J Med Syst (2016) 40: 155
DOI 10.1007/s10916-016-0509-2

SYSTEMS-LEVEL QUALITY IMPROVEMENT

Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges

Anam Sajid[1] · **Haider Abbas**[2,3]

Received: 12 January 2016 / Accepted: 25 April 2016 / Published online: 7 May 2016

Abstract The widespread deployment and utility of Wireless Body Area Networks (WBAN's) in healthcare systems required new technologies like Internet of Things (IoT) and cloud computing, that are able to deal with the storage and processing limitations of WBAN's. This amalgamation of WBAN-based healthcare systems to cloud-based healthcare systems gave rise to serious privacy concerns to the sensitive healthcare data. Hence, there is a need for the proactive identification and effective mitigation mechanisms for these patient's data privacy concerns that pose continuous threats to the integrity and stability of the healthcare environment. For this purpose, a systematic literature review has been conducted that presents a clear picture of the privacy concerns of patient's data in cloud-assisted healthcare systems and analyzed the mechanisms that are recently proposed by the research community. The methodology used for conducting the review was based on Kitchenham guidelines. Results from the review show that most of the patient's data privacy techniques do not fully address the privacy concerns and therefore require more efforts. The summary presented in this paper would help in setting research directions for the techniques and mechanisms that are needed to address the patient's data privacy concerns in a balanced and light-weight manner by considering all the aspects and limitations of the cloud-assisted healthcare systems.

Keywords Patient data privacy · Cloud computing · Healthcare cloud data privacy

This article is part of the Topical Collection on *Systems-Level Quality Improvement*

✉ Haider Abbas
hsiddiqui@ksu.edu.sa;
haiderabbas-mcs@nust.edu.pk

[1] Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology (SZABIST), Islamabad, Pakistan

[2] King Saud University, Riyadh, Saudi Arabia

[3] National University of Sciences and Technology, Islamabad, Pakistan

Introduction

The advancements in wireless sensor technologies have made a way to a variety of new applications like enterprise usage, sports, medical, social networking etc. Among these the most promising and influential applications are the electronic healthcare systems. These systems are able to monitor critical health situations, but they rely on WBAN's, which alone are unable to achieve the ultimate goal of the healthcare stakeholders. We require more advanced technologies involved in improving the healthcare systems performance, for this purpose concepts like Internet of Things—IoT and cloud computing can be of benefit [1].

Although for Wireless Sensor Networks—WSN's, security is considered to be a vital aspect, but due to the limitation of resources to these sensors, used by WBAN's, gave rise to the need for moving towards outsourced cloud infrastructures [1, 2]. These outsourced cloud infrastructures, are mostly considered as public clouds, and they manage the healthcare systems data, through a Cloud Service Provider—CSP [3, 4]. The CSP is then responsible for providing data storage services. Hence, for achieving efficiency and mobility in monitoring a patient's health conditions, the healthcare systems deploy both cloud computing and WBAN's together. The cloud healthcare systems are capable of providing scalable solutions which are efficient as well, but has security issues. However, in the name of efficiency, the privacy of healthcare data must not be compromised [5].

Shifting the patients' health data to the cloud improves the data management and efficiency of the healthcare systems, by reducing the costs, providing round the clock availability and scalable health services. However, this shift of healthcare systems to the cloud infrastructure gave rise to critical security and privacy issues related directly to the patients' health data.

One of the top security concerns to the healthcare systems is to provide healthcare data privacy. If the patients involved in the healthcare cloud systems are not ensured about their data's privacy, they will refuse to utilize these beneficial systems. The data related to a patient's health is always considered as sensitive and private [6]. A major issue that is still unsolved is that when data is collected from the WBAN's storage and transit, certain challenges are faced [7]. These challenges have a direct impact on the security and privacy of healthcare data. Therefore, we need to have such solutions that are able to provide healthcare systems data protection by all means.

In order to build such privacy preserving and efficient solutions; first we need to understand the knowledge base of the existing cloud-assisted healthcare systems, with respect to security and privacy of data. By gaining this knowledge it would be easy for the researchers to identify the research gaps, present in the existing work, for improving the healthcare cloud's data privacy. Therefore, a systematic literature review is performed in this study, by following the guidelines of Kitchenham et al. [8], and two important research questions are answered. First, we identified the data privacy concerns in the healthcare cloud and found 13 concerns at an abstract level. Second, we highlighted the techniques and mechanisms that are currently addressing these concerns, along with their benefits and drawbacks.

The rest of the research article is organized as follows: First, the systematic mapping describes the research methodology that is followed in this review. In this section, the research questions are first formalized, and then according to these questions primary studies within the range of 6 years (2010–2015) from five selected electronic sources; Elsevier Journals, IEEE Xplore, Science Direct, ACM Digital Library and Springer Link, based on a pre-defined inclusion and exclusion criteria are selected. After that, the selected sources were assessed according to a quality assessment checklist and thorough screening of texts. Second, the systematic review process with results of the performed review is described in detail, which also includes the answered research questions findings, after performing an extensive and detailed study on the selected primary literature. Third, a thorough analysis of the current literature is presented, that will help the research community to find gaps in the existing approaches and methodologies followed for the improvement of data privacy in healthcare cloud. The results of the review show that, the current practices for addressing patient's data in healthcare cloud still lack in their efficiency and practicality, and identify the areas which require more research efforts. At last, a glimpse of the performed study is provided in the conclusion section.

Systematic mapping

This research follows a systematic literature review approach with the intension of highlighting the privacy concerns of patient's data within the cloud-based health monitoring systems. Further, these identified concerns are then explored in detail, in order to present a clear picture of the mechanisms that are currently being used to address the identified data privacy concerns.

Question formalization

The primary focus of this paper is to highlight the challenges that are being faced in a cloud-based healthcare system that result in the patient's data privacy leakage. In order to keep the research strongly focused, following research questions are carefully formed:

- RQ1: What are the data privacy concerns of cloud-assisted healthcare systems?
- RQ2: What are the data privacy mechanisms in cloud assisted healthcare systems that address the privacy concerns identified in RQ1?

Answer to these questions is based on an extensive search performed for finding high quality research articles, that are published in well reputed sources and are also peer-reviewed, keeping into consideration the guidelines proposed by Kitchenham et al. [8]. The search strictly revolved around these research questions, and following keywords were initially used in the review protocol phase; patient data privacy, cloud computing, healthcare cloud data privacy.

Search strings

In order to refine our search for finding primary literature, search strings were designed. The keywords mentioned above were used exclusively to design the following search strings, as shown in Table 1, for both research questions.

Selection of sources

The primary literature search selection was confined to five electronic sources. These primary studies were searched within the electronic databases using the search strings designed. The electronic databases included are ACM Digital Library, Elsevier Journals, Springer Link, IEEE Xplore and Science Direct. These databases are selected based on the fact that they are peer-reviewed both technically and scientifically. Also that it contains literature of great importance and relevance from key journals and conferences with respect to computer engineering and computer science technology. Primary research article search is confined to 6 years, with range 2010 to 2015.

Table 1 Search strings for research questions

Search strings for RQ1	Search strings for RQ2
Data privacy concerns in cloud-assisted healthcare system	(Cloud-assisted healthcare data privacy techniques) OR (cloud-assisted healthcare data security solution) OR (cloud-assisted healthcare data privacy framework)
Data privacy AND cloud healthcare	(Cloud-assisted healthcare data privacy techniques) OR (cloud-assisted healthcare data security solution) OR (cloud-assisted healthcare data privacy framework)

Inclusion and exclusion criteria

The primary articles searched by following the above mentioned steps has to go through an organized criteria, that will decide whether a research article is included or excluded for this review paper. For this a concise criteria is set as described in Table 2.

Quality assessment checklist

In order to assess the quality of each primary study, the Kitchenham [8] guidelines were followed to develop a quality assessment checklist. The individual primary study was given a "Yes" if it met the above mentioned quality assessment criteria and a "No" otherwise. Table 3 shows the questions that were included in the quality assessment checklist.

Data extraction and synthesis

For extracting the data from each primary study, a form was constructed in MS Excel as presented in Fig. 1. The extracting information was divided into following items for each paper; title of paper, DOI, source of publication, year of publication, author list, patients privacy concerns addressed, methodologies used and its analysis.

