World Applied Sciences Journal 32 (9): 1820-1827, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.32.09.1061

Securing Healthcare Records Using Proxy Re-Encryption Scheme in Cloud

[1]E. Sathiyamoorthy, [1]K. Govinda and [2]Sathiyamoorthy

[1]School of Computing Science and Engineering,
VIT University, Vellore, Tamil Nadu-632014, India
[2]School of Information Technology and Engineering,
VIT University, Vellore, Tamil Nadu-632014, India

Abstract: The advent of semi-conductors emerged day to day and lead us to the current trend of Cloud computing, which brings the information required to our life at our finger tips. The technology of today is getting expanded every day, especially in the management of EHR's. In order to provide high security for health care data we need a strong security mechanism for EHR, Proxy re-encryption schemes are cryptographic method which makes third party (proxy) to transform cipher text in one encrypted form to another, so that it is decrypted by receiving party's private key without revealing the original text to proxy. These schemes have many applications such as mail forwarding, access control in networked file storage and securing personal health records storage system (PHRS). PHRS is the storage of health information. The data in the system is not from one health center instead it is combined from various health centers. This collected storage data can be further usedby different health and research centers. Patient can share their personal health care information anytime and anywhere whenever required. According to person's confidentiality right on their own health related information needs to be maintained in a highly secured way by the system. In this paper an algorithm is proposed and implemented based ElGamalpublic key cryptographic method, this approach allows different re-encryptions for different users through proxy re-encryption.This is highly suitable for PHRS for different health centers.

Key words: Proxy re-encryption scheme · Personal health record system · Cloud computing · Cloud service provider

INTRODUCTION

Cloud Computing appears as a computational prototype as well as allocation structural design and its most important purpose is to make available protected, rapid, suitable data storage space and net computing examination, with all computing possessions visualized as services and delivered in excess of the Internet. The cloud enhances relationship, dexterity, scalability, accessibility, capacity to get used to fluctuations according to stipulate, increase speed expansion work and provides probable for cost decrease from end to end optimized and well-organized computing. Although the grid computing was at first meant for scientific and engineering purposes the expected desire of computer professionals was to take it to the social money-making domains. Data grids, medical grids etc were urbanized to meet the challenges of computer industry capitalizing on high capacity networks and announcement systems for electronic data processing and arrangement. In spite of many success stories of grid computing paradigms it lacked support of ecommerce.

PHR scheme is an appliance through which you can manage, right of entry and contribute to your health information in a confidential, secure and concealedenvironment. PHR systems are intended to put together the circulated information at a choice of medical and health center into one organization which can be used anytime and anywhere as approved by the entity. It contains all types of health connected information of an individual provided by various health centers such as surgery, injury, hereditary disease, illness, side effects, allergies, vaccination, etc. It also contains information about patient such as weight change, height rise, food chart, diet, etc. Such vital information of an individual is

Corresponding Author: K. Govinda, School of Computing Science and Engineering, VIT University, Vellore, India.

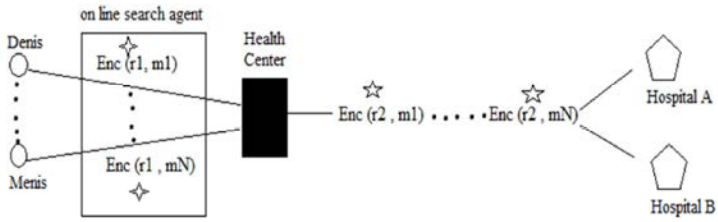

Fig. 1: Traditional approach

stored into it so it requirements to be protected. Some obtainable PHR systems such as Microsoft Health Vault and Google Health provide such services but they present whole or not anythingresources either they supply the entire PHR access to the medical providers or no solitary record access. An additional problem is refuge of data at server [1,2]. Cloud PHR will be appropriate to together hold the medical records and provide the compulsory services. The only difficulty of cloud is its open structural design so security is the major issue. So for security the proxy re-encryption scheme is used in which data is encrypted during transmissionfrom one form to other form without knowing the plaintext and the private key. The proxy transforms the cipher text for decryption to the intended user [3-5]. This makes it well-organized than others [6, 7].

