Global Journal of Health Science; Vol. 9, No. 3; 2017
ISSN 1916-9736 E-ISSN 1916-9744
Published by Canadian Center of Science and Education

Security Challenges in Healthcare Cloud Computing: A Systematic Review

Esmaeil Mehraeen[1], Marjan Ghazisaeedi[2], Jebraeil Farzi[3] & Saghar Mirshekari[4]

[1] PhD Student of Health Information Management, School of Allied Medical Sciences, Tehran University of Medical Sciences, Tehran, Iran

[2] School of Allied Medical Sciences, Tehran University of Medical Sciences, Tehran, Iran

[3] Assistant Professor, School of Paramedical, Zabol University of Medical Sciences, Zabol, Iran

[4] Students Research Committee, Faculty of Paramedical, Zabol University of Medical Sciences, Zabol, Iran

Correspondence: Marjan Ghazisaeedi, Assistant Professor, School of Allied Medical Sciences, Tehran University of Medical Sciences, Qhods Street, Tehran, Iran. Tel: 98-912-327-7921. E-mail: ghazi.saeedi@yahoo.com

Received: May 9, 2016 Accepted: June 1, 2016 Online Published: July 11, 2016

doi:10.5539/gjhs.v9n3p157 URL: http://dx.doi.org/10.5539/gjhs.v9n3p157

Abstract

Background: Healthcare data are very sensitive records that should not be made available to unauthorized people in order for protecting patient's information security. However, in progressed technologies as cloud computing which are vulnerable to cyber gaps that pose an adverse impact on the security and privacy of patients' electronic health records and in these situations, security challenges of the wireless networks need to be carefully understood and considered. Recently, security concerns in cloud computing environment are a matter of challenge with rising importance.

Objective: In this study a systematic review to investigate the security challenges in cloud computing was carried out. We focused mainly on healthcare cloud computing security with an organized review of 210 full text articles published between 2000 and 2015.

Method: A systematic literature review was conducted including PubMed, Science direct, Embase, ProQuest, Web of science, Cochrane, Emerald, and Scopus databases.

Findings: Using the strategies described, 666 references retrieved (for research question one 365, research question two 201, and research question three 100 references).

Improvements: Review of articles showed that for ensuring healthcare data security, it is important to provide authentication, authorization and access control within cloud's virtualized network. Issues such as identity management and access control, Internet-based access, authentication and authorization and cybercriminals are major concerns in healthcare cloud computing. To manage these issues many involved events such as Hybrid Execution Model, VCC-SSF, sHype Hypervisor Security Architecture, Identity Management, and Resource Isolation approaches have to be defined for using cloud computing threat management processes.

Keywords: security, healthcare data, cloud computing, electronic health record, systematic review

1. Introduction

In the recent century, information technology has created the ability to electronically store and transfer health information to improve the quality of health care and increase the effectiveness and efficiency of health care services organization (Zhang et al., 2010, pp. 268-275; Mehraeen et al., 2016, p. 47). Health information should be available to authorized healthcare providers (including researchers who are trying to find the causes, treatments, and cure patients) (Alnuem et al., 2011). Moreover, healthcare organizations with large volume of data are the most critical areas that require powerful calculation tools. Physicians must complete medical information to provide complete and accurate treatment to patients (Lupse et al., 2012, pp. 81-85) and so medicine is an increasingly data-intensive and collaborative endeavor (Rostrom et al., 2011, pp. 8219-22).

Current developments in remote healthcare system, has been influenced by the development of IT industry and it will provide health services everywhere and in an easy way. These systems provide a platform for sharing

medical information systems, infrastructure and applications in a format with the ability to provide automatic subscription. Communications security and confidentiality of healthcare information is one of the aspects that will increase the confidence of users in such tele-health systems (Khana et al., 2014, pp. 511-517). Also, advances in health care information systems generate considerable amounts of data to be processed and stored. Secondary use of clinical data with text or data mining algorithms requires dynamic and scalable resources. Cloud computing is the perfect solution to fulfill these demands (Griebel et al., 2015, p. 2). Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements (Kuyoro et al., 2011, pp. 247-255).