Systematic reviewing process and results

In a nutshell, the whole process of our systematic review can be expressed in the form of few basic steps, as shown in Fig. 2.

After structuring the research questions, the relevant search strings were designed and then based on the criteria set for inclusion and exclusion, the primary research articles were selected for the systematic review. Initially, a wide range of papers were found from all the selected electronic databases, but as we filtered them based on the inclusion and exclusion criteria and especially the year of publications, we were left with approximately half of the literature that was being searched at first. In order to refine our selection of papers, these papers were then screened by reading their abstracts, introductions and conclusions. By doing so we got a clear idea of which study is addressing precisely our targeted concern. At last, 55 remaining papers were given a detail oriented full text reading which resulted into the formation of this review, as they fully addressed the research questions mentioned above and also met our quality assessment criteria in a positive manner. Table 4 provides an insight on the final selection of primary literature based on search strings and the Fig. 3 provides a glimpse on the distribution of the selected primary literature with respect to their publications present in ACM Digital Library, Elsevier Journals, Springer Link, IEEE Xplore and Science Direct in the form of few basic steps. Figure 4 depicts year-wise distribution of research work done in each year (2010–2015) for preserving the patient's data privacy in could-assisted healthcare systems.

Addressing the research questions based on selected literature

This section provides detailed information about how the developed research questions were addressed by the selected primary literature.

Table 2 Inclusion exclusion criteria

Inclusion criteria	Exclusion criteria
Literature is within the range of years 2010 to 2015.	Literature that only focuses on BAN's, WBAN's, wireless sensors in healthcare but not cloud-based healthcare systems.
Literature is focused towards cloud-based healthcare systems. They also address data privacy concerns in one way or the other i-e; either they provide knowledge about the privacy and security challenges to patient's healthcare data or they address these challenges through some methodology or architecture.	Literature providing overlapping knowledge and duplicate studies.
	Literature that neither identify nor address any data privacy concern in healthcare cloud in a clear and explicit manner.

Table 3 Quality assessment for studies

Quality assessment questions	Answer
Does the research paper clearly identify its aims and scope?	() Yes
	() No
Does the research paper fully address the claims made in the paper properly?	() Yes
	() No
Is the research methodology presented in the research paper clearly and completely explained?	() Yes
	() No
The method or technique that is addressing the research problem, in the research paper, in parallel with the problem under study?	() Yes
	() No
Is the method or technique being properly analyzed with clear results?	() Yes
	() No

RQ1: What are the patient's data privacy concerns of cloud-assisted healthcare systems?

This question forms the basis of this review. As mentioned in the introduction, the need to preserve the privacy of a patient data who is involved in sharing his/her data in a cloud-based healthcare system, has the most demand and is also a genuine right of patients. Now in order to provide data privacy within these systems, we need to first have a detailed knowledge about the concerns of patient's data privacy. For this we have thoroughly read the selected papers in detail and have come up with a concise view in the form of Fig. 5, which provides an overview of the frequency of patients data privacy concerns identified in the healthcare cloud, and Table 5, that represents what concerns does patient's data have in order to preserve privacy, while limiting this to only cloud-assisted healthcare systems.

A brief explanation to the patient's data privacy concerns in cloud-assisted healthcare systems for both data at rest and data in transit is described below:

Integrity Healthcare data contains sensitive medical information related to patients, which if not provided protection of integrity may cause harm to the patient's life. For example; even a little modification to the patient's prescription or lab reports can have devastating consequences on the patient's life. By maintaining the integrity of data we provide a way to verify that the medical data is not modified by anyone other

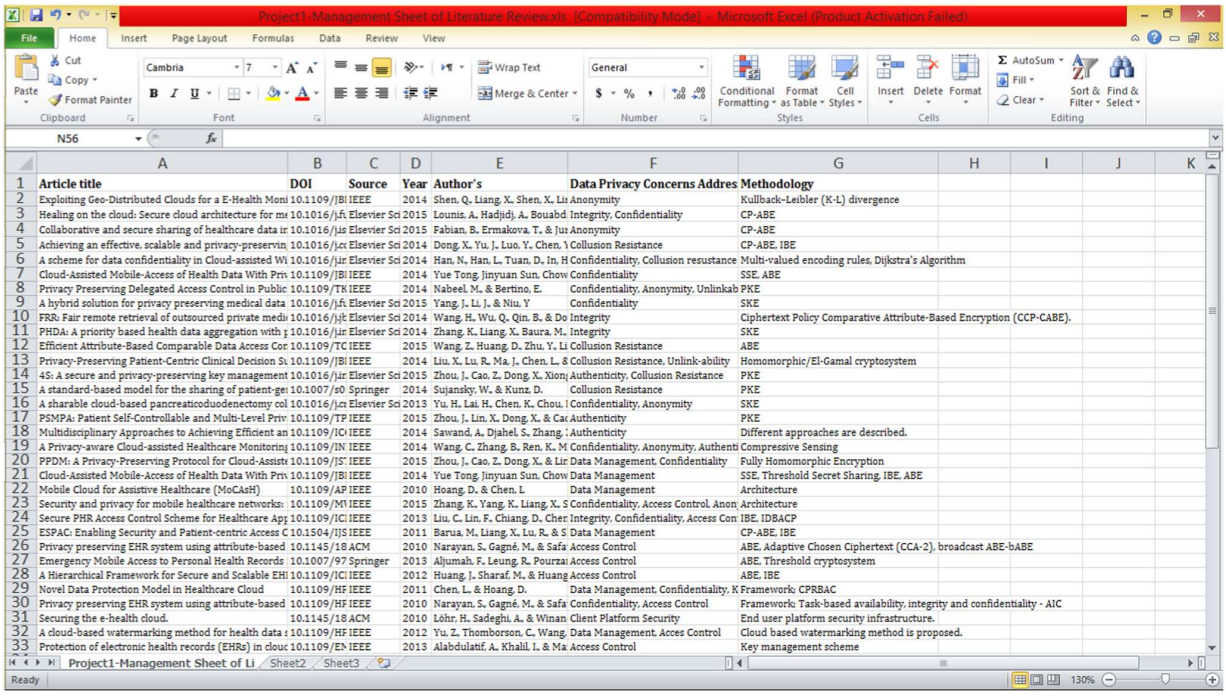

Fig. 1 Data extraction MS excel sheet

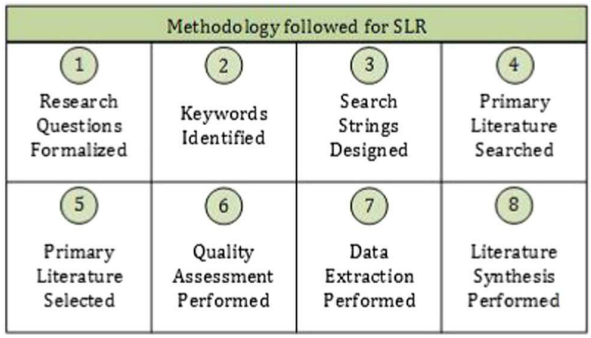

Fig. 2 Steps followed in the SLR

than the concerned person's (i.e. doctors or nurses), and this as a result prevents from giving wrong treatments [2, 10, 15, 16].

Data management The patient's data, to be stored, processed and shared within the cloud healthcare systems, need proper and secure management. The privacy of patient's data can be breached if this data is mismanaged during collection, processing, storage, diagnosis and communication tasks. As the healthcare data is growing there is a demand for such solutions that will maintain the patient data privacy and at the same time maintain low overhead on sensors. There are different kinds of medical data that need to be managed, like digital images, medical reports, diagnostic videos [41], and each data kind requires attention for preservation of privacy.

Confidentiality Another major concern for patient data privacy management is to achieve confidentiality of patient's healthcare data in cloud environment. By maintaining data confidentiality we want to become certain about the contents being disclosed only to the authorized parties, such that the unintended and unauthorized personals are unable to learn the data contents during data storage and data communication [13]. For achieving these privacy concerns; cryptography concepts and encryption primitives are to be followed, such that the overhead on sensors is also managed efficiently [2, 31].

