed methodology. Data security (including authentication, authorization, and access control) is one of these aspects, and the other side is data privacy, so studies have alternated between dealing with these aspects separately or in combination, and this depends on the quality of the security aspect in addition to the type of data. Thus, this study was revealed that many studies are focusing on security or privacy in healthcare systems, but there is no focusing on both (security and privacy) in these systems. This needs attention from the researchers as the information and images of such a system are significant and vital. In addition, meeting the requirements of both security and privacy will increase the user's trust in using such system which resulting in the success of these systems and achieve many advantages in terms of reducing healthcare services cost, providing the medical service at any time and at any pace and much more.

References

1. Samy, "Security issues in electronic health record," Open Int. J. Informatics, vol. 1, no. n/a, pp. 59–68, 2013.

2. P. S. Ruotsalainen, "Chapter 5 - Privacy, Trust and Security in Two-Sided Markets," V. B. T.-E.-H. T.-S. M. Vimarlund, Ed. Academic Press, 2017, pp. 65–89.
3. R. Sridevi, "10-2016 E-Health Security using ECC algorithm.pdf," vol. 2, no. 19, pp. 114–117, 2016.
4. Kadhim and R. M. Mohamed, "Visual cryptography for image depend on RSA & AlGamal algorithms," in *2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, 2016, pp. 1–6, doi: 10.1109/AIC-MITCSA.2016.7759935.
5. M. Bachiri, A. Idri, J. L. Fernández-Alemán, and A. Toval, "Evaluating the Privacy Policies of Mobile Personal Health Records for Pregnancy Monitoring," J. Med. Syst., vol. 42, no. 8, 2018, doi: 10.1007/s10916-018-1002-x.
6. K. L. Solem et al., "A user-centered approach to an evidence-based electronic health pain management intervention for people with chronic pain: Design and development of EPIO," J. Med. Internet Res., vol. 22, no. 1, 2020, doi: 10.2196/15889.
7. Aldosari, "Supportive care pathway functionalities of EHR system in a Saudi Arabian hospital," Comput. Biol. Med., vol. 89, pp. 190–196, 2017, doi: https://doi.org/10.1016/j.compbiomed.2017.08.012.
8. F. Klaib and M. S. Nuser, "Evaluating EHR and health care in Jordan according to the international health metrics network (HMN) framework and standards: A case study of hakeem," IEEE Access, vol. 7, no. July, pp. 51457–51465, 2019, doi: 10.1109/ACCESS.2019.2911684.
9. L. A. Destino et al., "Improving Communication with Primary Care Physicians at the Time of Hospital Discharge," Jt. Comm. J. Qual. Patient Saf., vol. 43, no. 2, pp. 80–88, 2017, doi: https://doi.org/10.1016/j.jcjq.2016.11.005.
10. K. Wilson and L. Khansa, "Migrating to electronic health record systems: A comparative study between the United States and the United Kingdom.," Health Policy, vol. 122, no. 11, pp. 1232–1239, Nov. 2018, doi: 10.1016/j.healthpol.2018.08.013.
11. O. W. Bello, N. Faruk, and S. I. Popoola, "Implementation in Nigeria : A Proposal," Proc. 1St Int. Conf. IEEE Niger. Comput. Chapter, no. November, 2016.
12. Essén et al., "Patient access to electronic health records: Differences across ten countries," Heal. Policy Technol., vol. 7, no. 1, pp. 44–56, 2018, doi: https://doi.org/10.1016/j.hlpt.2017.11.003.
13. S. Hellberg and P. Johansson, "eHealth strategies and platforms – The issue of health equity in Sweden," Heal. Policy Technol., vol. 6, no. 1, pp. 26–32, 2017, doi: https://doi.org/10.1016/j.hlpt.2016.09.002.
14. C. Powell, J. K. Ludhar, and Y. Ostrovsky, "Electronic health record use in an affluent region in India: Findings from a survey of Chandigarh hospitals," Int. J. Med. Inform., vol. 103, pp. 78–82, 2017, doi: https://doi.org/10.1016/j.ijmedinf.2017.04.011.