The emergence of cloud computing technology with significant advantages is one of the current major challenges. This is a new prototyping technology based on the "pay on demand" for the use of information communications and technology (Bildosola et al., 2015). The National Institute of Standards and Technology in the United States has targeted three models of cloud computing: software as a service, platform as a service and infrastructure as a service (Balasubramaniam et al., 2015, pp. 121-130). In a healthcare cloud computing for internal communications, extensive number of computers and servers are specifically dedicated to meet the needs of the medical care industry. Health care services can pass to users (patients or physicians) through the Internet connection (Parekh et al., 2015, pp. 537-542).

The cloud service empowered registered users to access the hardware and software through a third section in remote locations. It has conveyed fundamental changes in the way the information is stored and accessed (Bildosola et al., 2015). Despite all the benefits of cloud computing, there are several challenges that delay the migration of customer software and data to the cloud (Itani et al., 2009, pp. 711-716). Control and data protection are among the most important challenges that have to be considered in the development of cloud network (Neisse et al., 2015, pp. 60-76) and there will be potential gains achieved from the cloud computing. Security is one of the main obstacles to the growth of cloud computing in the health field, because of the need for high level of data integration, interoperability, and sharing among different healthcare physicians and organizations, various hospitals should be able to create standard guidelines and identify security challenges for improving information security in healthcare cloud computing (Alnuem et al., 2011; Kuyoro et al., 2011, pp. 247-255). The aim of this study was to review published articles in the field of health care cloud computing security to study the current challenges in this field.

2. Research Methods

2.1 Research Aim

The aim of this study was to investigate the security challenges in cloud computing. Reframing to healthcare field is the difference of this study from other similar researches. So, this paper introduces a detailed review of the healthcare cloud computing security issues and explores the main challenges focusing on the compliance concerns and ensuring trust data security with a systematic review of 210 articles.

2.2 Research Questions

- What are the security concerns in the healthcare cloud computing?
- How can we ensure trust data security in cloud computing infrastructures?
- How healthcare cloud computing is protected currently?

2.3 Research Strategy

In this phase, we found relevant sources where searches for particular studies should have been executed. The selection of sources should be related to both security challenges and healthcare cloud computing. To identify published, original research that reported the security challenges in the healthcare cloud computing, an organized search was conducted with the following search keywords: Cloud computing security, Cloud computing and information security, Healthcare cloud computing security, Healthcare information security and cloud computing, Healthcare cloud computing and security. A systematic search was conducted including PubMed, Science direct, Embase, ProQuest, Web of science, Cochrane, Emerald, and Scopus databases from 2000 to 2015 (Figure 1).

2.4 Criteria for Paper Selection and Evaluation

Following criteria were considered for selecting the studies related to security in the healthcare cloud computing:

-*Key words in the title or abstract:* The key words might be used in a paper as common words, therefore, only full text papers with the keywords in the title or abstracts were selected.

-*Date of publication:* The studies published between 2000 and 2015 were reviewed.

-*Language:* Only studies published in English were evaluated.

-*Type of a study:* The research papers and review articles were reviewed, and we excluded resources such as editorial letters, newspapers, and other types of sources.