Table 4 Selection of primary literature based on search strings

Source	RQ's	Search by strings	Selected studies
IEEE Xplore	RQ 1	469 for patient data privacy concerns in cloud-assisted healthcare system	21
		54 for patient data privacy AND cloud healthcare	
	RQ 2	70 for (((cloud-assisted healthcare data privacy techniques) OR cloud-assisted healthcare data security solution) OR cloud-assisted healthcare data privacy framework)	
Science Direct/ Elsevier Journals	RQ 1	215 results found for (patient data privacy concerns in cloud-assisted healthcare system).	14
		539 results found for (patient data privacy AND cloud healthcare).	
	RQ 2	384 results found for ((cloud-assisted healthcare data privacy techniques) OR (cloud-assisted healthcare data security solution)) or (cloud-assisted healthcare data privacy framework).	
Springer	RQ 1	933 results for 'patient data privacy AND cloud healthcare'	8
	RQ 2	27 Result(s) for '(cloud-assisted AND healthcare AND data privacy techniques) OR (cloud-assisted AND healthcare AND data security solution) OR (cloud-assisted AND healthcare AND data privacy framework)'	
ACM Digital Library	RQ 1	504 results found. Searched for content.ftsec:(+ patient + data + privacy + concerns + in + cloud-assisted + healthcare + system)	13
		194 results found. Searched for content.ftsec:(patient AND data AND privacy AND cloud AND healthcare)	
	RQ 2	134 results found. Searched for content.ftsec:(cloud-assisted AND healthcare AND data privacy techniques) OR (cloud-assisted AND healthcare AND data security solution)) or (cloud-assisted AND healthcare AND data privacy framework))	
Final selection of primary literature			55

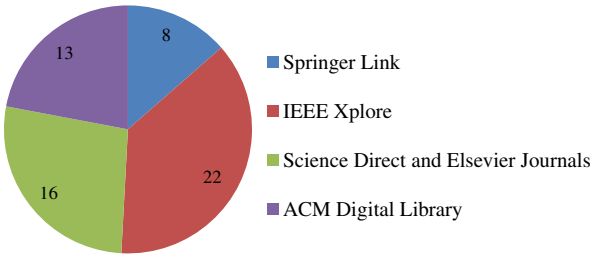

Fig. 3 Distribution of primary literature in selected sources

Access control Patient's data access control is also a growing concern for maintaining the privacy of healthcare data in cloud environment. This is due to the sensitivity of information which the patient's health records possess. The reason for keeping a strong check, on access to these systems, is that generally the patients are very much concerned about where their information is going and who will be able to access their data [30]. For the purpose of controlling such access, a set of access control policies are to be defined. The access policies are complex, but they completely define who can and cannot access a particular set of data. Also that providing such policies which are fine-grained is a challenging task. Certain issues need to be taken into consideration while writing these access policies, such as; overhead, scalability and security management [2].

Keyword and search pattern privacy When healthcare information is being communicated among different parties involved; like healthcare providers, patients, cloud service providers, the data sometimes need to be searched. It is against the privacy concern of a patient that these search patterns and their corresponding keywords are exposed to the unintended personals. This requires that the keywords that are being used for the purpose of searching remain confidential, as sensitive medical information may be a part of these keywords. Despite the fact that, whether the keywords being searched were same or not, the access patterns must never be revealed i.e. the document set of

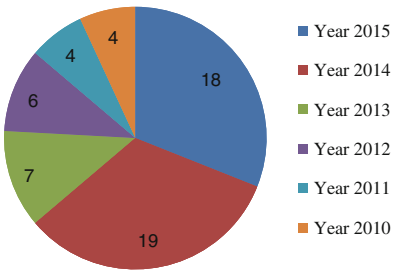

Fig. 4 Year-wise distribution of selected literature addressing RQ1 and RQ2

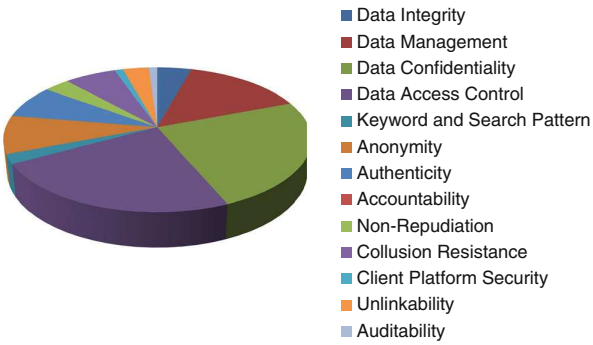

Fig. 5 Frequency of current literature addressing patient's data

which the keyword is a part, must not be exposed [13]. Another benefit is that the cloud service provider will also not be able to perform searches on the encrypted data [31].

Anonymity In order to make the data more secure and to preserve its privacy the anonymization techniques can be utilized in the cloud environment, [9, 11, 13, 20, 23, 44, 49]. By anonymizing data in the cloud healthcare system the main goal is to make the sensitive information hidden, such that a patient's key identity information is not exposed to unintended party. The anonymized data protects its privacy such that a particular individual cannot be linked or associated with his/her corresponding data retrieval or storage process, thereof making these processes as anonymous as possible [13].

Authenticity Authenticity is one of the early process to be performed by any system that requires security and privacy to be preserved. Healthcare systems are no different in this regard, especially when these systems are integrated with the cloud and are holding sensitive medical data. A simple example that describes the need for authentication in healthcare cloud is that, when doctors need to access a particular patient's data which is stored on the cloud, he/she sends a request to the Cloud Service Provider—CSP for that particular data's access. As a result, the CSP has to authenticate the source from such request and then responds accordingly based on the patient's data privacy levels or access control policies [53]. A number of attacks are possible to these systems, if proper authentication procedures are not followed, like; impersonation attack, insider attacks, man-in-the-middle attack, replay attacks, stolen verifier attacks, password guessing attacks etc. [44].

Accountability In order to deal with the dishonest individuals involved in the cloud-based healthcare systems, there is a requirement to make these users accountable for their actions, so that the patient's data privacy can be enhanced and managed effectively. The user accountability problem is quiet new and needs more research attention as well. Patients Health Records—PHR are shared within these systems and there

Table 5 Patient's data privacy concerns in healthcare cloud system present in current literature

Patients data privacy concern's in cloud-assisted healthcare system														
References	Integrity	Data management	Confidentiality	Access control	Keyword and search pattern privacy	Anonymity	Authenticity	Accountability	Non-repudiation	Collusion resistance	Client platform security	Unlink ability	Auditability
[9]						Y							
[10]	Y		Y										
[11]						Y							
[1]										Y			
[12]			Y										
[13]			Y			Y						Y	
[14]			Y										
[15]	Y												
[16]	Y												
[17]										Y			
[18]										Y		Y	
[19]										Y			
[20]			Y			Y							
[21]							Y						
[22]							Y						
[23]			Y			Y	Y						
[24]		Y	Y										
[25]		Y											
[26]		Y											
[13]			Y	Y	Y	Y						Y	Y
[27]		Y											
[28]				Y									
[29]				Y									
[30]				Y									
[31]		Y	Y		Y								
[32]			Y	Y									
[33]		Y	Y	Y									
[34]		Y		Y									
[35]				Y									
[36]											Y		
[37]		Y											
[38]				Y									

Table 5 (continued)

Patients data privacy concern's in cloud-assisted healthcare system

References	Integrity	Data management	Confidentiality	Access control	Keyword and search pattern privacy	Anonymity	Authenticity	Accountability	Non-repudiation	Collusion resistance	Client platform security	Unlink ability	Auditability
[39]		Y											
[40]		Y											
[41]		Y											
[42]			Y	Y				Y					
[43]			Y						Y				
[44]			Y				Y		Y				
[45]			Y	Y									
[46]			Y	Y									
[47]		Y											
[48]				Y									
[49]				Y			Y						
[50]				Y									
[51]				Y									
[52]			Y	Y		Y							
[53]			Y	Y			Y		Y				
[54]		Y	Y										
[55]			Y	Y									
[56]				Y									
[57]		Y											
[58]		Y		Y									
[59]				Y									
[60]						Y							
[61]			Y										

Solutions addressing patient's data privacy concerns in healthcare cloud	Reviews	Analysis
IBE and ABE [31–33, 46, 54–56]	To enforce access policies, IBE and ABE are combined together for secure and scalable access of EHR's between multiple clouds. Drawback: only read access privileges are considered and a secure channel is assumed between trust server and HER owner [33]. Fine-grained access control and data confidentiality is attained. It combines ABE with threshold encryption to provide access to Emergency Care Provider – ECP for PHR's, such that they only view the selected record instead of each record. Drawback: data decryption is dependent on any two parties out of four, among whom the decryption keys were split [32]. Under multi-owner settings fine-grained access control framework is presented by using ABE revocation [55]. Their future work [56] presents Multi-authority ABE and solved key escrow	IBE was proposed after PKE hence the disadvantages of PKE are also present in IBE. ABE is the extension for IBE, in it the attributes of users are used for encrypting data. A drawback of ABE is that it encrypts data for a group of users with no defined group membership. Although the proposed schemes, utilizing ABE and IBE approach, do preserve patient's privacy, but not to the extent required, as their focus is more on providing access to data i.e. who to provide data but not on what to provide from the data.

