Journal of King Saud University – Computer and Information Sciences (2017) **29**, 281–287

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

Design of cloud security in the EHR for Indian healthcare services

Pradeep Deshmukh

Rajarshi Shahu College of Engineering, Thathawade, Pune 33, India

Received 17 March 2015; revised 10 January 2016; accepted 13 January 2016
Available online 29 March 2016

KEYWORDS

Cloud computing;
EHR;
Encryption;
Decryption;
Cloud security;
Health record

Abstract An ease of data or record sharing at will has compelled most of the physicians to adopt EHR (Electronic Health Record) for record-keeping of patients. It also makes convenient to the other stake holders of healthcare ecosystem such as nurses, specialists and patient. Due to lower costs and scalability of application, the cloud is becoming the infrastructure for most of the EHR but without comprising the privacy of data. In this paper we have proposed a frame work for storing the health records and accessing them by patients and physicians as authorized by key-control scheme. The scenarios we have considered here are of rural and urban health care centers and hence more appropriate for Indian health care services. The proposed scheme has double data security by introducing isolation between encryption schemes of transmitted data and stored data. The experimental result shows that it has a capability of scaling in number of patients and also no of elements in health record.

1. Introduction

For improving safety, quality and efficiency of patient care and reducing healthcare delivery costs, both EMRs (Electronic Medical Records) and EHRs Electronic Health Records are critical to the grand vision of healthcare digitization. To provide a documented record of care which supports both present and future care received by the patient from the same or other clinicians or Care providers, is the primary purpose of the EHR. This EHR provides means of communication between patients and clinicians. For EMRs to reach their full potential in revolutionizing the healthcare delivery with high quality and affordable costs, the interoperability of EHRs is a fundamental enabling technology.

In this paper, we proposed the design of EHR system and its access control management, especially, suitable for a mass populated country like India. We also presented the privacy preserving mechanism based on privacy homomorphism (PH). The scenarios we have considered here are of rural and urban health care centers and hence more appropriate for Indian health care services. We perform the experiments with cloud environment and found the system suitable for scalable and flexible requirements of health management system in India. The proposed scheme has double data security by introducing isolation between encryption schemes of transmitted data and stored data.

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2016.01.002

2. Literature survey

The Szolovits et. al. in 1994 introduced the concept of patient-centered health record to be stored in web based system. For sharing and authentication, Hu et al. (2010) presented the use of public key infrastructure (PKI) in order to maintain the confidentiality of the health records. A similar work has also been presented in Yu and Chekhanovskiy (2007). In order to provide the security and privacy of EHR, cryptographic key management has been discussed in Lee and Lee (2008). In particular, hierarchical identity-based encryption and privacy preserving EHR system based on cloud is used in Benaloh et al. (2009). The trade-off between real time performance and security levels has been considered in Takabi et al. (2010) for cloud based EHR systems.

The trust is one of the main concerns of the users Shen et al. (2010) and it requires the complexity of the security mechanism be at a minimum so that it will not be difficult for the users to use the system. The various vulnerabilities have been examined in Li et al. (2010). To analyze the risk in third party clouds, Popovic and Hocenski (2010) discuss challenges, security issues and requirements that Cloud Service Providers (CSP) face during cloud engineering. Few critical concerns of Cloud computing have been identified by Xiao and Xiao in Xiao and Xiao, 2013. The requirements for achieving privacy and security for data sharing in cloud have been discussed by Chen and Zhao (2012).

A survey focusing on how privacy laws should also take into consideration Cloud computing and to prevent security and privacy breaches of one's personal data in the Cloud what work can be done is provided by Zhou et al. (2010). Factors affecting management of information security in Cloud computing has been explored by Wang et al. (2011). To understand the dynamics of information security in the Cloud the necessary security needs for enterprises are explained by it. Among enterprises through pilot testing privacy/security compliance a study on privacy and security compliance of Software-As-A-Service (SaaS) is carried out by Wang (2011). To determine the user experience of Cloud computing a survey is carried out on a number of users by Oza et al. (2010) and found that the trust and how to choose between different Cloud Service Providers was the main issue of all users.