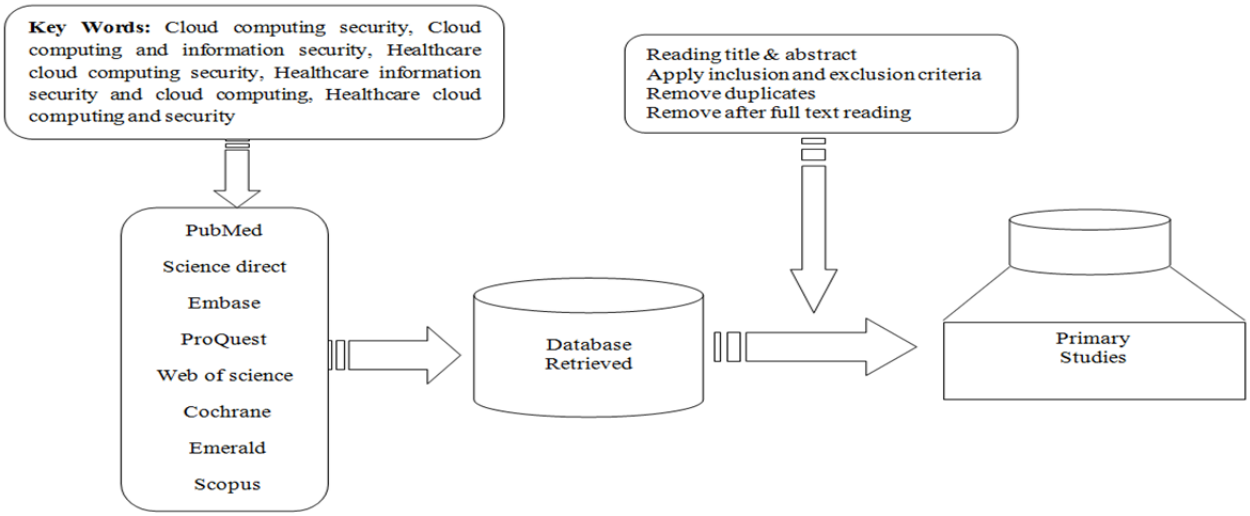

Figure 1. Study source selection

2.5 Results

All articles from 2000 to 2015 were taken into account for the purpose of searching in different databases. Using the strategies described above, 666 references were retrieved (for research question one 365, research question two 201, and research question three 100 references). Searched articles were compared based on their titles and abstracts. Comparison of the searched articles showed that, even though, different keywords have been used, most of the articles were duplicated. To identify more relevant articles for our purpose, the abstracts were considered by which 210 articles were selected. By going through the full texts of these papers, 52 articles were found to be more related to the questions of this paper from which 48 articles are included. Moreover, from all the articles referenced in this paper, 21 articles are used for the purpose of analysis and investigation of research questions (Table 1).

Table 1. Search results from different databases

Year Published	2000-2015				
Research Question	Total Reference Retrieved	Total Abstract Screened	Total Full-Text Screened	Final Included Papers	Number of Analyzed Articles
RQ1	365	110	27	27	10
RQ2	201	75	17	15	7
RQ3	100	25	8	6	4
Total	666	210	52	48	21

Note. RQ1= Research Question 1, RQ2= Research Question 2, RQ3= Research Question 3

2.5.1 Information Extraction

Table 2 shows final articles that were used for the purpose of analysis and investigation of research questions.

Table 2. Summary of final studied articles and their relevance to the research questions

N	Researcher(s)	Year	Study Context	Results Related		
				RQ1	RQ2	RQ3
1	*Balasubramaniam and Kavitha*	*2015*	*Security Architecture for Cloud Computing*	√		
2	*Koo et al.*	*2015*	*Industrial Security for the Adoption of Cloud Computing*	√		
3	*Gunamalai, and Sivasubramanian*	*2015*	*Method of security and privacy for cloud computing*	√		
4	*Kang et al.*	*2015*	*Service-Oriented Security Framework for Vehicular Cloud Computing*			√
5	*Rahman et al.*	*2015*	*Secure data exchange in cloud healthcare environment*	√		
6	*Velumadhava Rao and Selvamani*	*2015*	*Data Security Challenges in Cloud Computing*	√		
7	*Haufe et al.*	*2014*	*Security Management in Cloud Computing for Health Care*			√

Table 2. Summary of final studied articles and their relevance to the research questions (Continued)

N	Researcher(s)	Year	Study Context	Result Related		
				RQ1	RQ2	RQ3
8	*Zapata et al.*	*2014*	*Security in Cloud Computing*		√	
9	*Sun et al.*	*2014*	*Security and Privacy in Cloud Computing*		√	
10	*Aslam Khan et al.*	*2014*	*A cloud-based healthcare framework for security*		√	
11	*Yu et al.*	*2014*	*A Security-Awareness Virtual Machine Management Scheme in Cloud Computing*			√
12	*Youssef*	*2014*	*A Framework for Secure Healthcare Systems in Mobile Cloud*		√	
13	*Aruna Devi et al.*	*2014*	*Enhancing security features in cloud computing*		√	
14	*Azar and Laxman*	*2014*	*Secured Health Monitoring in Cloud Computing*	√		
15	*Jaswanthi and NaliniSri*	*2013*	*Confidentiality and Privacy in Cloud Computing*			√
16	*Chen et al.*	*2012*	*Secure PHR in Cloud Computing*		√	
17	*Johnstone*	*2012*	*Cloud security*	√		
18	*Vidya et al.*	*2012*	*Homomorphic Encryption In Cloud Computing*		√	
19	*Cheng and Lai*	*2012*	*Protection of Information Privacy in Cloud Computing*	√		
20	*Kuyoro et al.*	*2011*	*Cloud Computing Security Challenges*	√		
21	*Li. et al.*	*2010*	*Securing Personal Health Records in Cloud Computing*	√		