Table 5 (continued)

Patients data privacy concern's in cloud-assisted healthcare system

References	Integrity	Data management	Confidentiality	Access control	Keyword and search pattern privacy	Anonymity	Authenticity	Accountability	Non-repudiation	Collusion resistance	Client platform security	Unlink ability	Auditability
			problem of [55]. Drawback: both approaches in case of health emergency gave access to all healthcare related data to the ECP.										
CP-ABE and KP-ABE [1, 10, 17, 29, 30]			CP-ABE based construction provides fine-grained access control and confidentiality. Authentications mechanism used are Digital Certificates in an untrusted cloud model. Drawback: has an issue in specifying access policy [10]. CP-ABE for ensuring strong access control on the files related healthcare data stored on the cloud. Minimizing the key management overhead. Drawback: create key escrow issue in semi-trusted cloud [1]. Efficient and Secure Patient Centric Access Control – ESPAC use CP-ABE for cloud-based healthcare and provide patient centric access control, confidentiality and authenticity in trusted cloud. Drawback: if hospital server fails the data won't be able to get processed [7, 30]. Priority based Healthcare Data Aggregation – PBHD methodology preserves the data privacy and the identity during the data is being transmitted from WBAN's in cloud healthcare for this Paillier Cryptosystem is used. Drawback: has key management issue [17].				CP-ABE, KP-ABE both provides data confidentiality and access security, but their proposed solutions need to be strongly protected against other privacy concerns as well. When we combine the encryption, with other privacy preserving techniques, the overhead of communication time and cost increases.				
Privacy preserving data mining – PPDM [26, 40]			Fully homomorphic encryption for data aggregation is used instead of partial homomorphic encryption. This scheme is protective against CCA. Drawback: overhead with respect to time [26]. Data perturbation is used, to deal with the above drawback, and also applied data clustering technique [40].						Fully homomorphic data aggregation method is very new and also meets the desired patient's data privacy requirement. If only, the time overhead is reduced, by doing more research this solution can be of very benefit.				
Healthcare image data privacy protection [37, 47, 48, 57]			Watermarking technique, as an added privacy assuring service, in case, cryptographic control got breached. Drawback: no guarantee for the resilience of the watermark against the modification or removal of data through attacks [37]. Framework, to handle the healthcare data visualization privacy issue in healthcare cloud. Cryptographic secret sharing is integrated with volume ray casting. Drawback: data and computation overhead [47].						The effectiveness and efficiency of image data protection is not stable yet, as the current literature is unable to handle the overhead issues and the feasibility of the watermarking approaches.				
Secure channel free Public-Key Encryption with Keyword Search – PEKS [31]			TA generates keys for the EHR proposed system. SKC is used for encrypting the original data and the broadcast ABE – bABE is used in order to make the accessibility of symmetric key possible. This scheme provides keyword search, user revocation, data privacy and access delegation. For keyword search PEKS is used. Drawback: high computation cost [31].						By using TA the privacy of data can be breached as the TA has control over all the encrypted data keys and can access the patient's data anytime. By using SKE the patient's data privacy cannot be assured fully, as SKE uses single key pair for encrypting and decrypting, hence if the key get compromised the entire data will also be compromised.				
K-anonymity technique [52, 60]			K-anonymization technique for preserving the patients data in cloud healthcare and improve data sharing in this environment. Combines k-anonymization with CP-ABE. This approach divides the data into four types of identifiers and out of them two is anonymized for each patient [52]. To improve k-anonymization new methodology is proposed that combines k-anonymity with l-diversity, t-closeness and ∂-presence [60]. Drawback: in both [52] and [60] information loss is predicted to happen.						User revocation and medical emergency cases are not taken into consideration by [52]. Re-identification risk is handled by [60], which are new and are not considered as yet, by other literature reviewed; however, their scheme needs more research in order to make it a practical solution.				
Patient data privacy preserving schemes in healthcare cloud [27,			Cipher-text Policy Attribute based Signcryption – CP-ABSC framework ensures fine-grained access control and secure sharing of patient's healthcare data on cloud. CP-ABSC provides										

Table 5 (continued)

Patients data privacy concern's in cloud-assisted healthcare system													
References	Integrity	Data management	Confidentiality	Access control	Keyword and search pattern privacy	Anonymity	Authenticity	Accountability	Non-repudiation	Collusion resistance	Client platform security	Unlink ability	Auditability
[34–36, 38, 39, 43, 44, 49, 50, 53, 59]			anonymity, collusion resistance, authenticity and confidentiality. Drawback: for constructing access policies monotone tree policy is used that make policy construction complex [59]. Cryptographically enforced and Privacy Enhanced Scheme – CRYPE combines CP-ABSC with lazy-encryption and proxy re-encryption PRE techniques [53]. Mobile Cloud for Assistive Healthcare – MoCAsH addresses the patient's data privacy, ownership and protection issued in federated Peer to Peer – P2P cloud environment [27]. Drawback: MoCAsH limitations were dealt by [34], by proposing another framework, Cloud-based Privacy Role Based Access Control – CP- RBAC, in order to achieve fine-grained access control, active auditing and data traceability.				The secret key used for signing and decryption key in [59] will linearly grow in size with the number of attributes used for decryption and signing. As compared to the ESPAC scheme [7, 30] the CRYPE [53] has less overhead and decryption time. Both [27] and [34] deal with securing data when it has reached the cloud, but do not discuss about the data privacy assurance while it is in transit.				

are multiple users involved. A dishonest user can leak or share his/her private key credentials with some unauthorized users and by doing so there will be no clue as to who did this. Hence for this reason user accountability is required, as it directly violates the patient's privacy of data [42].

Collusion resistance Another essential patient data privacy requirement in cloud-based healthcare systems is to be collusion resistant. The concept of collusion is very simple, in it more than one party mutually cooperates illegitimately to learn the user's private credentials like their identities or their private medical data. This collusion is considered to be performed among both authorized and unauthorized entities. In order to deal with collusion and make these systems resistant against collusion attacks, we need to limit the possibility of an adversary to learn anything about the patient's data, even if the authorized and unauthorized users managed to collude [1, 6, 7, 17–19].

Client platform security Currently, less work is done on maintaining the security of the software and hardware that is being utilized by the patients and other involved clients within the cloud healthcare system. The patient's healthcare data should also be managed for end-user systems. By end-user system, it is meant; the personal computers, operating systems, network structures and configurations etc., being used by mostly patients and healthcare providers. These systems are not properly managed by the end-user in terms of security. If these systems get compromised then the patient's health record, being stored on these systems, will also lose its privacy, thereof leaving these systems open to attacks and data disclosure as a result [36].

Unlinkability The patient's data privacy would be highly affected if somehow an adversary manages to link multiple healthcare data files and create a profile for that user. For this random file identifier would help to preserve privacy of such data, creating unlinkability and at the same time not leaking any useful information [13]. Therefore, the main goal of maintaining unlinkability is that an adversary is unable to deduce or conclude any relationships among the patient's identification information e.g. name, contact details, social security number etc. and the health data e.g. medical history, lab reports, diagnosis, treatments etc. [13, 26].

Non-repudiation The privacy of a patient needs to be protected from more than one direction. If the healthcare system is accessed by authenticated users, still there need to be a way to keep the authenticated users actions on a constant check. For this we require non-repudiation such that an entity is unable to deny his or her authenticity of signature over a particular set of documents or messages, made by them.

