Security Solutions in Cloud-based Healthcare Information Systems: A Systematic Review

Mohsen S. Tabatabaei[1], Mostafa Langarizadeh[2]*, Mohammad K. Akbari[3]

[1]School of Health Management and Information Sciences, International Campus (IUMS-IC), Iran University of Medical Sciences. Tehran, Iran
[2]School of Health Management and Information Sciences, Iran University of Medical Sciences. Tehran, Iran
[3]Department of Computer Engineering and Information Technology, Amirkabir University. Tehran, Iran
*Corresponding Author: Dr. M. Langarizadeh, E-mail: langarizadeh2001@yahoo.com, Phone: +98-919-861-6016

Summary
Cloud computing technology has attracted various industries including healthcare systems, as an efficient and cost-effective medium for providing services over the Internet for various purposes worldwide. Despite the growing popularity, healthcare institutions are concerned about ensuring the security of patient data shared over the Internet. The aims of this article were: a) to examine the existing information security solutions in healthcare industry, b) to review the strengths and weakness, and c) to propose a new cloud-based information security approach by combining the strengths and minimizing the weaknesses. We searched four major databases: PubMed, Scopus, ISI Web Sciences, and Science Direct, in two phases, using such key terms as cloud-based health information security; healthcare informatics; and cloud computing technology. Of the 231 initial quality entries, 21 eligible articles and 15 projects were examined systematically by an expert panel, and the findings were grouped into: administrative, technical and physical information security domains.
Five groups of security solutions were identified (Table 1), collectively offering 17 advantages to cloud-based information communication (Table 2). Also, 15 successful cloud-based information projects with their effective security solutions and methods are presented in Table 3.
Appropriate security solutions for cloud-based healthcare data communication enhance the confidentiality of the Internet services and improve collaborations among healthcare institutions. The best approach for providing cloud-based information exchange is to combine security solutions to ensure confidentiality and accessibility, maximizing collaboration among healthcare institutions, while reducing or eliminating potential threats worldwide.

Key Words:
Healthcare information; Security solutions; Healthcare informatics; Cloud computing technology.

1. Introduction

Cloud computing is an important topic in the development of information technology (IT) and has attracted the attention of communication researchers as a new opportunity for the provision of internet services to a whole host of clients worldwide (1, 2). This technology is efficiently capable of providing services over the internet on demand and at a set cost by sharing computing resources with users for various purposes (3, 4). The application of cloud computing in healthcare industry has enabled users to have efficient access to myriad of hardware and software resources worldwide, at any time and place where internet is available (5). Without cloud computing technology, healthcare institutions have to invest separately in the infrastructures to maintain effective communication, prompt access to patients' records and provision of quality medical services among their physicians and providers (6). However, in the presence of cloud computing technology, the subscribing healthcare institutions equally benefit the system and enjoy its services without a need to own the technology (7).
Besides the growing popularity of cloud computing applications in healthcare industry, there exist some concerns, mainly surrounding the security of patient information. Although there are innovative and effective protocols for information security, particularly for healthcare applications exists; a large number of institutions are concerned about adopting cloud computing over locally controlled internet servers. Further, the architecture of information security in traditional internet system has major differences with the protocols designed for cloud computing, with which most users are not familiar (8, 9).
Unless the information security concerns are properly and transparently addressed, most healthcare institutions will remain hesitant to adopt cloud computing services as a modern means of information exchange among physicians, other institutions, and most importantly, the patients (10).
Therefore, providers of cloud services to healthcare institutions must pay high attention to the security and privacy of not only their own information but also those of other institutions to minimize or eliminate security threats. This effort not only provides security to the cloud computing providers but also gains the satisfaction and trust of the healthcare institutions involved
(11).

Manuscript received September 5, 2018
Manuscript revised September 20, 2018

To date, several research projects have been conducted to investigate the potential threats to cloud-based health information systems and some promising solutions on the system architecture and ensuring information security have been suggested. However, some fundamental disagreements by IT experts still remain. Major troubling issues regarding health information security include:
Inconsistencies among current health information systems and the technical architecture.
Limited access to cloud-based health information in some geographic regions.
Shortage of healthcare information laws in many countries, at federal, state and local levels (7, 12, 13).
Given the above facts, the urgent need for a systematic research to explore and resolve the security challenges facing cloud-based health information systems remains a vital task. The aims of this systematic review were: a) to compare and contrast the current health information security protocols, b) to examine their strengths and weakness, and c) and to design and recommend a new health information security protocol that combines the strengths of the current protocols, while minimizing or eliminating their weaknesses.