3. Discussion

3.1 Research Question 1

Despite the potential benefits of cloud computing in e-health services, information security is still questionable and a security problem have become more complex in the cloud models and requires additional investments to implement data management policies (Almorsy et al., 2010; Koo et al., 2015). For all the predictable or informative events in health care cloud computing, basic data (what, where, when, risks and consequences) must

be registered and approved by the relevant people so that they can propose and/or take the necessary measures (Runciman et al., 2006, pp. 82-90).

The data stored in cloud virtualized environment can be accessed or managed through many of people (Velumadhava et al., 2015, pp. 204-209); thus, use of healthcare cloud computing has several major issues and concerns, including data transmission and access control (Balasubramaniam et al., 2015, p. 121). On the other hand, when users store and transfer their information on the cloud, the integrity of data protection and issues related to how to transfer healthcare data is challenging task (Azhar et al., 2014, p. 138; Johnstone et al., 2012, p. 43). However, by storing healthcare information in the cloud, the patients lose physical control to their personal information (Li et al., 2010, pp. 89).

Data motion and transmission from one organization to another is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment (Kuyoro et al., 2011, pp. 247). To the best of our knowledge, currently there is no existing anonymous secure data exchange solution in healthcare cloud environment (Rahman et al., 2015, p. 2). Data mobility and inability to locate or process, are the main challenges of cloud computing in healthcare. Data stored in the cloud is often placed in a virtual environment and a virtual server space cloud be shared with other customers of cloud service providers. Healthcare organizations that transmit sensitive and regulated data into the cloud should ensure that the data is encrypted and secured.

Another concern of shared computing resources within cloud infrastructures is the identity and access management. Modern technology, increase their functionality and accessibility and it introduces additional needs in terms of information security, particularly authentication. Authentication using widely documented PINs is designed as a solution to overcome the fundamental issues that are usable and to secure through biometric-based techniques to user identity (Saevanee et al., 2015, pp. 234-246). In the conventional authentication process for access management there might be illegal use of data if the password is disclosed to an unauthorized person (Gunamalai et al., 2015, p. 4636)**.** Current identification and authentication methods in healthcare organizations may not be applicable in cloud computing and if these have a combination of unique username/password for certain and sensitive applications, they will present a poor link in the security structure. In the cloud, identity management helps to maintain security, identification and control and focuses on identity and access control.

Internet-based access is another significant challenge in healthcare cloud computing. Clouds are on Internet; therefore, all the security concerns related to Internet, including frauds and attacks by hackers, may happen (Cheng et al., 2012, p. 243). When multiple organizations share resources on Internet-based environment, there is a threat of data misuse and breaches (Velumadhava Rao et al., 2015, p. 206). Use of internet in healthcare services delivery outside the clinic or hospital provides vital benefits to providers and patients equally. However, access to health care data in unsecured virtual environments, creates challenges such as theft or loss of data and regulatory noncompliance. Increasing use of the Internet in healthcare area is required to use cybernetic management solutions for the secure transmission of data, providing solutions across broadband networks, protecting devices from data breaches and unauthorized access.

3.2 Research Question 2

Data security in the cloud computing consistently had been a major issue because the data is transferred in different places. Ensure data security protection is the main issue of user's concern in the cloud technology, therefore, data security protection is becoming more important for the future expansion of cloud computing technology in healthcare organizations (Sun et al., 2014, p.1). Due to interoperability features, concerning when data transferred to an external provider, moving to cloud computing in healthcare organizations is the major challenge rather than other areas. This is due to adopting a variety of data modeling structures on Medicare organizations that lead to different database designs, implementation, management, operating systems, programming languages and incompatible systems (Aruna et al., 2014, pp. 200-203).