The impact of the Internet on data sharing is reviewed by Sarathy and Muralidhar (2006) across many different organizations such as businesses and government agencies into record matching, data dissemination and query restriction. The data is classified by them for secure and useful sharing of data on the internet. They also provide a framework. The issues of data sharing on the Internet are described by Butler (2007) where details about users are allowed to infer by sharing information. This is helpful as it raises awareness to organizations about the privacy issues of the data they choose to share with the public and the confidentiality of its users is not guaranteed. From a banking perspective the benefits of data sharing are described by Mitchley (2006) and the privacy issues still affecting it are highlighted. The important benefit of data sharing is discussed by Feldman et al. (2012) in terms of professional development, public health and in particular for education. A list of organizations that effectively secure and share information via the Cloud is discussed by Geoghegan (2012). A number of different access control models and evaluation of their effectiveness are surveyed by Sahafizadeh and Parsa (2010).

In most of the existing methods, the security has been considered at data level without considering the data networking and data storage separately. This gives the two hackers two places where data can be hacked comprising security and privacy of EHR. To over come this problem, we considered double encryption system, separately for data communication and data storage. Doing so, even if at all data are hacked while data in communication channel, theft doesn't get propagated to cloud.

3. Methodology

The question of security with conventional device based EHR arises because of theft of unencrypted computers, portable devices and media used to store patient records. Cloud-based EMR does not suffer from this problem, since the data are stored on a remote server instead of directly on the device. The lower cost and security against the data theft has made physicians and EHR vendors to migrate from their desktop EHR to cloud based EHR. The cloud based EHR will play an important role in connecting the various EHRs of all health care centers and will remove the drawbacks of the current system.

3.1. Indian scenario and EHR

The need of EHR in the mass population of India is inevitable. The involvement of citizens across the countries in health record leads to the inclusive health care system for that country. Different languages are being used in different parts of or states of India. Thus converting EHR from one language to another language is very much possible at one click on electronic device. The language translator APIs also become cheaper to be employed in the EHR system based on cloud due to mass subscription base. The literacy is an issue in the encouragement of using the EHR system. However, the literacy rate of India is growing year by year and it is visible from the census records of the decades from the time of independence of India. From year 1951 to 2011, the literacy rate goes from 20% to 80%. This trend clearly shows within this decade (till 2021) the Indian literacy rates will touch to 100%, enabling the positive environment for using the EHR for all the citizens of India. The high literacy will drive most people to get acquainted with mobile device and computers. Additionally, most of population of India is English speaking as compared to other developing countries. This also gives the added advantage to the suitability of EHR in Indian health care system.

3.2. EHR system architecture

One of the templates of the integrated health care system has been considered here to give an example of EHR, where cryptography can be used to secure the access of data stored in the cloud. The proposed architecture with hierarchy and cloud connectivity of the EHR network is shown in Fig. 1. In this scenario, various elements of health care services are included for representing the population of one district of India. The same EHR can be replicated in the most of the districts as it