Auditability Auditability is the least addressed privacy concern to patient's healthcare data in the cloud environment. The need to track the access activities, performed by the authorized parties, after going through a fine-grained authorization, arises mostly in the medical emergency cases. During emergency, the patients are not convinced for granting access to their PHR, because the patients are not sure about the legitimacy of the Emergency Medical Care—EMC provider. For this reason an audit is required, so that if the EMC tries to misuse the patient's data he/she can be tracked [13].

RQ2: What are the patient's data privacy mechanisms in cloud assisted healthcare systems that address the privacy concerns identified in RQ1

In order to answer RQ2 we have read the selected papers in depth and found a wide number of solutions and methodologies that are proposed for addressing the patient's data privacy concerns in cloud-assisted healthcare systems identified in RQ1. This section gives insight knowledge on the study conducted for RQ2, in which we have divided the proposed methodologies into multiple sections depending on the privacy concerns that they address. For this, few recent mechanisms are described in brief below, highlighting their strengths and weaknesses, and addressing patient's data privacy mechanisms for both, data at rest and on transit.

Mechanisms dealing with patient data integrity in cloud-assisted healthcare systems Yang et al. [15] presents a hybrid approach for preserving the healthcare data's privacy, which is being shared within the cloud. The authors use the concept of cryptography and follow a statistical analysis in their proposed model and as a result ensure multi-level privacy. The Electronic Medical Record—EMR attributes of identification e.g. name and contact information, are all encrypted using symmetric key encryption. In this model the medical data is partitioned vertically and on each partition a different level of security is implemented, due to this the data also becomes unlinkable by an adversary. Also remote and local data integrity is ensured by the data recipients and data owners. However, the CSP, who is the data recipient in the proposed model, can act maliciously and as a result disclose the patient information.

Wang et al. [16] proposed a scheme to prevent the tempering efforts on healthcare data that is outsourced to some third party servers, in the cloud environment. In the proposed scheme, an independent outsourced third-party is given the responsibility of maintaining the healthcare data integrity. Public Key Encryption—PKE and Diffie-Hellman key exchanges are used, for exchanging the keys in a secure manner. Homomorphic verifiable tags are used to ensure that computations are performed on the data which is encrypted. However, there is a possibility of performance issues to be faced, as larger encrypted texts are processed by the homomorphic encryption.

Lounis et al. [10] proposed architecture for healthcare Wireless Sensor Network—WSN which is cloud-based and addresses the concern for maintaining the integrity of outsourced medical data, its collection and secure access. They used the Attribute Based Encryption—ABE and Symmetric Key Cryptography – SKC, to deal with the problem of accessing the data and also provide fine-grained access control. The healthcare data files in the proposed architecture are encrypted, before storing them on the cloud using SKE and further these keys are made secure through ABE. However, this approach has a potential of facing management issues, as the policies for access can change due to access revocation.

Mechanisms dealing with patient data confidentiality in cloud-assisted healthcare systems Thilakanathan et al. [6] proposed a platform to remotely monitor and securely exchange the patient's healthcare data in cloud assisted healthcare systems. They implemented a security protocol by using a proxy re-encryption technique based on El-Gamal approach. Transmission of the healthcare data from a patient to its consumers is made secure by this protocol. By using proxy re-encryption the encrypted data, that was generated by using a patients (or data owners) public key, gets translated by some semi-trusted party into an encrypted text, which can only decrypt by private key of another user. Although the proposed solution makes the systems collusion resistant and ensures easy revocation, but it does not provide much support for access policies that are complex.

Similarly, Han et al. [12] proposed work focuses on the secure communication that occurs between the cloud and the WBAN's in healthcare systems. The patient's data confidentiality is ensured in the proposed scheme, for this purpose they also utilize Dijkstra's algorithm and the concept of multi-value rules for encoding. However, as Dijkstra's algorithm is not time efficient, hence this scheme would have high overhead in terms of encryption and decryption, which is not acceptable to the healthcare sensitive data systems.

A Two Layer Encryption—TLE technique is employed by [14]. In this technique the two layers of encryption are; fine-grained encryption and coarse-grained encryption. The cloud implements fine-grained encryption whereas the coarse-grained encryption is performed by the data owner. The message is encrypted by employing a broadcast encryption methodology and is then transmitted to users. The subsets of users, who satisfy the particular access policy, are distributed messages, by using Oblivious Commitment Based Envelop—OCBE protocol. By using this methodology, attribute management overhead is reduced at the data owners end and new and revoked members are managed effectively.

However, key escrow problem is created in the proposed approach which can result into misuse of keys by others.

Mechanisms dealing with patient data management in cloud-assisted healthcare systems A cloud-based healthcare monitoring system is proposed by Wang et al. [25], which ensure to maintain patient's privacy of data, while at the same time reducing the overhead on sensors in processing ever-growing data, by using compressive sensing technique. In this approach to protect the data privacy, the sensitive samples acquired from sensor nodes never leave in unprotected form. The authors of this study theoretically prove that their proposed approach provide computational saving, minimizes the cost of communication for data acquisition and its transmission through sensors and it is capable of achieving robust and effective image recovery as well. However, their study does not provide a clear picture for describing that, how the systems will be made secure and what encryption scheme would be used, that will have a direct impact on the frequency of overhead on the sensors and on the overall performance and efficiency of the system.

For providing efficient and secure solution for managing healthcare data Zhou et al. [26] proposed a scheme called Privacy Preserving Data Mining—PPDM protocol for cloud-based healthcare system. They use the fully homomorphic data aggregation concept instead of using partial homomorphic data aggregation. The reason for using fully homomorphic concept is that, in order to manage dynamic health data we need such data aggregation encryption strategy that supports both multiplication and addition of operations. The proposed scheme provides protection against Chosen Cipher text Attack – CCA. However, fully homomorphic encryption is considered to be a new solution for sensitive healthcare data and its processing is time consuming. In order to deal with the PPDM problem a privacy preserving technique is proposed by Huang et al. [40], which utilizes the concept of data perturbation combined with data clustering technique.

To make the data privacy of patient's more secure and manageable another recent approach is proposed by Yu et al. [37], which use the concept of watermarking. The authors claim that for mitigating; in specific insider threats apart from other threats, cloud-based watermarking can be followed, which will be an inexpensive solution as compared to encryption strategies. For this purpose, in the service layer of the cloud, a watermarking process is applied, such that, the medical accuracy and the functional efficiency of the medical health record of patient is not compromised. This approach is considered to be a second line of defense, in case, when the already existing cryptographic mechanisms applied on the healthcare cloud data are breached. However, as this technique is recently proposed so more research is required. Also that, its performance, effectiveness and usability has not been evaluated by the authors [37].

Mohanty et al. [47] presents a framework, that focus on, the secure healthcare data visualization in cloud-assisted systems. The aim is to protect the color coded medical data information and details from an adversary, who has an access to the cloud data center. For this purpose, a volume ray casting pipeline is utilized, that securely hides the healthcare image data's color-coded information. However, the authors of [47] state that their proposed approach has computational overhead and data overhead involved, and it needs to be investigated and researched further.

Mechanisms dealing with patient data access control in cloud-assisted healthcare systems Liu et al. [29] proposed an access control scheme for patient healthcare record in cloud environment. The core concept of this scheme is based on Identity Based Encryption—IBE and bilinear pairing. This scheme developed an access control matrix, which will contain the access permissions for the users and files. The policy is named as Identification Based Access Control Policy – IDBACP. This approach uses a Trusted Authority—TA or a Certification Authority – CA for the secure management of keys. However, these authorities are given the right to use data regularly, which is against the patient's data privacy.

To enhance the access policies Li et al. [56] provides a practical framework for providing fine-grained access control of patient's healthcare data in cloud systems. For this they adopt the concept of Multi-authority Attribute Based Encryption—MA-ABE, but their proposed solution does not deal with the key escrow problem. To solve this issue the authors proposed an enhancement to their MA-ABE framework in [55], which also analyzes the scalability and complexity of this system. However, both proposed studies are unable to maintain the privacy of patient's data in case of medical emergency.

Mechanisms dealing with patient's data keyword and search pattern privacy in cloud-assisted healthcare systems In order to preserve patient's data, searches need to be performed on encrypted data, for this reason Narayan et al. [31] adopts secure channel free Public-key Encryption with Keyword Search – PEKS. Although the data privacy is achieved in performing search tasks, but as this methodology uses a Trust Authority—TA for key management, hence the TA has full access capability to all the encrypted data.