To ensure data security in cloud computing infrastructures, health care organizations should have direct control on many aspects of security. In this area, health care providers usually have great confidence in cloud service providers. Cloud service providers have a vital role in the execution incident response, including transaction analysis, access control, data protection, rehabilitation and services integration. For sensitive and regulatory agencies such as health care organizations, should organize and implement data management tools to recognize and ensure data security policies within cloud virtual environment. Besides, to ensure data security in cloud computing, providing authentication, authorization and access control for data stored in the cloud virtual space is important. Authentication and Authorization are two important issues to health information security management across virtual environment. Authentication in health care cloud infrastructures encompasses both health

information and identities of users (health care providers, physicians and patients).

Access control scheme is a safe technique to trust to data security in cloud computing infrastructures. With Lagrange interpolation polynomial to establish a secure and effective healthcare information access scheme, it allows to accurately accessing control and is suitable for enormous multi-users (Chen et al., 2012, p.4005). Although, user's identity, multi-biometric based encryption mechanism, and data auditing to verify the correctness of healthcare data are other ensure ways to security assurances of information stored in cloud environment (Aslam Khan et al., 2014, p. 511; Vidya et al., 2012, p.1). The user's identity should be verified at the entry of all accesses using username and password allocated by the cloud providers. Authorization is a critical security requirement to control access priority, permissions and users sources ownership in the cloud. Cloud users are permitted rights on their account to access to information. But it does not conflict with the patients' rights and they can accept or reject sharing information with other physicians or health care organizations.

For patients' consents in a health care system, there may be donation rights to users who have a role in healthcare providing. Access control primarily refers to data security policies. For health care providers, the staff can have access to part of the data according to their organization security policies. To protect data from unauthorized users the data security policies must be strictly followed. Since Internet-based access is given for all cloud users, it is necessary to define privileged user access. Users can use data encrypt and protection mechanisms to evade security risks.

There are different approaches for trust of security aspects in cloud computing. A taxonomy approach that classification security issue is an applicable way that covers eight categories: software, storage and computing, virtualization, Internet and services, network, access, trust, and compliance and legality (Zapata et al., 2014, p.166). In addition to, healthcare organizations should be propose a framework to apply a set of security constraints and access control that guarantee integrity, confidentiality, and privacy of healthcare data in cloud environment. Accredited healthcare providers, physicians, and patients are authorized by the Cloud Service Providers (CSPs) at different levels of privilege and permissions to secure access and retrieve patients' information (Youssef et al., 2014, p.2).

4.3 Research Question 3

One of the most important changes in the health care area over the past two decades was the increasing investment in healthcare information security and confidentiality. Protecting healthcare information security, privacy and confidentiality is a continuous process and serious responsibility of every health care organization (Haufe et al., 2014, p. 7). Despite the attractive aspects and features that cloud offers, the move toward cloud technology and its use is relatively slow, mainly due to the inherent security challenges related to the technology. These challenges include data privacy, transparency, risk management, compliance and information security (Jansen, 2011, pp. 1-10; Subashini et al., 2011, p. 11; Habiba et al., 2014, pp. 1-37).

The healthcare industry is a highly disciplined environment and the nature of cloud computing infrastructures—sharing software and servers and communicates via Internet—increases concerns about privacy, security, access and compliance. Sharing medical and personal information beyond the secure milieu of the healthcare organization, and accessing it by a collection of devices and from various sites, leads to many compliance issues. Internet-based virtual infrastructure is a large system with great potential for information security breaches. Cyber-attacks and lack of knowledge of authorized users are the important risks in the healthcare systems. Hackers use various methods to change confidentiality, integrity, and information accessibility, while users intentionally or through negligence are a significant danger for information security (Safa et al., 2015, pp. 65-78).

Recent security protection ways in healthcare cloud computing includes in Hybrid Execution Model, Vehicular Cloud Computing (VCC) Service-oriented Security Framework (VCC-SSF), sHype Hypervisor Security Architecture, Identity Management, and Resource Isolation approaches. A new execution model for security protection in cloud computing is the Hybrid Execution model. This model provides a unified way for an organization to utilize their own infrastructure for sensitive, private data and computation (Jaswanthi et al., 2013, p. 84). Vehicular Cloud Computing (VCC) Service-oriented Security Framework (VCC-SSF) to address the limitations and security threats is the other way for protection of healthcare cloud computing. This framework considers security for suitable and efficient services of VCC and includes new user-oriented payment management and active accident management services. Furthermore, it provides authentication, encryption, access control, confidentiality, integrity, and privacy protection for user personal healthcare data (Kang et al., 2015, p. 2028).