2. Methods

Phase 1: We searched four major healthcare literature databases, such as PubMed, Scopus, ISI Web Sciences, and Science Direct. The key terms used to search these databases included "cloud-based health information security; healthcare informatics; and cloud computing technology". We identified and reviewed many relevant articles, 21 of which had all of the following selection criteria:

- Studied various aspects of cloud-based healthcare information security or healthcare informatics.
- Were published between 2010 and 2017 in reputable English journals and were retrieved in full-text.
- Were indexed by one or more of the selected databases, as identified above.

The selected articles were primarily reviewed and approved by a panel of three academicians experienced in medical informatics. The articles (N=21) were further reviewed in detail by two members of the panel, who noted their findings of the selected articles independently and grouped them into specific categories (Table 1). The members' findings were deliberated collectively by the panel with a focus on the significant merits of the extracted security methods. The approved findings were then assigned for inclusion in the manuscript.
Phase 2: Following the completion of Phase 1, we compared the security architecture of 15 credible published projects (Table 3) that had utilized cloud computing technology. The key terms and major databases used to search for these projects were the same as those in Phase 1.

3. Results

In this review, "security controls" refer to protecting, defeating, preventing or minimizing security threats to cloud-based health information and related data (14). These are categorized in three groups: administrative, technical (or logical) and physical controls. Administrative Control involves standard procedures and written guidelines that have been established by experts in the field. Technical Control refers to monitoring the appropriate access to information and computer systems through the use of software, hardware and relevant data. Physical Control covers the protection of computers, technical equipment, and the work environment (15, 16). Alternatively, and based on recent research, security solutions to safeguard cloud computing technology are grouped into five headings: security standards, security protocols, encryption techniques, regulations and procedures, and access control mechanisms (Table 1). Detailed descriptions of these heading and the components are presented below.

Table 1: Security solutions to safeguard cloud computing technology

Solutions	Security Standards	Security Protocols	Encryption Techniques	Regulations & Policies	Access Control Mechanisms
Methods	ISO27001 ISO27002 ISO27006 ISO27799 ISO18808 DICOM HL7	HTTP SMTP MIME HTML5 TCP/IP WADO	SKE PKE SOAP STTP SSL TLS	HIPAA Federation ID	Access Controls: ACL, RBAC, FGAC Access Methods: OpenID, XACML, Shibboleth

Security Standards:
The security standards provide specific frameworks for the management of cloud-based health information exchange and its environment, such that potential threats and hacking against the system are prevented or minimized.
International Organization for Standardization (ISO) was founded in 1946. ISO is an international organization aimed at establishing and standardizing the security and management of computer information systems worldwide. ISO27001, ISO27002, ISO27006, ISO27799 and ISO18808 are well known information security standards that are issued and authorized by ISO (17, 18).
Digital Imaging and Communications in Medicine (DICOM) is one of the most successfully applied standards in clinical computing systems. It is used for the

exchange of image data between picture archiving and communication system (PACS) and other healthcare communication systems locally, regionally and worldwide (19).

HL7 or Health Level -7 refers to a set of international standards for transfer of clinical and administrative data between software applications used by various healthcare providers. These standards focus on the application layer, which is "layer 7" in the OSI model. The HL7 standards are produced by the Health Level Seven International, that is an international standards organization, and are adopted by other standards issuing bodies such as American National Standards Institute and ISO (20, 21).

Security Protocols:

The most popular security protocols used in cloud computing technology are HTTP, SMTP, MIME, HTML5, TCP/IP and WADO.

HTTP or Hyper Text Transfer Protocol refers to the communications protocol used to connect to Web servers on the Internet or on a local network (intranet). Its primary function is to provide secure connection with servers via Web and send HTML pages to the users' browsers (22).

SMTP is part of the application layer of the TCP/IP protocol. Using a process called "store and forward", SMTP moves Email messages across networks. It works closely with another protocol called the Mail Transfer Agent (MTA) to send user's communications to the right computer and Email inbox (23).