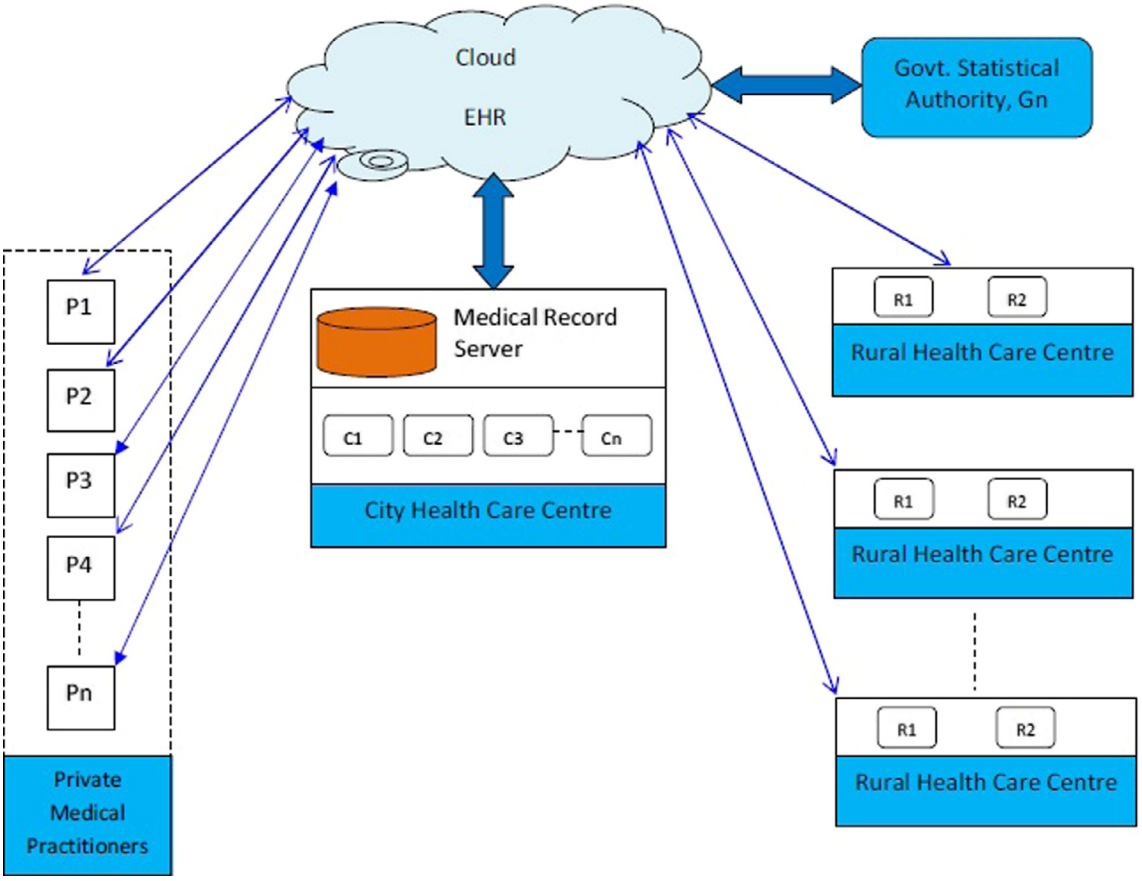


Figure 1 Proposed EHR access network on cloud in Indian context.

is or with few modifications. Thus, the example considered here is a good indicator of the unit of the overall health care services in India. In general, the health care services are divided as Urban (City) Health Service Centers (CHSC) and Rural Health Service Centers (RHSC). As compared to City health services, Rural health services will be very basic and less advanced. The treatment with specialized health services in physician and equipment point of view will not be available in most parts of the rural area. The differentiation in physicians is based on their affiliation to either the government health care centers or private clinics. The private practitioners either from rural area or city area can be put in the single category of private physicians. Rural health care units and Private medical practitioners are directly connected to the cloud-EHR. City health service center will have its own server and thus, any member of cloud-EHR from the city health center will access the data from cloud via medical server. The need of having medical server is that the city health center will have normally many health departments and medical and nursing college co-located with it. Thus, access management to the staff members or students of city health care center will put extra burden on the cloud management. In order to avoid this burden, access control in city health care center can be isolated using dedicated server. The multiple level of access management associated with hierarchical member entities can be an approach to achieve the key management for medical server. Thus, most of the requests from members of city health care will be verified and authorized for particular operations at server level and only after validating request positively, it will be forwarded to the cloud-EHR. An urban health care center is generally attached with medical institute. Hence, city health care center will have its own medical record server. The use of this medical record server is very complicated as there are different types of stakeholders involved in it. The essential set of primitives, namely, encryption and decryption, while writing and reading the data are shown in Fig. 2.

3.2.1. Pairing

the patient chooses to give the authority to one physician to access his/her medical record on the cloud any time. This is done by pairing the secret keys of both into the key access management scheme. This is expected to be done at the time registration of patient. Pairing is static and stored in key access management Table 1.

3.2.2. Assertion

Whenever a patient wants to give access to any physician to access the health record history the patient does so actively after logging into the users account. Assertion is dynamic and after it is raised, it gets deactivated after the record entry or predefined time.