The sHype hypervisor security architecture, which enforced isolation at the granularity of a cloud virtual environment, is a particular approach that can isolate the more sensitive and private information to stronger protection (Yu et al., 2014, p. 2). For cybercriminals, cloud virtual infrastructure produces a potential attack surface than a traditional data center. Cyber-attacks using malware and other acts cloud infect healthcare cloud system components such as operating systems and spread throughout the environment. Protection of healthcare cloud computing from malware and other security threats require identity management at network boundaries to ensure that only authorized users can access to system. Also, securing server and clients' platform is possible through systems integration. Integrity in healthcare systems means maintaining accuracy and consistency of the transmitted data. This feature is requirement for healthcare cloud computing and in this area, integration refers to the statement that healthcare information in virtual environment has not been accessed by unauthorized user. Resource isolation is the another approach to provide security isolation in the shared cloud infrastructure, this method helps to achieve resource isolation among virtual networks, which was per-slice shaping and per-link policing (Yu et al., 2014, p. 2).

4. Conclusion

It is clear that the security issue has played the most important role in hindering cloud computing acceptance. Issues such as identity management and access control for virtual cloud environment, Internet-based access, authentication and authorization and cybercriminals are major concerns in healthcare cloud computing. Putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Most important security challenges in cloud computing technology such as data mobility, multi-tenancy and access control pose serious threats to sensitive information and software in healthcare organizations. Thus, many involved events such as Hybrid Execution Model, VCC-SSF, sHype Hypervisor Security Architecture, Identity Management, and Resource Isolation approaches have to be defined for using cloud computing threat management processes. On the other hand, all involved parties and their interactions in healthcare cloud computing should be defined to ensure secure information exchange. Cloud service providers and healthcare organizations should be defined clear processes for maintaining security in cloud environments. Protecting sensitive electronic medical data is one of the most essential responsibilities of healthcare organizations, and one of the most tightly regulated in cloud area. An essential procedure to improve security and conquest in its threats is the comprehensive understanding and the effective execution of dependent concerns and data protection in healthcare cloud computing.

4.1 Recommendations

We have perceived that for ensuring trust data security in cloud computing infrastructures; healthcare organizations should have direct control over many aspects of security. Following recommendations proposed for secure communication and interoperability in virtualized healthcare cloud environments:

- Development and application of security policies in physical, virtual and private healthcare cloud computing environment for the prevention of cyber attacks
- Collaborate with cloud service providers to implement appropriate security controls in a cloud virtual environment
- Use of encryption and data protection mechanisms to authenticate authorized users and licensing
- Consider information security as a set of adaptive services integrated with compliance requirements and healthcare cloud architecture/design
- Maintain separation of duties between security policy enforcement and IT operations

4.1.1 Recommendations for Future Work

- Review the security status of remote communication systems
- Providing security solutions for cloud computing
- Review information security policies in health care organizations
- Review security policies on the healthcare cloud

Acknowledgments

This study was funded and supported by Tehran University of Medical Sciences (TUMS).

Authors' Contributions

Mehraeen E. proposed, started and conceived of the study and participated in the design of the study.

Ghazisaeedi M. provides instruction at various steps of study. Farzi J. & Mirshekari S. were responsible for searching keywords on search engines and drafting the manuscript.

Competing Interests Statement

The authors declare that the funding mentioned in the Acknowledgments section do not lead to any conflict of interest. Additionally, the authors declare that there is no conflict of interest regarding the publication of this manuscript.

References

Almorsy, M., Grundy, J., & Muller, I. (2010). An analysis of the cloud computing security problem. *Asia Pacific Software Engineering Conference* (APSEC '10), Sydney, Australia.