MIME stands for Multipurpose Internet Mail Extensions and is an Internet standard for extending Email format to support text in character sets other than ASCII and non-text attachments generated by audio, video, images, and other programs (24).

HTML5 is a markup language used to structuring and presenting content on the Web. It is the fifth and current major version that exists in two standardized forms (25).

TCP/IP or Transmission Control Protocol/Internet Protocol consists of communication protocols that are used to connect network devices together on the Internet. TCP/IP may also be used as a communication protocol in a private network such as intranet or extranet (26).

WADO or Web Access to DICOM Persistent Objects is a web-based protocol for sharing and retrieving DICOM image data to and from healthcare institutions, using the http and https protocols (13).

Encryption Techniques:

The use of encryption techniques is one of the powerful cloud-based security mechanisms against data loss or theft. The algorithms are divided into symmetric and asymmetric encryptions, depending on whether the technique uses a public or private key for the encryption or decryption of information, respectively, at the time of data transmission to the cloud computing system. Asymmetric algorithms provide a higher level of security than the symmetric ones, thus they are used more frequently to protect cloud computing technology (27, 28).

SKE or symmetric key encryption is an algorithm for cryptography, that uses the same keys for both encryption of plain text and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. In practice, the keys represent a shared secret between two or more parties that can be used to maintain a private information link. Although SKE is simpler and faster, the fact that both parties have access to the same secret key is one of the main drawbacks. The most popular SKE is data encryption standard (DES) (29).

PKE or public key encryption is used to secure electronic communication over an open networked environment, such as the Internet. This cryptographic system uses pairs of keys, i.e., public keys which may be disseminated widely, and private keys which are known only to the owner. This system avoids the SKE problem, because the public key can be distributed in a non-secure way, but the private key is never shared or transmitted (29).

SOAP stands for Simple Object Access Protocol, a messaging protocol that allows programs that run on disparate operating systems, such as Windows or Linux, to communicate with each other using HTTP and XML (30).

STTP or the Secure Token Transfer Protocol enables two entities to exchange a set of tokens that is needed to perform a certain task, e.g., verify authenticity. STTP is intended to be used in case a mechanism to securely transfer tokens is missing for a particular context in other protocols (31).

SSL or Secure Sockets Layer is a standard security technology for making an encrypted link between a web server and a browser. It ensures that all exchanged data remain private. SSL is an industry standard and is used by hundreds of websites to protect their online transactions and the clients (32).

TLS or Transport Layer Security and SSL are protocols that provide security for communication among computer and Internet networks. Multiple versions of TLS and SSL are frequently used for web browsing, Email, instant messaging, and voice over IP (VoIP). Websites use these protocols to secure communications between their servers and web browsers (32).

Regulations and Policies:

Considering the growth of cloud-based computing and the applicable services needed by various institutions, it is essential that the related security regulations and policies are developed and enforced by the governments and private sector alike. The regulation and policies provide a secure environment for various healthcare institutions, convincing them to trust the system when they share or exchange confidential patients' information among the members of healthcare community (27, 33, 34).

HIPAA stands for Health Insurance Portability and Accountability Act, which is a section within the U.S. Department of Health and Human Services. Passed in 1996, HIPAA was established to make health care delivery more efficient and confidential, as well as providing more Americans with health insurance coverage based on three provisions: portability, tax and administrative simplification (35).

Federation ID is a field within the Internet webpage of certain organizations that permits the administration to select case-sensitive usernames and format for their clients to log in (36).

Access Control Mechanisms & Methods:

Access control mechanisms enable the system to check the users' identity without them noticing it. Thus, only authorized users are allowed to enter the system and have access to the cloud-based information (37). There are three control mechanisms to access the cloud-based system: 1) Access Control list (ACL) consists of the eligibility checks to determine the person's right to access the system; 2) Role-based Access Control (RBAC) operates based on the role of individuals within the system; and 3) Fine-grained Access Control (FGAC) is similar to RBAC but includes certain predetermined targets before allowing access to the system (38). The most popular access methods are: Open ID, XACML and Shibboleth.

ACL or Access Control List is a table identifies which access rights each user has to a particular system object, such as a file or the directory. The list has an entry for each system user with access privileges, such as the ability to read, write or execute a file. The list is implemented differently by various operating systems (39).