Similarly Tong et al. [13] uses the concept of Searchable Symmetric Encryption—SSE, in order to perform search tasks over encrypted data, but has storage overhead that is linear with the amount of healthcare data files being outsourced.

Mechanisms dealing with patient data anonymity in cloud-assisted healthcare systems For geographically distributed cloud healthcare systems a traffic shaping algorithm is employed by Shen et al. [9]. The health related and non-

health related data is distributed equally by this algorithm. For anonymization purpose the authors used Kullback–Leibler (K-L) divergence entropy measurement. However this approach has the limitation of high delays in communication.

Another similar approach is proposed by Zhou et al. [20] in that they group the patients who are suffering from similar health issues in cloud-based WBAN's. In order to maintain anonymity, identity blinding matrices were used; however their proposed solution is unable to handle the insider threats to the keys and healthcare data.

K-anonymization technique is proposed by Mohandas et al. [52], in which they ensure not only that who access the patient's data, but also that which part of data becomes visible to them. For this, they combine ABE with k-anonymization technique. However, this approach does not deal with user revocation. According to Thilakanathan et al. [60], k-anonymization technique has a drawback associated with it. K-anonymity is unable to prevent the sensitive attribute disclosure. For this they propose an approach to deal with the re-identification risk issue. Their solution is based on k-anonymity combined with l-diversity, t-closeness and ∂-presence and for its implementation ARX anonymization tool is used. Even though their approach reduce the re-identification, however great information loss was observed due to the distortion of data.

Mechanisms dealing with patient data authenticity in cloud-assisted healthcare systems In [21] for ensuring authenticity of healthcare cloud systems, a model is presented which allows the patients to have access control of their data. In this model, the messages that are received by the patients are signed by the sending entities. The digital signatures and message encryption are accomplished by using protocols based on Public Key Infrastructure—PKI. However, their approach does not specify about the level of trust made on the CA, hence data tempering is possible.

Health Personal Cards – HPC are used for the authentication of new physicians by Yu et al. [22], and for the existing physicians the healthcare data access is provided through a secure protocol like Secure Socket Layer—SSL. Eavesdropping is reduced; however this approach has interoperability issues.

Mechanisms dealing with patient data accountability in cloud-assisted healthcare systems A Multi-authority Cipher-text Policy ABE is a scheme proposed by Xhafa et al. [42], which also imposes user accountability for the healthcare cloud based systems. A Black Box model is used for ensuring the attribute private key with some additional information specific to a user. However, while analyzing the performance of the proposed scheme, only time consuming operation exponentiation and pairing are considered.

Mechanisms dealing with non-repudiation of patient data in cloud-assisted healthcare systems Chen et al. [44] presents a protocol for securely exchanging the healthcare data in cloud environment. They use Symmetric Key Encryption—SKE for protecting patient's data and bilinear pairing based mutual authentication for achieving non-repudiation, as well as other data security and privacy benefits. However, their approach has some limitations that were removed by their future work [43], in that the authors use the concept of Elliptic Curve Digital Signature Algorithm—ECDSA in specific for achieving non-repudiation in the healthcare cloud systems, SHA-256 hash function and the AES encryption in their implementation. However both [44] and [43] impose computational overhead on the sensors.

Mechanisms dealing with collusion resistance of patient data in cloud-assisted healthcare systems Dong et al. [1] provides a scheme which is able to resist the collusion attacks by a CSP who is supposed to be semi-trusted. They use ABE and IBE techniques that minimized the key management overhead, but gave rise to the key escrow problem. Similarly, other techniques are also provided in literature, [6, 7, 13, 17–19], with drawbacks of key management issue, access control issues, computational overhead and single point failure of data servers.

Mechanisms dealing with client platform used for patient data in cloud-assisted healthcare systems Very less work is done for managing the patient's data at the user's or client's end-systems. Lohr et al. [36] proposed a preliminary architecture, which creates separate privacy domains for patient's healthcare data. According to the authors, their approach will be easy to integrate with legacy systems and the data's privacy is preserved by Trusted Virtual Domains—TVD. However, their approach is unprotected against viruses that can be induced into the system simply by a USB.

Mechanisms dealing with auditability and linkability of patient data in cloud-assisted healthcare systems Tong et al. [13] addresses the patient's health records auditability and unlinkability. For this purpose they build privacy into the cloud-based healthcare systems by creating a private cloud. This is achieved by combining the concept of threshold signing with ABE, to provide a role based access control integrated with auditability. Unlinkability is achieved by maintaining the keys, using pseudorandom number generator. However, this approach has communication and storage overhead. Similarly, Tong et al. [13] and Wang et al. [18] also provide solutions for maintaining the unlinkability of data in healthcare cloud, but each proposed approach has drawbacks of its own.

Analysis and potential futuristic research

Our goal in this systematic literature review is to provide the readers with a concise view of the patient's data privacy concerns being faced in recent research, to healthcare cloud environment. After performing an extensive and detailed review, we analyzed our study and created a table that will give a brief overview of our analysis, as shown in Table 5.

The results of analysis, performed for the reviewed literature, show that, most focus of research is on providing fine-grained access control to the patient's data in healthcare cloud and after that on maintaining confidentiality. The least addressed concerns are auditability, unlinkability, client platform security, non-repudiation, accountability, integrity, keyword and search pattern privacy and anonymization.

It is clear from the designed table, that ABE and IBE, along with their variants are the most applied solutions for achieving healthcare cloud data privacy. However, their major focus is on the access control and its related policies. Fully homomorphic encryption is considered to be a new approach for maintaining data privacy in these systems, but they follow time consuming computations. Use of PKE and SKE in healthcare data privacy assurance provided unwanted results; like high computation and time overhead's and key management issues. As healthcare data is of many kinds, hence, image and video protection efforts are also made, for example using watermarking techniques, but their efficiency and practicality is yet to be proved.

All the proposed solutions, for preserving the healthcare data's privacy in the cloud environment, studied within the scope of this systematic review, seem to be very promising solutions at first glance, however, on further analysis and comparison, the actual facts are revealed, which proves that, there remains a research gap that needs to be filled in order to make the healthcare cloud data more privacy ensured.

We can now have a clear idea as to which aspects of data privacy in healthcare cloud need further research and investigation. One aspect could be that; instead of using one methodology or solution; like only ABE, we should focus on multi-technology approach; this will focus on combining multiple solutions to achieve the fine-grained privacy preserved efficient and scalable solutions for maintaining the healthcare's data securely in the cloud environment.

Conclusion

The review presented in this paper was conducted systematically by following the guidelines of Kitchenham et al. [8]. All the steps presented in the guidelines were carefully applied to our research. As a result, it helped to find precise answers to our defined research questions. The patient's data privacy concerns were identified and their corresponding mechanisms were also found from the selected literature. The review revealed the fact that, the most applied technique to address the patient's data privacy concerns in healthcare cloud are IBE, ABE and its variants. Other techniques, that do not use any encryption strategy, are based on theoretical models and frameworks, hence are not applied in real world scenario.

There is a need to improve the existing security mechanisms, which deal with maintaining and achieving patient's data privacy in cloud-assisted healthcare systems. As all the mechanisms that are discussed in this review have some drawback involved, this makes them not the one perfect choice for achieving the patient's data privacy concerns in cloud-assisted healthcare systems. Each proposed technique addresses two or three patient's data privacy concerns and fail to consider other patient's data privacy concerns in cloud-assisted healthcare systems. If, on one hand, a technique is achieving confidentiality perfectly, then, on the other hand, it is reducing the systems efficiency by increasing overhead on the system. Also that there are many studies performed in order to secure telecare medical information systems [62, 63] and WBAN-based healthcare system [64, 65], but they do not seem to provide promising solutions for cloud-assisted healthcare data privacy. We, not only require complete solutions for preserving patient's data privacy in normal health related cases, but also for healthcare emergency cases as well. Therefore, in simple words we conclude that, patient's data privacy in healthcare cloud needs balanced solutions, which are able to manage the patient's data privacy while keeping all aspects of the healthcare cloud system into consideration.

Acknowledgments The authors would like to extend their sincere appreciation to the Deanship of Scientific Research at King Saud University for its funding of this research through the Research Group Project no. RG-1435-048.