Alnuem, M., Masri, S. E., Youssef, A., & Emam, A. (2011). Towards Integrating National Electronic Care Records in Saudi Arabia. *The 2011 International Conference on Bioinformatics and Computational Biology*, Monte Carlo Resort, Las Vegas, Nevada, USA. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.217.7526&rep=rep1&type=pdf

Aruna, D. S., & Manju, A. (2014). Enhancing security features in cloud computing for healthcare using cipher and inter cloud. *International Journal of Research in Engineering and Technology, 3*(3), 200-203. http://dx.doi.org/10.15623/ijret.2014.0303036

Aslam, K. F., Ali, A., Abbas, H., & Haldar, N. H. (2014). A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. *Procedia Computer Science, 34*, 511-517. http://dx.doi.org/10.1016/j.procs.2014.07.058

Azhar, M., & Laxman, M. (2014). Secured Health Monitoring System in Mobile Cloud Computing. International *Journal of Computer Trends and Technology, 13*(3), 138-142. http://dx.doi.org/10.14445/22312803/IJCTT-V13P129

Balasubramaniam, S., & Kavitha, V. (2015). Hybrid Security Architecture for Personal Health Record Transactions in Cloud Computing. *Advances in Information Sciences and Service Sciences, 7*(1), 121-130.

Balasubramaniam, S., & Kavitha, V. (2015). Geometric Data Perturbation-Based Personal Health Record Transactions in Cloud Computing. *The Scientific World Journal, 9*(2), 9. http://dx.doi.org/10.1155/2015/927867

Bildosola, I., Río-Belver, R., Cilleruelo, E., & Garechana, G. (2015). Design and Implementation of a Cloud Computing Adoption Decision Tool: Generating a Cloud Road. *PLOS ONE, 10*(7), e0134563. http://dx.doi.org/10.1371/journal.pone.0134563

Chen, T. S., et al. (2012). Secure Dynamic Access Control Scheme of PHR in Cloud Computing. *Journal of medical systems, 36*, 4005-4020. http://dx.doi.org/10.1007/s10916-012-9873-8

Cheng, F. C., & Lai, W. H. (2012). The Impact of Cloud Computing Technology on Legal Infrastructure within Internet—Focusing on the Protection of Information Privacy. *Procedia Engineering, 29*, 241-251. http://dx.doi.org/10.1016/j.proeng.2011.12.701

Griebel, L., et al. (2015). A scoping review of cloud computing in healthcare. *BMC Medical Informatics and Decision Making, 15*(17), 2. http://dx.doi.org/10.1186/s12911-015-0145-7

Gunamalai, C., & Sivasubramanian, S. (2015). A novel method of security and privacy for personal medical record and DICOM images in cloud computing. *Journal of Engineering and Applied Sciences, 10*(10), 4635-4638.

Habiba, U., Masood, R., Shibli, M. A., & Niazi, M. A. (2014). Cloud identity management security issues & solutions: a taxonomy. *Complex Adaptive Systems Modeling, 2*(5), 1-37. http://dx.doi.org/10.1186/s40294-014-0005-9

Haufe, K., Dzombeta, S., & Brandis, K. (2014). Proposal for a Security Management in Cloud Computing for Health Care. *The Scientific World Journal*, 146970, 7. http://dx.doi.org/10.1155/2014/146970

Itani, W., Kayssi, A., & Chehab, A. (2009). Privacy as a service: privacy-aware data storage and processing in cloud computing architectures, in *Proceedings of the 8th IEEE International Conference on Dependable, Autonomic and Secure Computing* (DASC '09), Chengdu, China, December, 711-716.

Jansen, W. A. (2011). Cloud hooks: Security and privacy issues in cloud computing. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on Piscataway*, New Jersey, United States: IEEE: 1-10.

Jaswanthi, B., & NaliniSri, M. (2013). Confidentiality and Privacy in Cloud Computing using Hybrid Execution Method. *International Journal of Science and Modern Engineering, 1*(5), 84-89.

Johnstone, M. (2012). Cloud security: A case study in telemedicine. *1st Australian e-Health Informatics and Security Conference,* December 3rd-5th, Perth, Western Australia.

Kang, W. M., Lee, J. D., Jeong, Y. S., & Park, J. H. (2015). VCC-SSF: Service-Oriented Security Framework for Vehicular Cloud Computing. *Sustainability, 7*, 2028-2044. http://dx.doi.org/10.3390/su7022028

Khana, F. A., Alia, A., Abbas, H., & Haldar, N. H. (2014). A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. *Procedia Computer Science, 34*, 511-517. http://dx.doi.org/10.1016/j.procs.2014.07.058

Koo, C. J., & Kim, J. Y. (2015). Decision Making for the Adoption of Cloud Computing for Sensor Data: From the Viewpoint of Industrial Security. *International Journal of Distributed Sensor Networks, 581563*, 5. http://dx.doi.org/10.1155/2015/581563

Kuyoro, S. O., Ibikunle, F., & Awodele, O. (2011). Cloud Computing Security Issues and Challenges. *International Journal of Computer Networks, 3*(5), 247-255.