RBAC refers to Role-based Access Control or Role-based Security. It is a policy neutral access control mechanism that authorizes users to access the system. RBAC is used by many organizations for mandatory or discretionary access controls, depending on the role and privileges of the users in the organization (40).

FGAC or Fine Grained Access Control is a mechanism to implement a transparent security policy. It is an efficient mechanism for ensure security while avoiding rewrites or modifications of applications written against the database (41).

Access Methods:

OpenID refers to an open standard and decentralized authentication protocol. It allows users to be authenticated by co-operating sites, using a third-party service and eliminates the need for webmasters to have their own login systems. It also permits users to log in to multiple websites without using a separate ID and password for each (42).

XACML or eXtensible Access Control Markup Language is a fine-grained, attribute-based access control policy language. It is a processing model describing how to evaluate access requests according to the published rules, regulations and policies for XACML (43).

Shibboleth is a single log-in protocol for computer networks and the Internet. It allows people to log in, using just one identity to various systems run by groups of federated organizations or institutions, such as universities or public service institutions (44).

The major advantages of applying security solutions to cloud-based information systems are listed in Table 2.

Table 2: Advantages of Security Solutions in Cloud Computing Technology

Solutions	Advantages
Security Protocols	• Capable of expansion and advancement • Executable on every transmission protocol • Not limited by programming models
Encryption Techniques	• Improving authentication methods • Compressed messages and transmittable information • Non-reputation ability • Improving digital signature methods • Enhancing encrypted data communication
Access Control Mechanisms and Methods	• Open, decentralized standard • Authentication ability for all security services • Enhancing the systems integrity • Accurate identification and management of users • Efficient number of authorized access and service fees determination
Regulations & Policies	• Consistency in security architecture per region • Consistency in the use of security solutions • Improving systems consistency • Enhancing the role of security policy makers

Methods and Solutions in Cloud-based Health Information Projects: Similar to other business sectors, healthcare industry has enjoyed the many services available by cloud computing system. Studies have shown that the application of cloud computing services is welcomed in many healthcare programs and is on the rise in various countries worldwide. This section presents the details on the types and methods of security solutions used in the architecture of cloud-based health information communication (Table 3).

Table 3: Security Solutions Used in Healthcare Information Projects

Project	Cloud Type (Service Type)	Security Standards	Security Protocols	Encryption Techniques	Regulations & Policies	Access Control Mechanisms & Methods
1(45)	Private (PaaS & SaaS)		✓			✓
2(46)	Public (SaaS)	✓	✓	✓		
3(47)	Private (SaaS)		✓			✓
4(48)	Community (SaaS)	✓	✓			
5(49)	Private (SaaS)	✓	✓			
6(50)	Public (SaaS)	✓		✓		
7(51)	Public (SaaS)	✓				✓
8(52)	Public (SaaS)				✓	✓
9(12)	Public& private (SaaS)		✓	✓		✓
10(53)	Private (SaaS)		✓			✓
11(54)	Public (SaaS)					✓
12(55)	Private (SaaS)		✓			
13(7)	Public (SaaS)		✓		✓	✓
14(56)	Private (SaaS)		✓			
15(57)	Private (SaaS)		✓	✓		✓

3. Discussion

Security challenges facing cloud computing technology, particularly in healthcare industry, can affect the advantages, efficacy and application of this technology by many users worldwide. The type of cloud impacts the choice of security solutions and techniques, and the architecture of the cloud-based information system. In the architecture of projects that use public clouds for service provision (12, 13, 46, 47), the security protocols and encryption are highly emphasized to prevent unauthorized access to the information. This enhances the system's trustworthiness for the users to transmit and receive their confidential information. However, in projects that provide services through private clouds (45, 49, 53, 55), less encryption and security techniques are used, due to the small work environments and limited number of individuals using the system.

Solutions to control access exist in the architecture of the majority of security projects (7, 12, 45, 47, 51-54, 57), and the cloud type does not have much influence over the choice of solutions. Ordinarily, SSO is popular in projects using public clouds as the access control solutions, whereas ACL is generally employed by those on private clouds, with limited and easily identifiable users and defined privileges for access.