15. S. Section and O. N. Editorial, "Editorial Ieee Access Special Section Editorial : Information Security Solutions for," vol. 6, pp. 79005–79009, 2018, doi: 10.1109/ACCESS.2018.2885256.
16. T. Graves, "A manual for developing countries.," Community Eye Health, vol. 15, no. 44, pp. 64–64, 2002.
17. Essén, R. Gerrits, and E. Kuhlmann, "Patient accessible electronic health records: Connecting policy and provider action in the Netherlands," Heal. Policy Technol., vol. 6, no. 2, pp. 134–141, 2017, doi: https://doi.org/10.1016/j.hlpt.2017.03.001.
18. S. Kazi, "From innovation to implementation: Optimizing long-term outcomes after TAVR," J. Am. Coll. Cardiol., vol. 64, no. 24, pp. 2616–2618, 2014, doi: 10.1016/j.jacc.2014.10.008.
19. A. Arman and L. Dwiyanti, "Framework of information system architecture for healthcare organization based on collaborative care model," Proc. - 5th Int. Conf. Electr. Eng. Informatics Bridg. Knowl. between Acad. Ind. Community, ICEEI 2015, pp. 710–715, 2015, doi: 10.1109/ICEEI.2015.7352590.
20. Gkoulalas-Divanis and G. Loukides, Medical data privacy handbook. 2015.
21. P. Kamble and S. Patil, "Medical Image Security with Cheater Identification," in 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018, pp. 1–6, doi: 10.1109/ICCUBEA.2018.8697460.M. Marwan, A. Kartit, and H. Ouahmane, "Security Enhancement in Healthcare Cloud using Machine Learning," Procedia Comput. Sci., vol. 127, pp. 388–397, 2018, doi: https://doi.org/10.1016/j.procs.2018.01.136.
22. M. Marwan, A. Kartit, and H. Ouahmane, "Security Enhancement in Healthcare Cloud using Machine Learning," Procedia Comput. Sci., vol. 127, pp. 388–397, 2018, doi: https://doi.org/10.1016/j.procs.2018.01.136.
23. P. M. Khilar, S. S. Khatua, and R. R. Swain, "A Secured Patients Monitoring System Using Sensor Nodes in Health Care Institutions," in 2018 International Conference on Recent Innovations in

Electrical, Electronics & Communication Engineering (ICRIEECE), 2018, pp. 2767–2772, doi: 10.1109/ICRIEECE44171.2018.9008858.

24. Ali and F. A. Khan, "Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications," Eurasip J. Wirel. Commun. Netw., vol. 2013, no. 1, pp. 1–19, 2013, doi: 10.1186/1687-1499-2013-216.
25. K. J. Deans, S. Sabihi, and C. B. Forrest, "Learning health systems," Semin. Pediatr. Surg., vol. 27, no. 6, pp. 375–378, 2018, doi: https://doi.org/10.1053/j.sempedsurg.2018.10.005.
26. Kardas and E. T. Tunali, "Design and implementation of a smart card based healthcare information system," Comput. Methods Programs Biomed., vol. 81, no. 1, pp. 66–78, 2006.
27. L. Mat Kiah, M. S. Nabi, B. B. Zaidan, and A. A. Zaidan, "An enhanced security solution for electronic medical records based on AES hybrid technique with SOAP/XML and SHA-1," J. Med. Syst., vol. 37, no. 5, 2013, doi: 10.1007/s10916-013-9971-2.
28. S. Irum, A. Ali, F. A. Khan, and H. Abbas, "A hybrid security mechanism for intra-wban and inter-WBAN communications," Int. J. Distrib. Sens. Networks, vol. 2013, 2013, doi: 10.1155/2013/842608.
29. Z. Siddiqui, A. H. Abdullah, M. K. Khan, and A. S. Alghamdi, "Smart environment as a service: three factor cloud based user authentication for telecare medical information system," J. Med. Syst., vol. 38, no. 1, p. 9997, 2014.