Apart from the above so called realapprehension there is one furthersignificant concern in cloud PHR system.believe an instance – a patient named Denis needs to look for a health center through an online explorationmanager which accomplisha fewcircumstancessimilar to health center should be next toto his home (within 5km range), have skilled doctors (around of 5 years), have most brain cancerexpert doctors, have all AC accommodation. For privacy of his health information he encrypts his therapeuticdocumentation 'm' earlier sending to the agent [8]. mediator cannot decrypt m without knowing private key. Agent finds the matched heath center and he forwards m to health center. Center decrypts m with its private key so as to read Denis's medical record. If some hospitals require Denis's health record during treatment from health center, then first the center gets the m and then re- encrypt it and forward it to the hospitals which satisfy some conditions similar to above. If there are N numbers of patients than by traditional means center has N encryptions and decryptions which will be too complex for the health center.

So to make it efficient proxy re-encryption scheme is suggested in which different encryptions for different hospitals are not performed, only one encryption will be there by the center, different transforms of the cipher text will be there by the proxy for different hospitals to decrypt.

Related Work: The main problem in cloud PHRS is the security of individual's health information stored in it. Security includes confidentiality, authentication and integrity of the data.In PHR system the information provider's and the information users identity needs to be verified at every access. These authentications of the identities prevent the fake middle attackers. The consumers and the providers of the PHRS can deny their access or storage which might cause false health information storage or access so non – deniability should be imparted to prevent such fakes [9-11]. The power of sharing health information should be with individual health centers. That can decide who he wants to share his information. Data in the PHR cloud needs to be accurate and consistent. No unauthorized user can change the information. Also data in PHR cloud is confidential means only authorized and authenticated users can access the information.

Research on the various security and privacy issues close to healthcare information systems has been heated in recent times. ISO/TS 18308 standard gives the definitions of security and privacy issue for EHR [12]. The Working Group 4 of IMIA was set up to investigate the issues of data protection and security within the healthcare environment. It is mainly concentrated on security in EHR networked systems and common security solutions for communicating patient data [13]. The European AIM/SEISMED project is initiated to address a wide spectrum of security issues within healthcare and provides practical guidelines for secure healthcare establishment [14-16]. US HHS recently published a report about personal health records (PHRs), aiming at developing PHRs and PHR systems to put forward a vision that "would create a personal health record that patients, doctors and other health care providers could securely access through the WWW no matter where a patient is seeking medical care."

One unique concept in healthcare clouds is "patient-centric" view, which is a term used mostly in group of people healthcare systems. Community healthcare system offers an open platform for patient to collect, store, use and share health information in a forbidden manner with omnipresent ease of access. It also offers secure storage and supervision of patients' EHRs for multiple applications (e. g. disease treatment, lab research, insurance and other social-networking applications). Most of the community healthcare cloud service models, such as Microsoft Health Vault and Google Health, adopt a centralized architecture with patient-centric views. By patient-centric, it means that the information stored in the community EHR system is imported by patients and only can be made available to a variety of applications under the control of patients the common security issues shared by healthcare cloud applications are ownership of information, authenticity, authentication, non-repudiation, patient consent and authorization, integrity and confidentiality of data are discussed [17].

In [18] the authors clearly state the goal-based cloud resources broker for health check informatics application. Goal-based apply for initially presents as new approach in optimizing the use of wherewithal in the cloud. The construction of this goal-based cloud negotiator is aggravated from earlier work on where the impression of goal is applied. Goal, mediator and web service must be well-defined using inbuilt keywords in order to reduce syntax burden for semantic web service (SWS) developer. Likewise, in cloud broker, user needs to define the goal in their request and broker will act as a go-between while cloud possessions represent the web services. Goal-based cloud broker architecture was proposed to fulfill the concept of goal-based request. Detection and selection algorithm in resource agent will be enhanced to achieve investigate goal.