(1) This operation enables writing the current patient record on to cloud. Patient record is strictly entered by an authorized physician. In this operation, the

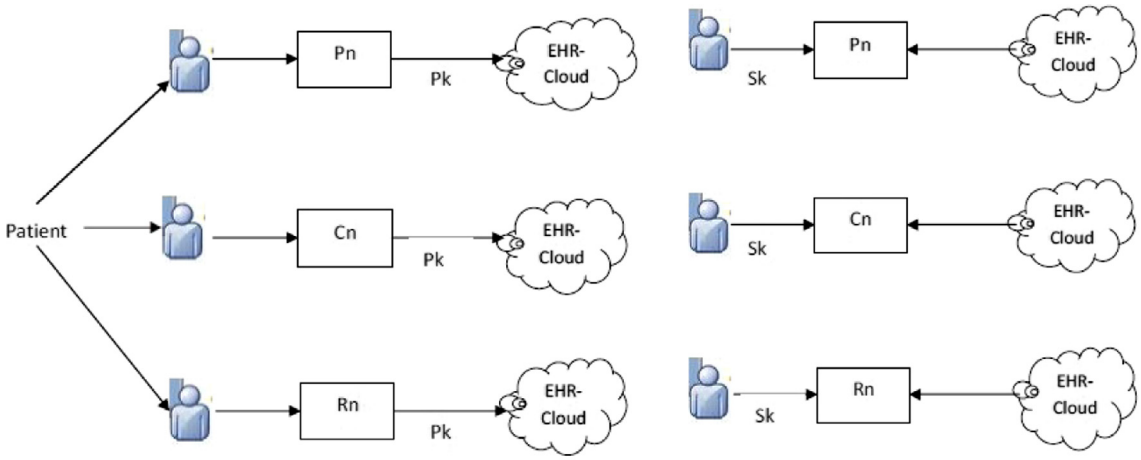


Figure 2 (Left) Write operation for health record after treatment, P_K is public key; (Right) read operation for health record history after treatment, S_K is private/secret key.

Table 1 Key-access management.

Patient location	Rural physician, Rn		City physician, Cn		Private physician, Pn	
	Write-record	Read-history	Write-record	Read-history	Write-record	Read-history
City-registered	(Sk, Assertion)	(Sk, Assertion)	Pairing	Pairing	(Sk, Assertion)	(Sk, Assertion)
Pairing	Pairing	City-registered	(Sk, Assertion)	(Sk, Assertion)	(Sk, Assertion)	(Sk, Assertion)

physician has to have rights to write the patient record for that particular patient. With the public key associated with patient's secret key, the text of patient record is encrypted and stored into the cloud element. Patients can read the past health record any time. However, a physician can access this record only when the patient performs assertion or the physician is paired with that patient.

(2) This operation is similar to the first data access operation. However, a physician C_n has to write the record via medical record system server of the city health care center. This medical record server manages the write and read operation for any physician C_n. The record written by a physician C_n can also be read by other physicians as allowed by key access management, specifically by paring or assertion.

(3) This data access operation allows a rural practitioner, R_n, to write patient records on cloud with patient key. However, a rural practitioner R_n can access the patient record history only when he/she is already paired with the patient. If not, the patient has to raise the assertion.

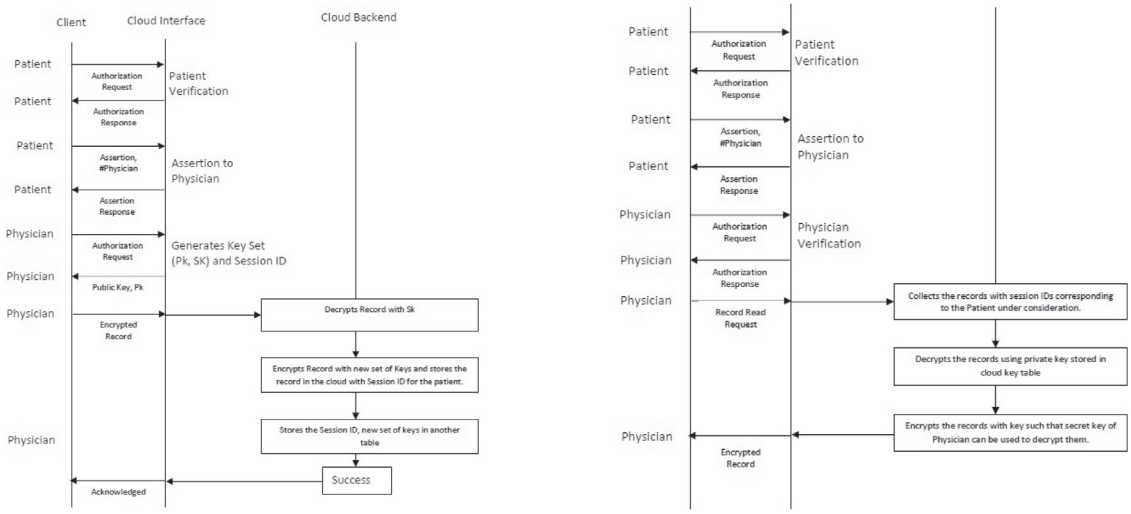
3.3. Cross-authority access & privacy mechanism