30. Alsadhan and N. Khan, "An LBP based key management for secure wireless body area network (WBAN)," SNPD 2013 - 14th ACIS Int. Conf. Softw. Eng. Artif. Intell. Netw. Parallel/Distributed Comput., pp. 85–88, 2013, doi: 10.1109/SNPD.2013.32.
31. Y. S. Lee, E. Alasaarela, and H. Lee, "Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system," Int. Conf. Inf. Netw., pp. 453–457, 2014, doi: 10.1109/ICOIN.2014.6799723.
32. M. Hamdi and H. Abie, "Game-based adaptive security in the Internet of Things for eHealth," 2014 IEEE Int. Conf. Commun. ICC 2014, pp. 920–925, 2014, doi: 10.1109/ICC.2014.6883437.
33. K. Saleem, A. Derhab, J. Al-Muhtadi, and B. Shahzad, "Human-oriented design of secure Machine-to-Machine communication system for e-Healthcare society," Comput. Human Behav., vol. 51, pp. 977–985, 2015, doi: 10.1016/j.chb.2014.10.010.
34. M. R. Abdmeziem and D. Tandjaoui, "An end-to-end secure key management protocol for e-health applications," Comput. Electr. Eng., vol. 44, pp. 184–197, 2015, doi: 10.1016/j.compeleceng.2015.03.030.
35. M. A. Iqbal and M. Bayoumi, "Secure End-to-End key establishment protocol for resource-constrained healthcare sensors in the context of IoT," in 2016 International Conference on High Performance Computing & Simulation (HPCS), 2016, pp. 523–530.
36. K. H. Yeh, "A Secure IoT-Based Healthcare System with Body Sensor Networks," IEEE Access, vol. 4, pp. 10288–10299, 2016, doi: 10.1109/ACCESS.2016.2638038.
37. K. Shankar, M. Elhoseny, E. D. Chelvi, S. K. Lakshmanaprabu, and W. Wu, "An Efficient Optimal Key Based Chaos Function for Medical Image Security," IEEE Access, vol. 6, pp. 77145–77154, 2018, doi: 10.1109/ACCESS.2018.2874026.
38. Citrin et al., "Developing and deploying a community healthcare worker-driven, digitally- enabled integrated care system for municipalities in rural Nepal," Healthcare, vol. 6, no. 3, pp. 197–204, 2018, doi: https://doi.org/10.1016/j.hjdsi.2018.05.002.
39. K. Fan et al., "Blockchain-based secure time protection scheme in IoT," IEEE Internet Things J., vol. 6, no. 3, pp. 4671–4679, 2019, doi: 10.1109/JIOT.2018.2874222.
40. S. F. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, "LACO: Lightweight Three-Factor Authentication, Access Control and Ownership Transfer Scheme for E-Health Systems in IoT," Futur. Gener. Comput. Syst., vol. 96, pp. 410–424, 2019, doi: https://doi.org/10.1016/j.future.2019.02.020.
41. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," Sensors (Switzerland), vol. 19, no. 2, pp. 1–17, 2019, doi: 10.3390/s19020326.
42. S. M. Ahmed and A. Rajput, Threats to patients' privacy in smart healthcare environment, vol. 2002. Elsevier Inc., 2020.
43. W. Chadwick et al., "A cloud-edge based data security architecture for sharing and analyzing cyber threat information," Futur. Gener. Comput. Syst., vol. 102, pp. 710–722, 2020, doi: https://doi.org/10.1016/j.future.2019.06.026.
44. M. Shamim Hossain, G. Muhammad, S. M. M. Rahman, W. Abdul, A. Alelaiwi, and A. Alamri, "Toward end-to-end biomet rics-based security for IoT infrastructure," IEEE Wirel. Commun., vol. 23, no. 5, pp. 44–51, 2016, doi: 10.1109/MWC.2016.7721741.
45. M. Brindha, "Confidentiality, integrity and authentication of DICOM medical images," in 2018 2nd International Conference on Inventive Systems and Control (ICISC), 2018, pp. 71–75, doi: 10.1109/ICISC.2018.8398924.

46. X. Cheng et al., "Secure Identity Authentication of Community Medical Internet of Things," IEEE Access, vol. 7, pp. 115966–115977, 2019, doi: 10.1109/ACCESS.2019.2935782.