A key element in the renovation of healthcare is an elementary shift in the importance of preventive care. The United States Congressional Budget Office has stated that one key focus for healthcare modernism is precautionary care. Instead of considerate for "sickness" using an immediate model, the society might be better off investing in disease avoidance and wellness using a practical model. The end goal is to lower the possibility of disease onset in order to reduce the overall expenditure of care. Private employers such as Safeway have established successes of adopting wellness programs to help reduce healthcare costs [19]. It is predictable that patrons will participate in retentive care activities such as blood pressure quantity and excises in retail stores, home, administrative center, using web information managers to supervise and unite with care channels such as a primary care doctor with handiness. Although early results from wellness/prevention-centric initiatives are not yet conclusive, they are promising enough for many to see preventive care as transformative [20].

The real meaning of a business service ecosystem is that the associations among service providers need to be analyzed from a higher holistic level rather than from the viewpoint of personal services. A business service ecosystem's scope is the set of symbiotic relationships among actors who work together around a core technology platform. James Moor has recognized the business ecosystem notion as a ground-breaking strategic arrangement concept involving enterprises, supply chain and network of trading systems. We apply this strategic thoughts to the domain of incubating services on Cloud. The main difference between the ecosystem approach and the conventional enterprise architecture approach to organizing interrelated applications is that the former supports a large number of actors with a organization style that calls for the lowest level of control. It is therefore worthwhile to investigate lessons from biological systems [21].

Nkosi and Mekuria in their proposal for Cloud Computing for Enhanced Mobile Health Applications [22] Research developments towards cloud computing will have a direct impact to a number of issues in accessible technologies. Unusual approaches are necessary to productively address those issues. Research efforts in cloud computing has recognized services that can be delivered via the cloud. Below we list some of those services: A basic idea of this framework is that a multimedia sensor signal processing will require increased power consumption for it to execute in a mobile device. To prevent this power drainage, the proposed model uploads complex computational algorithms to be executed in the cloud and final output is then uploaded back to the mobile device and the application server (AS). The model framework, therefore, classifies the required computational service request as weak and strong classes. The weak class requires low security and computation and strong class complex Multimedia processing and security. It is assumed that weak class offload request consumes less power and will be entirely performed in a mobile device and strong class is performed in the cloud with varied conditions. Furthermore, we innovatively propose a transitional performance of strong class multimedia and security verification. Transitional offloading where, part of

(eg., 85%) a complex multimedia operation is performed in the cloud and the other remaining part (15%) is transferred to mobile device for completion. Mobile device is therefore expected to execute the remaining 15% and send a completion acknowledgement feedback to the mechanism in the cloud.

An event monitoring system is useful in e-healthcare structure where the ICT services increase the interactivity between patients and medical community. The events may be normal arrangement of problem-solving tests, medicine agenda along with alerts which necessitate awareness of patient or the medical staff. The health care history is proactively analyzed by intelligent agents embedded in the system which raise alerts of various natures. Some of the alerts may require only a normal response and others may have to be approved by the staff within particular time failing which the alert may be passed on to a higher level in the system. This is particularly important in aged patients, post operation treatment and special citizens where the medical examination provider assumes a higher level of conscientiousness and vigilance.

Basically, SCP is a tamper-resistant hardware capable of limited general-purpose computation. For example, IBM 4758 Cryptographic Coprocessor (IBM) is a single-board computer consisting of a CPU, memory and special-purpose cryptographic hardware contained in a tamper-resistant shell, certified to level 4 under FIPS PUB 140-1. When installed on the server, it is capable of performing local computations that are completely hidden from the server. If tampering is detected, then the secure co-processor clears the internal memory. Since the secure coprocessor is tamper-resistant, one could be tempted to run the entire sensitive data storage server on the secure coprocessor. Pushing the entire data storage functionality into a secure co-processor is not feasible due to many reasons.