Regulations and policies have not been emphasized and enforced as much in the majority of projects using cloud computing technology (7, 52), despite the fact that governments and policy makers can and should play an important role in this context. Indeed, the shortage of regulations and policies for the new technology can affect its growth and application in the society. Whereas development and implementation of clear and enforceable regulation and policies can minimize if not eliminate much potential conflicts in the application of cloud computing in many public and private sectors including healthcare industry (33).

4. Conclusions

Using appropriate security solutions in the design and development of cloud-based health information system enhances the trust and confidentiality of the service users. Also, having a secure internet environment for information exchange and collaboration stimulates the participation and constructive interactions among healthcare institutions. The findings of this systematic review indicate that the best and plausible approach to develop an enhanced security for the provision of cloud-based health information would be combining several security solutions. Such an approach not only ensures the confidentiality of private information but also provides immense capability and potentials for professional collaborations among healthcare institutions, locally, regionally and globally. Applying multiple solution techniques to the system improves the health information security, accessibility, architecture and the satisfaction, and significantly reduces or eliminates potential threats to the security of highly private information.

Acknowledgements

The authors greatly appreciate Dr. Kamran Tavakol, Professor Emeritus, School of Medicine, University of Maryland, Baltimore, MD, USA, for translating this manuscript into English from the original Persian version. The current study was extracted from a doctoral dissertation project, supported by a grant (IUMS/SHMIS/I-2016/9223668202) provided by Iran University of Medical Sciences, International Campus, Tehran, Iran.

References

[1] Patel A, Taghavi M, Bakhtiyari K, JúNior JC. An intrusion detection and prevention system in cloud computing: A