References

1. Dong, X., Yu, J., Luo, Y., Chen, Y., Xue, G., and Li, M., Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing. *Comput. Sec.* 42:151–164, 2014. doi:10.1016/j.cose.2013.12.002.
2. Othman, S., Bahattab, A., Trad, A., and Youssef, H., Secure data transmission protocol for medical wireless sensor networks. *AINA '14 Proc. 2014 I.E. 28th Int. Conf. Adv. Inform. Networking Appl.* 649–656, 2014. doi:10.1109/AINA.2014.80.
3. Divi, K., and Liu, H., Modeling of WBAN and cloud integration for secure and reliable healthcare. *Proc. 8Th International Conf. Body Area Networks*. 128–131, 2013. doi:10.4108/icst.bodynets.2013.253706.
4. Waqar, A., Raza, A., Abbas, H., and Khurram Khan, M., A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata. *J. Network Comput. Appl.* 36(1):235–248, 2013. doi:10.1016/j.jnca.2012.09.001.
5. Wooten, R., Klink, R., Sinek, F., Bai, Y., and Sharma, M., Design and implementation of a secure healthcare social cloud system.

2012 12Th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput. (Ccgrid 2012). 805–810, 2012. doi:10.1109/CCGrid.2012.131.

6. Javadi, S., and Razzaque, M., Security and privacy in wireless body area networks for health care applications. *Sign. Commun. Technol*. 165–187, 2013. doi:10.1007/978-3-642-36169-2_6.
7. Li, M., Lou, W., and Ren, K., Data security and privacy in wireless body area networks. *IEEE Wireless Commun.* 17(1):51–58, 2010. doi:10.1109/mwc.2010.5416350.
8. Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., and Linkman, S., Systematic literature reviews in software engineering—a systematic literature review. *Inform. Software Technol.* 51(1):7–15, 2009. doi:10.1016/j.infsof.2008.09.009.
9. Shen, Q., Liang, X., Shen, X., Lin, X., and Luo, H., Exploiting geo-distributed clouds for a e-health monitoring system with minimum service delay and privacy preservation. *IEEE J. Biomed. Health Inform.* 18(2):430–439, 2014. doi:10.1109/JBHI.2013.2292829.
10. Lounis, A., Hadjidj, A., Bouabdallah, A., and Challal, Y., Healing on the cloud: Secure cloud architecture for medical wireless sensor networks. *Futur. Gener. Comput. Syst.* 55:266–277, 2015. doi:10.1016/j.future.2015.01.009.
11. Fabian, B., Ermakova, T., and Junghanns, P., Collaborative and secure sharing of healthcare data in multi-clouds. *Inf. Syst.* 48: 132–150, 2015. doi:10.1016/j.is.2014.05.004.
12. Han, N., Han, L., Tuan, D., In, H., and Jo, M., A scheme for data confidentiality in cloud-assisted wireless body area networks. *Inf. Sci.* 284:157–166, 2014. doi:10.1016/j.ins.2014.03.126.
13. Tong, Y., Sun, J., Chow, S., and Pan, L., Cloud-assisted mobile-access of health data with privacy and auditability. *IEEE J. Biomed. Health Inform.* 18(2):419–429, 2014. doi:10.1109/JBHI.2013.2294932.
14. Nabeel, M., and Bertino, E., Privacy preserving delegated access control in public clouds. *IEEE Trans. Knowl. Data Eng.* 26(9): 2268–2280, 2014. doi:10.1109/tkde.2013.68.
15. Yang, J., Li, J., and Niu, Y., A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Futur. Gener. Comput. Syst.* 43–44:74–86, 2015. doi:10.1016/j.future.2014.06.004.
16. Wang, H., Wu, Q., Qin, B., and Domingo-Ferrer, J., FRR: Fair remote retrieval of outsourced private medical records in electronic health networks. *J. Biomed. Inform.* 50:226–233, 2014. doi:10.1016/j.jbi.2014.02.008.
17. Zhang, K., Liang, X., Baura, M., Lu, R., and Shen, X., PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs. *Inf. Sci.* 284:130–141, 2014. doi:10.1016/j.ins.2014.06.011.
18. Wang, Z., Huang, D., Zhu, Y., Li, B., and Chung, C., Efficient attribute-based comparable data access control. *IEEE Trans. Comput.* 64(12):3430–3443, 2015. doi:10.1109/tc.2015.2401033.
19. Liu, X., Lu, R., Ma, J., Chen, L., and Qin, B., Privacy-preserving patient-centric clinical decision support system on naive Bayesian classification. *IEEE J. Biomed. Health Inform.* 20(2):655–668, 2015. doi:10.1109/jbhi.2015.2407157.
20. Zhou, J., Cao, Z., Dong, X., Xiong, N., and Vasilakos, A., 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. *Inf. Sci.* 314:255–276, 2015. doi:10.1016/j.ins.2014.09.003.
21. Sujansky, W., and Kunz, D., A standard-based model for the sharing of patient-generated health information with electronic health records. *Personal Ubiquitous Comput.* 19(1):9–25, 2014. doi:10.1007/s00779-014-0806-z.
22. Yu, H., Lai, H., Chen, K., Chou, H., Wu, J., Dorjgochoo, S., et al., A sharable cloud-based pancreaticoduodenectomy collaborative database for physicians: Emphasis on security and clinical rule supporting. *Comput. Methods Programs Biomed.* 111(2):488–497, 2013. doi:10.1016/j.cmpb.2013.04.019.
23. Zhou, J., Lin, X., Dong, X., and Cao, Z., PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing system. *IEEE Trans. Parallel Distrib. Syst.* 26(6):1693–1703, 2015. doi:10.1109/tpds.2014.2314119.
24. Sawand, A., Djahel, S., Zhang, Z., and Na¨ıt-Abdesselam, F., Multidisciplinary Approaches to achieving efficient and trustworthy eHealth monitoring systems. IEEE/CIC ICCC 2014 *Symp. Privacy Sec. In Commun* 187–192, doi:10.1109/ICCChina.2014.7008269.
25. Wang, C., Zhang, B., Ren, K., M. Roveda, J., Wen Chen, C., and Xu, Z., A privacy-aware cloud-assisted healthcare monitoring system via compressive sensing. *IEEE INFOCOM 2014 - IEEE Conf. Comput. Communi*. 2130–2138, 2014. doi:10.1109/INFOCOM.2014.6848155.
26. Zhou, J., Cao, Z., Dong, X., and Lin, X., PPDM: A privacy-preserving protocol for cloud-assisted e-healthcare systems. *IEEE J. Sel. Top. Sign. Process* 9(7):1332–1344, 2015. doi:10.1109/jstsp.2015.2427113.
27. Hoang, D., and Chen, L., Mobile Cloud for Assistive Healthcare (MoCAsH). *2010 I.E. Asia-Pacific Serv. Comput. Conf*. 325–332, 2010. doi:10.1109/APSCC.2010.102.
28. Zhang, K., Yang, K., Liang, X., Su, Z., Shen, X., and Luo, H., Security and privacy for mobile healthcare networks: from a quality of protection perspective. *IEEE Wireless Commun* 22(4):104–112, 2015. doi:10.1109/mwc.2015.7224734.
29. Liu, C., Lin, F., Chiang, D., Chen, T., Chen, C., and Lin, H. et al., Secure PHR access control scheme for healthcare application clouds. *2013 42Nd Int. Conf. Parallel Process*. 1067–1076, 2013. doi: 10.1109/icpp.2013.127.
30. Barua, M., Liang, X., Lu, R., and Shen, X., ESPAC: Enabling security and patient-centric access control for eHealth in cloud computing. *Int. J. Sec. Networks* 6(2/3):67–76, 2011. doi:10.1504/ijsn.2011.043666.
31. Narayan, S., Gagné, M., and Safavi-Naini, R., Privacy preserving EHR system using attribute-based infrastructure. *Proc. 2010 ACM Workshop Cloud Comput. Sec. Workshop - CCSW '10*. 47-52, 2010. doi:10.1145/1866835.1866845
32. Aljumah, F., Leung, R., Pourzandi, M., and Debbabi, M., Emergency mobile access to personal health records stored on an untrusted cloud. *Health Inform. Sci*. 30–41, 2013. doi:10.1007/978-3-642-37899-7_3.
33. Huang, J., Sharaf, M., and Huang, C., A hierarchical framework for secure and scalable ehr sharing and access control in multi-cloud. *2012 41St Int. Conf. Parallel Process. Workshops*. 279–287, 2012. doi: 10.1109/icppw.2012.42.
34. Chen, L., and Hoang, D., Novel data protection model in healthcare cloud. *2011 I.E. Int. Conf. High Perform. Comput. Commun*. 550–555, 2011. doi: 10.1109/hpcc.2011.148.
35. Narayan, S., Gagné, M., and Safavi-Naini, R., Privacy preserving EHR system using attribute-based infrastructure. *Proc. 2010 ACM Workshop Cloud Comput. Sec. Workshop - CCSW '10*. 47–52, 2010. doi:10.1145/1866835.1866845.
36. Löhr, H., Sadeghi, A., and Winandy, M., Securing the e-health cloud. *Proc. ACM Int. Conf. Health Inform. - IHI '10*. 220–229, 2010. doi: 10.1145/1882992.1883024.
37. Yu, Z., Thomborson, C., Wang, C., Wang, J., and Li, R., A cloud-based watermarking method for health data security. *2012 Int. Conf. High Perform. Comput. Simulation (HPCS*. 642–647, 2012. doi: 10.1109/hpcsim.2012.6266986.
38. Alabdulatif, A., Khalil, I., and Mai, V., Protection of electronic health records (EHRs) in cloud. *2013 35Th Ann. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*. 4191–4194, 2013. doi: 10.1109/embc.2013.6610469.