First of all, due to the tamper-resistant shell, secure co-processors have more often than not inadequate memory and computational power. Performance will progress over time, but troubles such as heat debauchery/authority use will force a gap between general purposes and secure computing. One more issue is that the software running on the SCP must be totally trusted and confirmed. This safety measures requirement implies that the software running on the SCP should be kept as simple as possible. So how does this hardware help in storing large sensitive data sets? We can encrypt the responsive data sets using unsystematic private keys and to improve the danger of key disclosure, we can use tamper-resistant hardware to store some of the encryption/decryption keys (i.e., a main key that encrypts all other keys). Since the keys will not reside in memory unencrypted at any time, an attacker cannot learn the keys by taking the snapshot of the system. Also, any attempt by the attacker to take control of (or tamper with) the co-processor, either through software or physically, will clear the co-processor, thus eliminating a way to decrypt any sensitive information. This framework will facilitate (a) secure data storage and (b) assured information sharing. For example, SCPs can be used for privacy preserving information co-operation which is significant for guaranteed information distribution.

An uncomplicated approach to guard the data reliability would be using conventional cryptographic procedures, such as the well-known message authentication codes (MACs). Initially, data owners can locally maintain a small amount of MACs for the data files to be outsourced. Whenever the data owner needs to get back the file, she can verify the integrity by recalculating the MAC of the received data file and comparing it to the in the neighborhood precompiled value. If the data file is large, a hash tree can be employed, where the leaves are hashes of data blocks and internal nodes are hashes of their children of the tree. The data owner only needs to store the root hash of the tree to authenticate his data received.

While this technique allows data owners to verify the rightness of the acknowledged data from the cloud, it does not give any declaration about the accuracy of other outsourced data. In other words, it does not give any assurance that the data in the cloud are all actually intact, unless the data are all downloaded by the owner. Because the amount of cloud data can be huge, it would be quite unrealistic for a data owner to retrieve all of her data just in order to verify the data is still correct. If the data auditing task is delegated to a TPA, this method unavoidably violates our recommended necessities, with large auditing cost for a cloud server (for accessing and transferring all of the data) and data privacy exposure to the TPA (for retrieving a local copy of data). Thus, new approaches are obligatory.

In distinguish to established enterprise IT solutions, where the IT services are under proper physical, logical and human resources controls, cloud computing moves the application software and databases to servers in large data centers on the Internet, where the administration of the data and services are not fully responsible. This distinctive aspect raises many new security challenges in areas such as software and data security, recovery and privacy, as well as legal issues in