systematic review. Journal of network and computer applications. 2013;36(1):25-41.
[2] Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems. 2009;25(6):599-616.
[3] Fernando N, Loke SW, Rahayu W. Mobile cloud computing: A survey. Future generation computer systems. 2013;29(1):84-106.
[4] Silva LAB, Costa C, Oliveira JL. A common API for delivering services over multi-vendor cloud resources. Journal of Systems and Software. 2013;86(9):2309-23017.
[5] Pino C, Di Salvo R, editors. A survey of cloud computing architecture and applications in health. International Conference on Computer Science and Electronics Engineering; 2013: Citeseer.
[6] Junior E. Teleradiology: Central Remote Diagnostic Imaging Digital Integrated Portal to a Distributed Medical Information. Application of public. Federal University of São Paulo, São Paulo. 2009.
[7] de Souza RF, Westphall CB, dos Santos DR, Westphall CM, editors. Challenges of Operationalizing PACS on Cloud Over Wireless Networks. ICWMC 2013; 2013.
[8] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation computer systems. 2012;28(3):583-592.
[9] Gul I, Hussain M. Distributed cloud intrusion detection model. International Journal of Advanced Science and Technology. 2011;34(38):135.
[10] Xiao Z, Xiao Y. Security and privacy in cloud computing. IEEE Communications Surveys & Tutorials. 2013;15(2):843-859.
[11] Prakash K. A Survey On Security and Privacy in Cloud Computing. International Journal of Engineering Research & Technology. 2013;2(2):1-9.
[12] Monteiro EJM, Costa C, Oliveira JL. A Cloud Architecture for Teleradiology-as-a-Service. Methods of information in medicine. 2016;55(03):203-214.
[13] Viana-Ferreira C, Costa C, editors. A cloud based architecture for medical imaging services. e-Health Networking, Applications & Services (Healthcom), 2013 IEEE 15th International Conference on; 2013: IEEE.
[14] Jensen M, Schwenk J, Gruschka N, Iacono LL, editors. On technical security issues in cloud computing. Cloud Computing, 2009 CLOUD'09 IEEE International Conference on; 2009.
[15] Stouffer K, Falco J. Guide to supervisory control and data acquisition (SCADA) and industrial control systems security: National institute of standards and technology; 2006.
[16] Kim S, Seong Leem C. Security of the internet-based instant messenger: risks and safeguards. Internet Research. 2005;15(1):88-98.
[17] At available at: http://www.iso27001security.com/html/27001.html [
[18] International Organization for Standardization (ISO). ISO/IEC 27000 Information security management http://www.iso.org/iso/home/standards/management-standards.htm.
[19] Mildenberger P, Eichelberg M, Martin E. Introduction to the DICOM standard. European radiology. 2002;12(4):920-927.
[20] Bogdan O, Alin C, Aurel V, Serban M. Integrated medical system using DICOM and HL7 standards. New Advanced Technologies: InTech; 2010.
[21] Winkler VJ. Securing the Cloud: Cloud computer Security techniques and tactics: Elsevier; 2011.
[22] Jestratjew A, Kwiecien A. Performance of HTTP Protocol in Networked Control Systems. IEEE Transactions on Industrial Informatics. 2013;9(1):271-276.
[23] Moore K. Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs). 2002. Report No.: 2070-1721.
[24] Malcolm J, Smith N. Method and apparatus for filling out electronic forms. Google Patents; 2002.
[25] At available: https://www.techopedia.com/definition/1891/html5 [
[26] At available: https://searchnetworking.techtarget.com/definition/TCP-IP.
[27] Kuo AM-H. Opportunities and challenges of cloud computing to improve health care services. Journal of medical Internet research. 2011;13(3).
[28] Fernández-Cardeñosa G, de la Torre-Díez I, López-Coronado M, Rodrigues JJ. Analysis of cloud-based solutions on EHRs systems in different scenarios. Journal of medical systems. 2012;36(6):3777-3782.
[29] Agrawal M, Mishra P. A comparative survey on symmetric key encryption techniques. International Journal on Computer Science and Engineering. 2012;4(5):877.
[30] Mein G, Pal S, Dhondu G, Anand TK, Stojanovic A, Al-Ghosein M, et al. Simple object access protocol. Google Patents; 2006.
[31] Fielding R, Reschke J. Hypertext transfer protocol (HTTP/1.1): Message syntax and routing. 2014. Report No.: 2070-1721.
[32] Freier A, Karlton P, Kocher P. The secure sockets layer (SSL) protocol version 3.0. 2011. Report No.: 2070-1721.
[33] Fern'ndez G, De La Torre-díez I, Rodrigues JJ, editors. Analysis of the cloud computing paradigm on mobile health records systems. Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on; 2012: IEEE.
[34] Mgozi T, Weeks R, ERASMUS L, editors. Cloud computing impact on healthcare in South Africa. 24th International Association for Management of Technology Conference: Technology, Innovation and Management for Sustainable Growth, IAMOT, Cape Town, June 8; 2015.
[35] Available at: https://www.hhs.gov/hipaa/index.html.
[36] Leandro MA, Nascimento TJ, dos Santos DR, Westphall CM, Westphall CB, editors. Multi-tenancy authorization system with federated identity for cloud-based environments using shibboleth. Proceedings of the Eleventh International Conference on Networks; 2012.
[37] Marcu R, Popescu D, editors. Security solution for healthcare hybrid cloud platform. System Theory, Control and Computing (ICSTCC), 2014 18th International Conference; 2014: IEEE.
[38] 38. Neuhaus C, Polze A, Chowdhuryy MM. Survey on healthcare IT systems: standards, regulations and security: Universitätsverlag Potsdam; 2011.