39. Ermakova, T., and Fabian, B., Secret sharing for health data in multi-provider clouds. *2013 I.E. 15Th Conf. Bus. Inform*. 93–100, 2013. doi:10.1109/CBI.2013.22.
40. Huang, M., Chen, Y., Chen, B., Liu, J., Rho, S., and Ji, W., A semi-supervised privacy-preserving clustering algorithm for healthcare. *Peer-To-Peer Network. Appl*. 1–12, 2015. doi:10.1007/s12083-015-0356-9.
41. Rahman, S., Masud, M., Hossain, M., Alelaiwi, A., Hassan, M., and Alamri, A., Privacy preserving secure data exchange in mobile P2P cloud healthcare environment. *Peer-To-Peer Network. Appl*. 1–16, 2015. doi:10.1007/s12083-015-0334-2.
42. Xhafa, F., Feng, J., Zhang, Y., Chen, X., and Li, J., Privacy-aware attribute-based PHR sharing with user accountability in cloud computing. *J Supercomput*. 71(5):1607–1619, 2014. doi:10.1007/s11227-014-1253-3.
43. Chen, C., Yang, T., Chiang, M., and Shih, T., A privacy authentication scheme based on cloud for medical environment. *J. Med. Syst*. 38:143, 2014. doi:10.1007/s10916-014-0143-9.
44. Chen, C., Yang, T., and Shih, T., A secure medical data exchange protocol based on cloud environment. *J. Med. Syst*. 38:112, 2014. doi:10.1007/s10916-014-0112-3.
45. Jafari, M., Safavi-Naini, R., and Sheppard, N., A rights management approach to protection of privacy in a cloud of electronic health records. *Proc. 11Th Ann. ACM Workshop Digit. Rights Manag. - DRM '11*. 23–30, 2011. doi:10.1145/2046631.2046637.
46. Lam, P., Mitchell, J., Scedrov, A., Sundaram, S., and Wang, F., Declarative privacy policy. *Proc. 2Nd ACM SIGHIT Symp. Int. Health Inform. - IHI '12*. 323–332, 2012. doi:10.1145/2110363.2110401.
47. Mohanty, M., Atrey, P., and Ooi, W., Secure cloud-based medical data visualization. *Proc. 20Th ACM Int. Conf. Multimed. - MM '12*. 1105–1108, 2012. doi:10.1145/2393347.2396394.
48. Sanz-Requena, R., Mañas-García, A., Cabrera-Ayala, J., and García-Martí, G., A cloud-based radiological portal for the patients: IT contributing to position the patient as the central axis of the 21 st century healthcare cycles. *Proc. First Int. Workshop Tech. Legal Aspects Data Privacy*. 54–57, 2015. Retrieved from http://dl.acm.org/citation.cfm?id=2821479.
49. Francis, T., Madiajagan, M., and Kumar, V., Privacy issues and techniques in E-Health systems. *Proc. 2015 ACM SIGMIS Conf. Comput. People Res. - SIGMIS-CPR '15*. 113115, 2015. doi:10.1145/2751957.2751981.
50. Balinsky, H., and Mohammad, N., Fine grained access of interactive personal health records. Proc. 2015 ACM Symp. Doc. Eng. - DocEng '15. 207–210, 2015. doi:10.1145/2682571.2797098.
51. Hei, X., and Lin, S., Multi-part file encryption for electronic health records cloud. *Proc. 4Th ACM Mobihoc Workshop Pervasive Wireless Healthcare - Mobilehealth '14*. 31–36, 2014. doi:10.1145/2633651.2637473.
52. Mohandas, A., and S, S., Privacy preserving content disclosure for enabling sharing of electronic health records in cloud computing. *Proc. 7Th ACM India Comput. Conf. - COMPUTE '14*. article no. 7, 2014. doi:10.1145/2675744.2675753.
53. Ragesh, G., and Baskaran, K., CRYPE. *Proc. First Int. Conf. Sec. Internet Things - Sec. '12*. 204–209, 2012. doi:10.1145/2490428.2490457
54. Lin, H., Shao, J., Zhang, C., and Fang, Y., CAM: Cloud-assisted privacy preserving mobile health monitoring. *IEEE Trans. Inform. Forensic Sec.* 8(6):985–997, 2013. doi:10.1109/tifs.2013.2255593.
55. Li, M., Yu, S., Zheng, Y., Ren, K., and Lou, W., Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Trans. Parallel Distrib. Syst.* 24(1):131–143, 2013. doi:10.1109/tpds.2012.97.
56. Li, M., Yu, S., Ren, K., and Lou, W., Securing personal health records in cloud computing: patient-centric and fine-grained data access control in multi-owner settings. *Lecture Notes Inst. Comput. Sci. Soc. Inform. Telecommun. Eng*. 89–106, 2010. doi:10.1007/978-3-642-16161-2_6.
57. Castiglione, A., Pizzolante, R., De Santis, A., Carpentieri, B., Castiglione, A., and Palmieri, F., Cloud-based adaptive compression and secure management services for 3D healthcare data. *Futur. Gener. Comput. Syst.* 43–44:120–134, 2015. doi:10.1016/j.future.2014.07.001.
58. Thilakanathan, D., Chen, S., Nepal, S., Calvo, R., and Alem, L., A platform for secure monitoring and sharing of generic health data in the Cloud. *Futur. Gener. Comput. Syst.* 35:102–113, 2014. doi:10.1016/j.future.2013.09.011.
59. Liu, J., Huang, X., and Liu, J., Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption. *Futur. Gener. Comput. Syst.* 52:67–76, 2015. doi:10.1016/j.future.2014.10.014.
60. Taneja, H., Kapil, and Singh, A., Preserving privacy of patients based on re-identification risk. *Proc. Comput. Sci.* 70:448–454, 2015. doi:10.1016/j.procs.2015.10.073.
61. Khan, F., Ali, A., Abbas, H., and Haldar, N., A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. *Proc. Comput. Sci.* 34:511–517, 2014. doi:10.1016/j.procs.2014.07.058.
62. Mishra, D., Mukhopadhyay, S., Kumari, S., Khan, M., and Chaturvedi, A., Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce. *J. Med. Syst*. 38(5), 2014. doi: 10.1007/s10916-014-0041-1.
63. Mishra, D., Srinivas, J., and Mukhopadhyay, S., A secure and efficient chaotic map-based authenticated key agreement scheme for telecare medicine information systems. *J. Med. Syst.* 38(10):120, 2014. doi:10.1007/s10916-014-0120-3.
64. Abbas, H., Magnusson, C., Yngstrom, L., and Hemani, A., Addressing dynamic issues in information security management. *Info. Mngmnt. Comp. Sec*. 19(1):5–24, 2011. doi:10.1108/09685221111115836.
65. Ali, A., and Khan, F., Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications. *EURASIP J. Wirel. Commun. Netw.* 2013(1):216, 2013. doi:10.1186/1687-1499-2013-216.