When the patient and physician are not paired and situation demands the physician to access that patient's health history, assertion raised by the patient is required. Assertions can be even raised by family members or the companion of patient in case the patient is not in a position to do so. In other situations, normally, the government wants to do health survey, statistics and analysis of citizens. In this case, government authorized member, G_n, can send the queries in high level and corresponding queries are fired at the server. This will be enabled by allowing government authority, G_n, to the data mining or statistical API only and not by giving access to the users' health history records exclusively.

There is also another way of giving access to government authorities to do the survey or analyze statistics of health care system without comprising the privacy of patient data. The range based queries for understanding the data can be processed with privacy preserving algorithms. The secure query processing approach based on privacy homomorphism (PH) is encouraged from Hu et al. (2011) and Domingo-Ferrer (2002). Domingo-Ferrer described PH and proposed a provably secure privacy homomorphism under the set of operations, i.e., modular addition, subtraction and multiplication. Thus, it is named as ASM-PH after its supported operations.

3.4. Write-record operation

While writing the health record on EHR that exist on a cloud, first authorization process is carried out between the credentials of patient and physician. The handshake signals and data access timing diagram for Write-Record Operation is shown Fig. 3a. Once successful verification of patient and physician due to either pairing or assertion happens, the cloud process generates the set of public and private keys and sends the public key to the physician's client device. He then enters the health record, which gets encrypted by device process and sends out the encrypted record to the cloud. Next, cloud decrypts the data with private key and again re-encrypts the data with the keys that are known to the cloud only. It then stores the data along with header information and record keys.



(a) Record-Write Timing Diagram

(b) Record-Read Timing Diagram

Figure 3 Timing diagrams a) Record-Write Cycle and b) Record-Read Cycle.

3.5. Read-record operation

The read-record operation is illustrated with handshake signals and data timing flow in Fig. 3b. Once the patient and physician authorization is successfully verified either by pairing or assertion, physician sends the request to read the health record along with patient id and range of records. Cloud process accesses the encrypted records corresponding to the patient id and range of records info. These records are first decrypted and then the public key and private key pair are generated such that the private key matches with physician key. Then, the record is encrypted with newly generated public key.

This includes the encrypting transmitted messages and stored messages with different sets of private and public keys. This scheme ensures the better security of the stored data in the sense that even if the transmitted message is exposed to the intruder, the stored message on the cloud will be safe. Since encrypted message in the cloud is exposed to the transmission, a set of keys message can be used in multiple cloud stored messages. This increases the number of keys available for encryption leading to an increase in the number of users and messages to be handled in the secure EHR system.

4. Experimental results and discussion

The authorization is normally done by using key management using access control schema which is shown in a typical case in Table 1. The security analysis of encryption methods and computational complexity for measuring time performance are discussed here.

4.1. Security analysis

In this section, we investigate the security of proposed access control mechanisms. The proposed EHR system uses text-based cryptographic schemes and numeric operation based privacy preserving approach. The text-based encryption is used for health record at the network and storage. The various encryption schemes can be used like AES (Advanced Encryption Scheme), ID based encryption, Attributes based Encryption or Predicate based Encryption; though we have used here Elgamal algorithm for text encryption. Every algorithm will have security analysis in their way. Similarly, Elgamal algorithm has a security analysis depending on the parameters, key generation infrastructure and type of implementation. The suitability of particular encryption algorithm depends on the requirements of specific EHR system. However, main concern of EHR system is to have simple structure of passwords and thus, attribute based or predicate based cryptographic algorithms are more suitable. In these types of cryptographic schemes, public/private key generators play a critical role.