Li, M., Yu, S., Ren, K., & Lou, W. (2010). S*ecuring Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings*. Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 89-106.

Lupşe, O. S., & Vida, M. M., & Tivadar, L. S. (2012). Cloud Computing and Interoperability in Healthcare Information Systems. *The First International Conference on Intelligent Systems and Applications*, 81-85.

Mehraeen, E., Ayatollahi, H., & Ahmadi, M. (2016). Health Information Security in Hospitals: the Application of Security Safeguards. *ACTA INFORM MED, 24(1): 47-50*.

Neisse, R., Steri, G., Fovino, I. N., & Baldini, G. (2015). SecKit: A Model-based Security Toolkit for the Internet of Things. *Computers & Security, 54*, 60-76. http://dx.doi.org/10.1016/j.cose.2015.06.002

Parekh, M., & Saleena, B. (2015). Designing a Cloud based Framework for HealthCare System and applying Clustering techniques for Region Wise Diagnosis. *Procedia Computer Science, 50*, 537-542. http://dx.doi.org/10.1016/j.procs.2015.04.029

Rahman, S. M., et al. (2015). Privacy preserving secure data exchange in mobile P2P cloud healthcare environment. *Peer-to-Peer Netw*, 1-16.

Rostrom, T., & Teng, C. C. (2011). Secure communications for PACS in a cloud environment. *Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 8219-22. http://dx.doi.org/10.1109/iembs.2011.6092027

Runciman, W. B., Williamson, J. A. H., Deakin, A., Benveniste, K. A., Bannon, K., & Hibbert, P. D. (2006). An integrated framework for safety, quality and risk management: an information and incident management system based on a universal patient safety classification. *Quality and Safety in Health Care, 15*(1), 82-90. http://dx.doi.org/10.1136/qshc.2005.017467

Safa, N. S., Sookhak, M., Solms, R. V., et al. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78. http://dx.doi.org/10.1016/j.cose.2015.05.012

Saevanee, H., Clarke, N., Furnell, S., & Biscione, V. (2015). Continuous user authentication using multi-modal biometrics. *Computers & Security, 53*, 234-246. http://dx.doi.org/10.1016/j.cose.2015.06.001

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *J Netw Comput Appl, 34*, 1-11. http://dx.doi.org/10.1016/j.jnca.2010.07.006

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks, 190903*, 1. http://dx.doi.org/10.1155/2014/190903

Velumadhava, R. R., & Selvamani, K. (2015). Data Security Challenges and Its Solutions in Cloud Computing. *Procedia Computer Science, 48*, 204-209. http://dx.doi.org/10.1016/j.procs.2015.04.171

Vidia, S., Vani, K., & Kavin, P. D. (2012). Secured Personal Health Records Transactions Using Homomorphic Encryption In Cloud Computing. *International Journal of Engineering Research & Technology, 1*(10), 1-5.

Yu, S., Gui, X., Lin, J., Tian, F., Zhao, J., & Dai, M. (2014). A Security-Awareness Virtual Machine Management Scheme Based on Chinese Wall Policy in Cloud Computing. *The Scientific World Journal, 805923*, 1-12. http://dx.doi.org/10.1155/2014/805923

Youssef, A. (2014). A Framework for Secure Healthcare Systems Based on Big Data Analytics in Mobile Cloud. *International Journal of Ambient Systems and Applications, 2*(2), 1-11. http://dx.doi.org/10.5121/ijasa.2014.2201

Zapata, B. C., Fernández-Alemán, J. L., & Toval, A. (2014). Security in Cloud Computing: A Mapping Study. *Computer Science and Information Systems, 12*(1), 161-184.

Zhang, R., & Liu, L. (2010). Security Models and Requirements for Healthcare Application Clouds. *IEEE 3rd International Conference on Cloud Computing*, Miami, 268-275. http://dx.doi.org/10.1109/cloud.2010.62