47. K. Lim, V. Iipinge, K. L. Tan, and N. Hambira, "Design and Development of Message Authentication Process for Telemedicine Application," in 2018 IEEE Conference on Wireless Sensors (ICWiSe), 2018, pp. 23–28, doi: 10.1109/ICWISE.2018.8633289.
48. S. Gull, S. A. Parah, and K. Muhammad, "Reversible data hiding exploiting Huffman encoding with dual images for IoMT based healthcare," Comput. Commun., vol. 163, pp. 134–149, 2020, doi: https://doi.org/10.1016/j.comcom.2020.08.023.
49. Cruz Zapata, J. L. Fernández-Alemán, A. Toval, and A. Idri, "Reusable Software Usability Specifications for mHealth Applications," J. Med. Syst., vol. 42, no. 3, pp. 1–9, 2018, doi: 10.1007/s10916-018-0902-0.
50. Dumka and A. Sah, "Smart ambulance system using concept of big data and internet of things," in Healthcare Data Analytics and Management, Elsevier, 2019, pp. 155–176.
51. T. Wen, R. Liu, L. Liu, W. Qin, L. Li, and J. Gu, "GPU-based volume reconstruction for freehand 3D ultrasound imaging," in 2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), 2017, pp. 3700–3703, doi: 10.1109/EMBC.2017.8037661.
52. Q. Li and H. Zhu, "Multi-authority attribute-based access control scheme in mHealth cloud with unbounded attribute universe and decryption outsourcing," in 2017 9th International Conference on Wireless Communications and Signal Processing (WCSP), 2017, pp. 1–7, doi: 10.1109/WCSP.2017.8171106.
53. P. Chinnasamy and P. Deepalakshmi, "Design of Secure Storage for Health-care Cloud using Hybrid Cryptography," in 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, pp. 1717–1720, doi: 10.1109/ICICCT.2018.8473107.
54. N. A. Azeez and C. Van der Vyver, "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis," Egypt. Informatics J., vol. 20, no. 2, pp. 97–108, 2019, doi: 10.1016/j.eij.2018.12.001.
55. L. Yeh, P. Chen, C. Pai, and T. Liu, "An Energy-Efficient Dual-Field Elliptic Curve Cryptography Processor for Internet of Things Applications," IEEE Trans. Circuits Syst. II Express Briefs, vol. 67, no. 9, pp. 1614–1618, 2020, doi: 10.1109/TCSII.2020.3012448.
56. S. Chauhan, A. Adarsh, B. Kumar, R. Gupta, and J. P. Saini, "Double secret key based medical image watermarking for secure telemedicine in cloud environment," in 2017 40th International Conference on Telecommunications and Signal Processing (TSP), 2017, pp. 626–631, doi: 10.1109/TSP.2017.8076062.
57. J. Carey et al., "The Geisinger MyCode community health initiative: An electronic health record-linked biobank for precision medicine research," Genet. Med., vol. 18, no. 9, pp. 906–913, 2016, doi: 10.1038/gim.2015.187.
58. S. Alshehri, S. P. Radziszowski, and R. K. Raj, "Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption," in 2012 IEEE 28th international conference on data engineering workshops, 2012, pp. 143–146.
59. R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," IEEE Trans. parallel Distrib. Syst., vol. 24, no. 3, pp. 614–624, 2012.
60. Demirkan, "A smart healthcare systems framework," IT Prof., vol. 15, no. 5, pp. 38–45, 2013, doi: 10.1109/MITP.2013.35.
61. A.-M. Rahmani et al., "Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems," in 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), 2015, pp. 826–834.
62. L. Catarinucci et al., "An IoT-aware architecture for smart healthcare systems. IEEE Internet Things J. 2 (6), 515–526 (2015)." 2015.
63. E. Tsiropoulou, I. Ziras, and S. Papavassiliou, "A Game Theoretic Model for Resource Allocation in Multi-Service SC-FDMA Wireless Networks," EAI Endorsed Trans. Mob. Commun. Appl, 2015.