4.2. Performance analysis

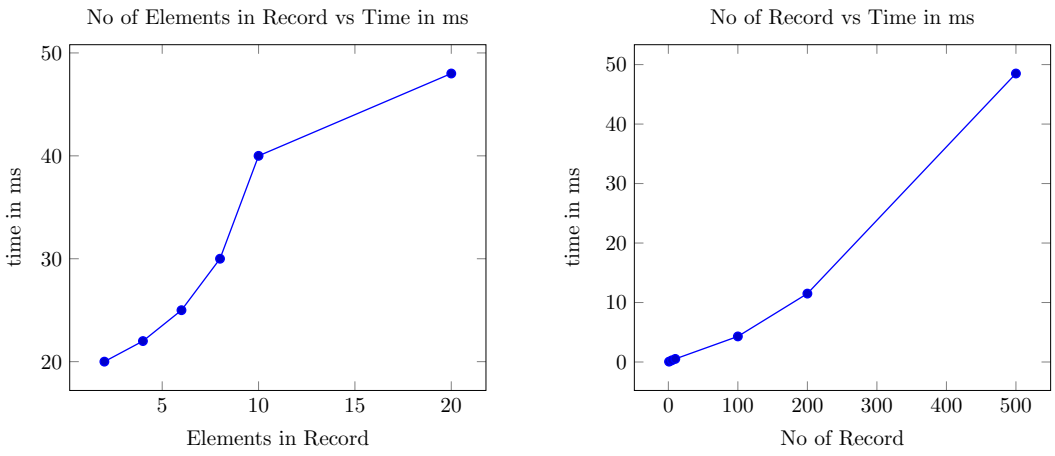
The record for any patient is composed of various information elements. The records were stored in database and fields of

Table 2 Time performance for read–write cycle of record with different number of elements.

	No of elements in record					
	2	4	6	8	10	20
Time in ms	20	22	25	30	40	48

Table 3 Time performance for number of record read by client node.

	No of records					
	1	5	10	100	200	800
Time in sec	0.6	0.28	0.52	4.3	11.5	48.5



(a) No of Elements in Record vs Time in ms (b) No of Records vs Time in ms

Figure 4 The performance graphs: a) Time vs No of Elements, b) Time vs No of records.

table were decided from the real clinic paper items like chief complaint, symptoms, prescription, lab measured health parameters along with patient information. The experiments are repeated for different numbers of elements in the record and respective times to write and read cycle of record are noted down. Collectively, the data are first written on the cloud and same data are read on the client device by accessing them from the cloud. The timing performance obtained in this experiment for the number of elements is shown in Table 2. We also experimented with a number of records from health history and time for the same is analyzed. The results for various numbers of records are shown in Table 3.

The access time performance for different numbers of elements in the record in the EHR with cloud is shown in Table 2 and plotted in Fig. 4a. It can be seen that the proposed scheme is scalable for the number of elements in the health record. The time for accessing the record including encryption and decryption is almost linear. The slope of linearity is varying due to different sizes of elements being accumulated in the record. The access time performance for different numbers of records is shown in Table 3 and plotted the graph in Fig. 4b. As the no. of records increases the time to access it linearly increases. It has been observed that the proposed scheme of health record security is scalable for a large number of health records.

5. Conclusion

Due to lower costs and scalability of application, the cloud is becoming the infrastructure for most of the EHR. However, it is important to store the data in cloud with high degree of security such that privacy of patients cannot be compromised. In this paper, we have proposed a frame work for storing the health records and accessing them by patient and physician as authorized by key-control scheme. The scenarios we have considered here are of rural and urban health care centers and hence more appropriate for Indian health care services. The proposed scheme has double data security by introducing isolation between encryption schemes of transmitted data and stored data. The experimental result shows that it has a capability of scaling in number of patients and also no. of elements in health record and is suitable for large population.

References

Benaloh, Josh, Chase, Melissa, Horvitz, Eric, Lauter, Kristin, 2009. Patient controlled encryption: ensuring privacy of electronic medical records. In: Proceedings of the 2009 ACM Workshop on Cloud Computing Security. ACM, pp. 103–114.

Butler, Declan, 2007. Data sharing threatens privacy. Nat. News 449 (7163), 644–645.

Chen, Deyan, Zhao, Hong, 2012. Data security and privacy protection issues in cloud computing. In: 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), vol. 1. IEEE, pp. 647–651.