[39] Sandhu RS, editor The typed access matrix model. Research in Security and Privacy, 1992 Proceedings, 1992 IEEE Computer Society Symposium on; 1992: IEEE.
[40] Kuhn DR, Coyne EJ, Weil TR. Adding attributes to role-based access control. Computer. 2010;43(6):79-81.
[41] Shen H-b, Hong F, editors. An attribute-based access control model for web services. Parallel and Distributed Computing, Applications and Technologies, 2006 PDCAT'06 Seventh International Conference on; 2006: IEEE.
[42] Koutelakis GV, Lymperopoulos DK, editors. PACS through web compatible with DICOM standard and WADO service: advantages and implementation. Engineering in Medicine and Biology Society, 2006 EMBS'06 28th Annual International Conference of the IEEE; 2006: IEEE.
[43] eXtensible Access Control Markup Language (XACML) Version 3.0 (2013), http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html
[44] Ying W, editor Research on multi-level security of shibboleth authentication mechanism. Information Processing (ISIP), 2010 Third International Symposium on; 2010: IEEE.
[45] Yang C-T, Chen L-T, Chou W-L, Wang K-C, editors. Implementation of a medical image file accessing system on cloud computing. Computational Science and Engineering (CSE), 2010 IEEE 13th International Conference on; 2010: IEEE.
[46] Teng C-C, Mitchell J, Walker C, Swan A, Davila C, Howard D, et al., editors. A medical image archive solution in the cloud. Software Engineering and Service Sciences (ICSESS), 2010 IEEE International Conference on; 2010: IEEE.
[47] Silva LAB, Costa C, Silva A, Oliveira JL, editors. A PACS Gateway to the Cloud. Information Systems and Technologies (CISTI), 2011 6th Iberian Conference on; 2011: IEEE.
[48] Yao Q, Han X, Ma X-K, Xue Y-F, Chen Y-J, Li J-S. Cloud-based hospital information system as a service for grassroots healthcare institutions. Journal of medical systems. 2014;38(9):104.
[49] Ukis V, Rajamani ST, Balachandran B, Friese T, editors. Architecture of cloud-based advanced medical image visualization solution. Cloud Computing in Emerging Markets (CCEM), 2013 IEEE International Conference on; 2013: IEEE.
[50] Hsu Y-C, Hwang J-J, editors. Controlling Decryption of Personal Health Records in the Cloud. Proceedings of the International Conference on IT Convergence and Security 2011; 2012: Springer.
[51] Hillestad R, Bigelow J, Bower A, Girosi F, Meili R, Scoville R, et al. Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. Health affairs. 2005;24(5):1103-1117.
[52] Patil MS. A review on enhancing healthcare system using cloud computing. International Journal of Computer Applications (0975–8887), Innovations and Trends in Computer and Communication Engineering (ITCCE). 2014.
[53] Ma W, Sartipi K, editors. Cloud-based Identity and Access Control for Diagnostic Imaging Systems. Proceedings of the International Conference on Security and Management (SAM); 2015: The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
[54] Ma W, Sartipi K, Sharghi H, Koff D, Bak P, editors. OpenID connect as a security service in Cloud-based diagnostic imaging systems. Medical Imaging 2015: PACS and Imaging Informatics: Next Generation and Innovations; 2015: International Society for Optics and Photonics.
[55] Valente F, Viana-Ferreira C, Costa C, Oliveira JL. A RESTful image gateway for multiple medical image repositories. IEEE Transactions on Information Technology in Biomedicine. 2012;16(3):356-364.
[56] Reddy ANG, Bhatnagar R, editors. Distributed medical image management: A platform for storing, analysis and processing of image database over the cloud. Advances in Energy Conversion Technologies (ICAECT), 2014 International Conference on; 2014: IEEE.
[57] Marwan M, Kartit A, Ouahmane H, editors. A secure framework for medical image storage based on multi-cloud. Cloud Computing Technologies and Applications (CloudTech), 2016 2nd International Conference on; 2016: IEEE.

Authors' Brief Biographies

Mohsen Tabatabaei completed two undergraduate studies (B.A., 2003; B.S., 2005) with a focus on Medical Records at Kashan and Kerman Universities of Medical Science, respectively, in Iran. He pursued his graduate studies at Iran University of Medical Sciences, Tehran, Iran, where he received his M.Sc. degree in Medical Record Education. He is currently in the final stage of his Ph.D. studies, awaiting the thesis defense in Fall 2018. His research interests focus on medical informatics, health information systems, and telemedicine.

Mostafa Langarizadeh received his M.Sc. degree in Medical Record Education (2001) at Iran University of Medical Sciences, Tehran, Iran. He later received a PhD degree in Medical Informatics (2011) at University Putra Malaysia, Kuala Lumpur, Malaysia. His research interests include artificial intelligence and computer applications in medicine. Currently, he is an Assistant Professor in the School of Health Management and Information Sciences, Iran University of Medical Sciences, Tehran, Iran. He has supervised Mr. Tabatabaei's thesis project.

Mohammad Kazem Akbari received his B.Sc. degree in Computer Engineering (1983) from Shahid Beheshti University, Tehran, Iran. He later pursued his graduate studies (M.Sc., 1990; Ph.D., 1994) in Computer Science at Case Western University, Cleveland, Ohio, USA.
His research interests include computer systems architecture, electronic commerce, cloud computing, and ultrafast data processing. Currently, he is an Associate Professor in the Department of Computer Engineering and Information Technology, Amirkabir University. Tehran, Iran. He has co-advised Mr. Tabatabaei's on his thesis project.