64. R. Basnet, S. Mukherjee, V. M. Pagadala, and I. Ray, "An efficient implementation of next generation access control for the mobile health cloud," in 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), 2018, pp. 131–138, doi: 10.1109/FMEC.2018.8364055.
65. Z. Ying, L. Wei, Q. Li, X. Liu, and J. Cui, "A Lightweight Policy Preserving EHR Sharing Scheme in the Cloud," IEEE Access, vol. 6, pp. 53698–53708, 2018, doi: 10.1109/ACCESS.2018.2871170.
66. Y. Zhang, R. Gravina, H. Lu, M. Villari, and G. Fortino, "PEA: Parallel electrocardiogram-based authentication for smart healthcare systems," J. Netw. Comput. Appl., vol. 117, pp. 10–16, 2018.

67. Y. Zhang, R. H. Deng, G. Han, and D. Zheng, "Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things," J. Netw. Comput. Appl., vol. 123, pp. 89–100, 2018.
68. Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," Inf. Sci. (Ny)., vol. 479, pp. 567–592, 2019.
69. Y. Liu and J. Zhang, "Large — Capacity LSB information hiding scheme based on two-dimensional code," in 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), 2017, pp. 528–532, doi: 10.1109/ICEIEC.2017.8076621.
70. C.-H. Liu and Y.-F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," Comput. Electr. Eng., vol. 59, pp. 250–261, 2017.
71. Abdel-Nabi and A. Al-Haj, "Efficient joint encryption and data hiding algorithm for medical images security," in 2017 8th International Conference on Information and Communication Systems (ICICS), 2017, pp. 147–152, doi: 10.1109/IACS.2017.7921962.
72. P. Tasatanattakool and C. Techapanupreeda, "User authentication algorithm with role-based access control for electronic health systems to prevent abuse of patient privacy," in 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 2017, pp. 1019–1024, doi: 10.1109/CompComm.2017.8322697.
73. D. Thilakanathan, S. Chen, S. Nepal, and R. Calvo, "SafeProtect: Controlled Data Sharing with User-Defined Policies in Cloud-Based Collaborative Environment," IEEE Trans. Emerg. Top. Comput., vol. 4, no. 2, pp. 301–315, 2016, doi: 10.1109/TETC.2015.2502429.
74. N. H. Hussein, "Cloud-Based Efficient and Secure Scheme for Medical Images Storage and Sharing using ECC and SHA-3," in 2019 2nd Scientific Conference of Computer Sciences (SCCS), 2019, pp. 109–115, doi: 10.1109/SCCS.2019.8852620.
75. Zhang, H. Liu, and L. Ni, "A Secure Energy-Saving Communication and Encrypted Storage Model Based on RC4 for EHR," IEEE Access, vol. 8, pp. 38995–39012, 2020, doi: 10.1109/ACCESS.2020.2975208.
76. R. Dalal, "A Novel Hybrid data security algorithm for Electronic Health Records security," in 2019 4th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS), 2019, vol. 4, pp. 1–4, doi: 10.1109/CSITSS47250.2019.9031012.
77. M. Bachiri, A. Idri, J. L. Fernández-Alemán, and A. Toval, "Mobile personal health records for pregnancy monitoring functionalities: Analysis and potential," Comput. Methods Programs Biomed., vol. 134, pp. 121–135, 2016, doi: 10.1016/j.cmpb.2016.06.008.
78. Esposito, "Interoperable, dynamic and privacy-preserving access control for cloud data storage when integrating heterogeneous organizations," J. Netw. Comput. Appl., vol. 108, pp. 124–136, 2018.
79. M. Slim et al., "Healthcare Policy Statement on the Utility of Coronary Computed Tomography for Evaluation of Cardiovascular Conditions and Preventive Healthcare: From the Health Policy Working Group of the Society of Cardiovascular Computed Tomography.," J. Cardiovasc. Comput. Tomogr., vol. 11, no. 5, pp. 404–414, 2017, doi: 10.1016/j.jcct.2017.08.008.
80. S. Patel, N. Singh, and S. Pandya, "IoT based smart hospital for secure healthcare system," Int. J. Recent Innov. Trends Comput. Commun., vol. 5, no. 5, pp. 404–408, 2017.