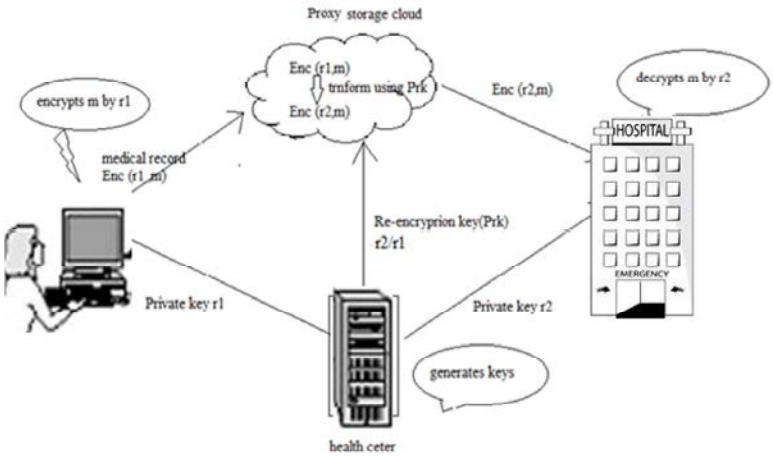

Fig. 2: Proposed Proxy Re-encryption scheme for PHRS

areas such as authoritarian fulfillment and auditing, all of which have not been well understood. In this article we focus on cloud data storage security. We first present in the network structural design for effectively describing, developing and evaluating secure data storage problems. We then suggest a set of methodically and cryptographically attractive properties for public auditing services of trustworthy cloud data storage security to become a reality. Through exhaustively analysis, some existing data storage security building blocks are examined. The pros and cons of their practical implications in the context of cloud computing are summarized. Further challenging issues for public auditing services that need to be focused on are discussed too. We believe security in cloud computing, an area full of challenges and of dominant consequence, is still in its infancy now but will attract gigantic amounts of follow a line of investigation effort for many years to come.

Proposed Woek: In the above section we have determine the problem in PHRS and to overcome we propose proxy re-encryption scheme as it is suitable solution for the given problem. In proxy re-encryption scheme the core part is the transformation by the proxy through re-encryption key. This key determines the way proxy works. If we determine the way transform occur (re-encryption) without knowing the underlying plain text than we convert the cipher text to another form with respect to destinations. Overall we say re-encryption key determines the scheme. Different forms of keys make different forms of schemes. One of the schemes is proposed by us which is suitable for Cloud PHRS.

Private Key generator (PKG) generates private keys for both sender and receiver and also sends the re-encryption key (Prk) to proxy for transformation [17]. This way proxy doesn't know the private keys of both sender and receiver and still transforms message encrypted in sender's private key (r1) to receiver's private key (r2).

Procedure: Let G be a group G of prime order p and let g be the generator of G.

- PKG (health center) chooses two different random number say r1 and r2 from the range Zp = (1 to p-1) and sends them as private keys to Denis and hospital respectively. It also sends Prk, (r1/r2) mod p, to proxy cloud as shown in Fig 3.
- Denis and hospital publishes their keys as X = pow (g, r1) and Y = pow (g, r2) respectively.
- Now Denis chooses a random number r from Zp and uses it to encrypt medical record m.
- From r he makes two cipher texts C1 and C2
- where C1 = pow (X, r) and C2 = m*pow (g, r). (C1,C2) is send to proxy cloud storage.
- C1 is cipher text which is transform and used for decryption and C2 is the encrypted medical record which remains unknown to the proxy.
- At proxy C1 is transformed to C3 by executingpow (C1, Prk). Hence, C3 = pow (Y, r).
- Now (C3,C2) is send to hospital.
- After hospital receive the cipher text pair it will first compute C3 inverse power of r2 to obtain the encryption key in C2 i.e. pow (g, r). After obtaining key it will take key's inverse with C2 to obtain the original Denis's medical record m.

Fig. 3: Encrypted Medical Record (Ciphertext)

Table 1: Medical record of patient

NAME	ViploveKhushalani
AGE	21
GENDER	MALE
CONDITION	Critical
ALLERGY	Dust
EYE HISTORY	Cataract: OU; Glaucoma: OU
MEDICAL HISTORY	HBP: controlled; Diabetes: type II; Hepatitis: C
FAMILY HISTORY	Glaucoma: Father open angle
ROS	Constitutional symptoms: fatigue
MEDICINES	Glynase: Tenormin; Hytrin
SOCIAL HISTORY	Non Smoker; Resident: permanent
PSYCHIATRIC EXAM	Oriented X3, normal mood and affect
NAME	ViploveKhushalani
AGE	21
GENDER	MALE
CONDITION	Critical
ALLERGY	Dust
EYE HISTORY	Cataract: OU; Glaucoma: OU
MEDICAL HISTORY	HBP: controlled; Diabetes: type II; Hepatitis: C
FAMILY HISTORY	Glaucoma: Father open angle
ROS	Constitutional symptoms: fatigue
MEDICINES	Glynase: Tenormin; Hytrin
SOCIAL HISTORY	Non Smoker; Resident: permanent
PSYCHIATRIC EXAM	Oriented X3, normal mood and affect