Domingo-Ferrer, Josep, 2002. A provably secure additive and multiplicative privacy homomorphism. In: Proc. 5th International Conference on Information Security.

Feldman, Lindsay, Patel, Deesha, Ortmann, Leonard, Robinson, Kara, Popovic, Tanja, 2012. Educating for the future: another important benefit of data sharing. Lancet 379 (9829), 1877–1878.

Geoghegan, S., 2012. The latest on data sharing and secure cloud computing. Law Order, 24–26.

Hu, Jiankun, Chen, Hsiao-Hwa, Hou, Ting-Wei, 2010. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. Comput. Stand. Interfaces 32 (5), 274–280.

Hu, Haibo, Xu, Jianliang, Ren, Chushi, Choi, Byron, 2011. Processing private queries over untrusted data cloud through privacy homomorphism. In: 2011 IEEE 27th International Conference on Data Engineering (ICDE), pp. 601–612.

Lee, Wei-Bin, Lee, Chien-Ding, 2008. A cryptographic key management solution for HIPAA privacy/security regulations. IEEE Trans. Inf. Technol. Biomed. 12 (1), 34–41.

Li, Huan-Chung, Liang, Po-Huei, Yang, Jiann-Min, Chen, Shiang-Jiun, 2010. Analysis on cloud-based security vulnerability assessment. In: 2010 IEEE 7th International Conference on e-Business Engineering (ICEBE). IEEE, pp. 490–494.

Mitchley, M., 2006. Data sharing: progress or not. Credit Manage., 10–11

Oza, Nilay, Karppinen, Kaarina, Savola, Reijo, 2010. User experience and security in the cloud – An empirical study in the finnish cloud consortium. In: 2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, pp. 621–628.

Popovic, Kresimir, Hocenski, Zeljko, 2010. Cloud computing security issues and challenges. In: MIPRO, 2010 Proceedings of the 33rd International Convention. IEEE, pp. 344–349.

Sahafizadeh, Ebrahim, Parsa, Saeed, 2010. Survey on access control models. In: 2010 2nd International Conference on Future Computer and Communication (ICFCC), vol. 1. IEEE, pp. V1–1.

Sarathy, Rathindra, Muralidhar, Krishnamurty, 2006. Secure and useful data sharing. Decis. Support Syst. 42 (1), 204–220.

Shen, Zhidong, Li, Li, Yan, Fei, Xiaoping, Wu., 2010. Cloud computing system based on trusted computing platform. In: 2010 International Conference on Intelligent Computation Technology and Automation (ICICTA), vol. 1. IEEE, pp. 942–945.

Szolovits, Peter, Doyle, Jon, Long, William J., Kohane, Isaac, Pauker, Stephen G., 1994. Guardian Angel: Patient-centered Health Information Systems. Massachusetts Institute of Technology, Laboratory for Computer Science.

Takabi, Hassan, Joshi, James B.D., Ahn, Gail-Joon, 2010. Security and privacy challenges in cloud computing environments. IEEE Secur. Priv. 8 (6), 24–31.

Wang, Yu-Hui, 2011. The role of SAAS privacy and security compliance for continued SAAS use. In: 2011 7th International Conference on Networked Computing and Advanced Information Management (NCM), pp. 303–306.

Wang, Jen-Sheng, Liu, Che-Hung, Lin, Grace T.R., 2011. How to manage information security in cloud computing. In: 2011 IEEE International Conference on Systems, Man, and Cybernetics (SMC). IEEE, pp. 1405–1410.

Xiao, Zhifeng, Xiao, Yang, 2013. Security and privacy in cloud computing. Commun. Surv. Tutorials, IEEE 15 (2), 843–859.

Yu, W.D., Chekhanovskiy, Mark A., 2007. An electronic health record content protection system using smartcard and PMR. In: 2007 9th International Conference on e-Health Networking, Application and Services. IEEE, pp. 11–18.

Zhou, Minqi, Zhang, Rong, Xie, Wei, Qian, Weining, Zhou, Aoying, 2010. Security and privacy in cloud computing: a survey. In: 2010 Sixth International Conference on Semantics Knowledge and Grid (SKG). IEEE, pp. 105–112.