81. Y. Zhang, D. Zheng, and R. H. Deng, "Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control," IEEE Internet Things J., vol. 5, no. 3, pp. 2130–2145, 2018, doi: 10.1109/JIOT.2018.2825289.
82. Zhang, J. Yu, C. Tian, P. Zhao, G. Xu, and J. Lin, "Cloud storage for electronic health records based on secret sharing with verifiable reconstruction outsourcing," IEEE Access, vol. 6, pp. 40713–40722, 2018, doi: 10.1109/ACCESS.2018.2857205.
83. S. Rahimi Moosavi et al., "SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways," in Procedia Computer Science, 2015, vol. 52, pp. 452–459.
84. M. Janveja et al., "Design of Efficient AES Architecture for Secure ECG Signal Transmission for Low-power IoT Applications," in 2020 30th International Conference Radioelektronika (RADIOELEKTRONIKA), 2020, pp. 1–6, doi: 10.1109/RADIOELEKTRONIKA49387.2020.9092417.B. Riedl, V. Grascher, and T. Neubauer, "A secure e-health architecture based on the appliance of pseudonymization.," JSW, vol. 3, no. 2, pp. 23–32, 2008.
85. Riedl, V. Grascher, and T. Neubauer, "A secure e-health architecture based on the appliance of pseudonymization.," JSW, vol. 3, no. 2, pp. 23–32, 2008.
86. T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A medical healthcare system for privacy protection based on IoT," in 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), 2015, pp. 217–222.

87. S. R. Moosavi et al., "Session resumption-based end-to-end security for healthcare internet-of-things," in 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, 2015, pp. 581–588.
88. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," Inf. Syst., vol. 48, pp. 132–150, 2015.
89. S. R. Moosavi et al., "End-to-end security scheme for mobility enabled healthcare Internet of Things," Futur. Gener. Comput. Syst., vol. 64, pp. 108–124, 2016.
90. Alzubi and A. Sari, "Deployment of hash function to enhance message integrity in wireless body area network (WBAN)," Int. J. Commun. Netw. Syst. Sci., vol. 9, no. 12, p. 613, 2016.
91. S. F. Raza, C. Naveen, V. R. Satpute, and A. G. Keskar, "A proficient chaos based security algorithm for emergency response in WBAN system," in 2016 IEEE Students' Technology Symposium (TechSym), 2016, pp. 18–23, doi: 10.1109/TechSym.2016.7872648.
92. R. Varatharajan, G. Manogaran, M. K. Priyan, and R. Sundarasekar, "Wearable sensor devices for early detection of Alzheimer disease using dynamic time warping algorithm," Cluster Comput., vol. 21, no. 1, pp. 681–690, 2018.
93. A. Kaw, N. A. Loan, S. A. Parah, K. Muhammad, J. A. Sheikh, and G. M. Bhat, "A reversible and secure patient information hiding system for IoT driven e-health," Int. J. Inf. Manage., vol. 45, pp. 262–275, 2019, doi: https://doi.org/10.1016/j.ijinfomgt.2018.09.008.
94. Caracas, T. Kramp, M. Baentsch, M. Oestreicher, T. Eirich, and I. Romanov, "Mote runner: A multi-language virtual machine for small embedded devices," in 2009 Third International Conference on Sensor Technologies and Applications, 2009, pp. 117–125.
95. Pacheco and S. Hariri, "IoT security framework for smart cyber infrastructures," in 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W), 2016, pp. 242–247.
96. S. Pirbhulal et al., "A novel secure IoT-based smart home automation system using a wireless sensor network," Sensors, vol. 17, no. 1, p. 69, 2017.
97. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," Egypt. Informatics J., no. xxxx, 2020, doi: 10.1016/j.eij.2020.07.003.
98. S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," IEEE Access, vol. 5, no. c, pp. 26521–26544, 2017, doi: 10.1109/ACCESS.2017.2775180.
99. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, "Big healthcare data: preserving security and privacy," J. Big Data, vol. 5, no. 1, pp. 1–18, 2018, doi: 10.1186/s40537-017-0110-7.
100. R. Miotto, L. Li, B. A. Kidd, and J. T. Dudley, "Deep Patient: An Unsupervised Representation to Predict the Future of Patients from the Electronic Health Records," Sci. Rep., vol. 6, no. April, pp. 1–10, 2016, doi: 10.1038/srep26094.
101. S. Soman, P. Srivastava, and B. K. Murthy, "Unique Health Identifier for India: An algorithm and feasibility analysis on patient data," in 2015 17th International Conference on E-health Networking, Application & Services (HealthCom), 2015, pp. 250–255, doi: 10.1109/HealthCom.2015.7454507.
102. O. Olakanmi and K. Odeyemi, "FEACS: A fog enhanced expressible access control scheme with secure services delegation among carers in E-health systems," Internet of Things, vol. 12, p. 100278, 2020, doi: https://doi.org/10.1016/j.iot.2020.100278.
103. Shin, S. Yoo, K. H. Lee, and D. Lee, "Electronic Medical Records privacy preservation through k-anonymity clustering method," in The 6th International Conference on Soft Computing and Intelligent Systems, and The 13th International Symposium on Advanced Intelligence Systems, 2012, pp. 1119–1124, doi: 10.1109/SCIS-ISIS.2012.6505046.
104. Singh, U. Lakhina, I. Elamvazuthi, A. Jangra, and A. K. Singh, "Biomedical Data Privacy Enhancement Architecture Based on Multi-Keyword Search Technique," in 2018 International Conference on Intelligent and Advanced System (ICIAS), 2018, pp. 1–6, doi: 10.1109/ICIAS.2018.8540586.
105. Y. H. Sidek and J. T. Martins, "Perceived critical success factors of electronic health record system implementation in a dental clinic context: An organizational management perspective," Int. J. Med. Inform., vol. 107, pp. 88–100, 2017, doi: https://doi.org/10.1016/j.ijmedinf.2017.08.007.
106. Gai, M. Qiu, L. C. Chen, and M. Liu, "Electronic Health Record Error Prevention Approach Using Ontology in Big Data," in 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems, 2015, pp. 752–757, doi: 10.1109/HPCC-CSS-ICESS.2015.168.

107. A. Mohamadali and N. A. Zahari, "The Organization Factors as Barrier for Sustainable Health Information Systems (HIS) – A Review," Procedia Comput. Sci., vol. 124, pp. 354–361, 2017, doi: https://doi.org/10.1016/j.procs.2017.12.165.
108. Kumari and N. K. Gupta, "An Efficient Storage in the cloud &Secure HER Retrieval by using HECC," in 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), 2020, pp. 277–282, doi: 10.1109/CSNT48778.2020.9115749..
109. J. S. Kumar, A. Nair, V. K. R. Raj, S. K. B.J., A. Nair, and R. R. V.K., "Hybridization of RSA and AES algorithms for authentication and confidentiality of medical images," in 2017 International Conference on Communication and Signal Processing (ICCSP), 2017, vol. 2018-Janua, pp. 1057–1060, doi: 10.1109/ICCSP.2017.8286536.
110. J. N. Cheltha and C. Jeba Nega Cheltha, "An innovative encryption method for images using RSA, honey encryption and inaccuracy tolerant system using Hamming codes," in 2017 International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC), 2017, vol. 2018-Janua, pp. 796–799, doi: 10.1109/ICCPEIC.2017.8290475.
111. R. Shahzadi, S. M. Anwar, F. Qamar, M. Ali, and J. J. P. C. Rodrigues, "Chaos Based Enhanced RC5 Algorithm for Security and Integrity of Clinical Images in Remote Health Monitoring," IEEE Access, vol. 7, pp. 52858–52870, 2019, doi: 10.1109/ACCESS.2019.2909554.
112. Bindhu Raj, R. Vandana, B. J. Santhosh Kumar, B. R. L., R. Vandana, and S. K. B.J., "Integrity based Authentication and Secure Information Transfer Over Cloud for Hospital Management System," in 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 2020, no. Iciccs, pp. 139–144, doi: 10.1109/ICICCS48265.2020.9121079.
113. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA Chaos Blend to Secure Medical Privacy," IEEE Trans. Nanobioscience, vol. 16, no. 8, pp. 850–858, 2017, doi: 10.1109/TNB.2017.2780881.
114. Y S. Dahiya and M. Bohra, "Hybrid parallel partial model for robust & secure authentication in healthcare IoT environments," in 2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON), 2017, pp. 239–243, doi: 10.1109/UPCON.2017.8251054. L. Zhang, X. Zhu, J. Ma, Z. Ma, and D. Yuan, "Medical Privacy-preserving Service Recommendation," in ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 2020, pp. 1–6, doi: 10.1109/ICC40277.2020.9148641.
115. Zhang, X. Zhu, J. Ma, Z. Ma, and D. Yuan, "Medical Privacy-preserving Service Recommendation," in ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 2020, pp. 1–6, doi: 10.1109/ICC40277.2020.9148641.
116. Khandge and S. B. Javheri, "Implementation of Security in a Healthcare Cloud using Decoy Technique and Fog Computing Facility," in 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA), 2019, pp. 1–4, doi: 10.1109/ICCUBEA47591.2019.9129057.
117. Y. Winnie, U. E., and D. M. Ajay, "Enhancing Data Security in IoT Healthcare Services Using Fog Computing," in 2018 International Conference on Recent Trends in Advance Computing (ICRTAC), 2018, pp. 200–205, doi: 10.1109/ICRTAC.2018.8679404.
118. E. Bouchti, S. Bahsani, and T. Nahhal, "Encryption as a service for data healthcare cloud security," in 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT), 2016, pp. 48–54, doi: 10.1109/FGCT.2016.7605072.
119. U. Kumar, R. K. Pathak, and A. Kumar, "Handling Secure Healthcare Data Streaming using R2E Algorithm," in 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020, pp. 732–737, doi: 10.1109/ICESC48915.2020.9156006.
120. N. Purnamasari, A. Sudarsono, and P. Kristalina, "Secure Data Sharing Scheme using Identity-based Encryption for e-Health Record," in 2018 International Electronics Symposium on Engineering Technology and Applications (IES-ETA), 2018, pp. 60–65, doi: 10.1109/ELECSYM.2018.8615549.
121. Aldosari, "Patients' safety in the era of EMR/EHR automation," Informatics Med. Unlocked, vol. 9, no. October, pp. 230–233, 2017, doi: 10.1016/j.imu.2017.10.001.
122. J. C. Dagadu, J. Li, F. Shah, N. Mustafa, and K. Kumar, "DWT based encryption technique for medical images," in 2016 13th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2016, pp. 252–255, doi: 10.1109/ICCWAMTIP.2016.8079849.
123. S. K. Bhopi, N. M. Dongre, and R. R. Gulwani, "Binary key based permutation for medical image encryption," in 2016 International Conference on Inventive Computation Technologies (ICICT), 2016, vol. 3, pp. 1–6, doi: 10.1109/INVENTIVE.2016.7830180.
124. Kiran, B. D. Parameshachari, H. T. Panduranga, and S. K. Naveenkumar, "Partial encryption of medical images by dual DNA addition using DNA encoding," in 2017 International Conference on

Recent Innovations in Signal processing and Embedded Systems (RISE), 2017, pp. 310–314, doi: 10.1109/RISE.2017.8378172.

125. Boussif, N. Aloui, and A. Cherif, "Smartphone application for medical images secured exchange based on encryption using the matrix product and the exclusive addition," IET Image Process., vol. 11, no. 11, pp. 1020–1026, 2017, doi: 10.1049/iet-ipr.2017.0229.
126. M. Boussif, N. Aloui, and A. Cherif, "Securing DICOM images by a new encryption algorithm using Arnold transform and Vigenère cipher," IET Image Process., vol. 14, no. 6, pp. 1209–1216, 2020, doi: 10.1049/iet-ipr.2019.0042atform. IEEE J. Biomed. Heal. Informatics 22, 1711–1719 (2018).