Table 2: User keys and their respective transformed keys by proxy

Name	Encrytped Key	Transformed Key
Viplovekhushalani	4096	32768
Anujagrawal	8192	77935
Prateeksaraf	16384	185363
Sahiljain	32768	440871

Table 3: Final medical record accessed by hospital

NAME	ViploveKhushalani
AGE	21
GENDER	MALE
CONDITION	Critical
ALLERGY	Dust
EYE HISTORY	Cataract: OU; Glaucoma: OU
MEDICAL HISTORY	HBP: controlled; Diabetes: type II; Hepatitis: C
FAMILY HISTORY	Glaucoma: Father open angle
ROS	Constitutional symptoms: fatigue
MEDICINES	Glynase: Tenormin; Hytrin
SOCIAL HISTORY	Non Smoker; Resident: permanent
PSYCHIATRIC EXAM	Oriented X3, normal mood and affect

Table 4: File Size Vs Time for encryption and decryption

File Size (in KB)	Time For Encryption (in Sec)	Time For Decryption (in Sec)
70	1	1.2
108	1.5	3.3
125	0.5	4.5
230	3	5.2
440	0.5	5.7

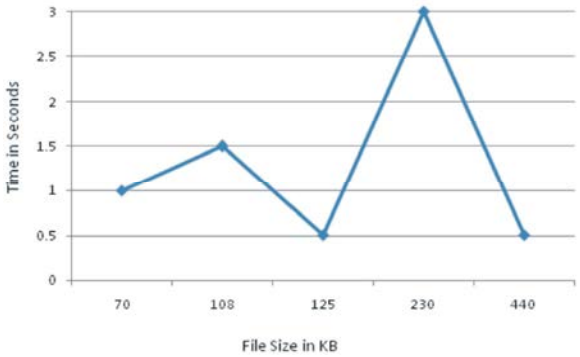

Fig. 4: Encryption time Vs File size

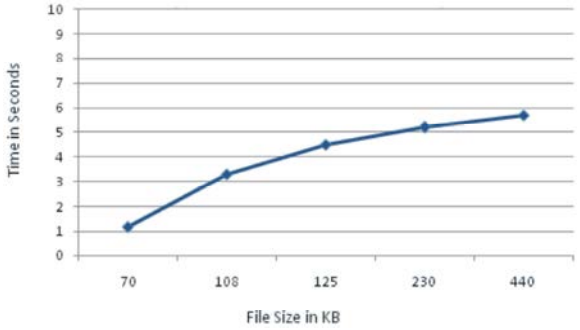

Fig. 5: Decryption time Vs File size analysis

RESULTS AND DISCUSSION

This way the encrypted data is transformed to another form without knowing the proxy through proxy, we can transfer the information from sender to receiver.We performed an experiment on Intel(R) Core(TM) 2Duo CPU 2.09 GHz processor with 4 GM of RAM on Windows 7 operating system. GCC compiler is used for evaluation of results. We carried out experiments on 70 KB, 108 KB, 125 KB and 230 KB text file sizes. Keys are of 32 bits. The experiment is conducted across four hospitals in Vellore and the sample medical record is shown in Table1.

Figure 4 shows the way computational time varies with file size. Graph doesn't follow any rhythm; time is high for some values and very low for some. Whereas in figure 10 decryption time increases as the file size increases but at a very slow rate. Both the graphs are very much similar to Elgamal encryption and decryption graphs [18].

CONCLUSION

We have taken a methodical approach to maintain security of the PHRS,PHRS helps the medical field a lot, patients and medical centers doesn't have to maintain separate record system of their own, they can store the information collectively in one cloud based centralized system known as Cloud PHRS. As there is role of cloud in such systems, the stored data security will be our major concern. To overcome that we proposed proxy re-encryption scheme involving PKG which generates all the three keys (two private keys for each user at two ends and proxy re-encryption key), proxy cloud which uses PKG to transform the encryption, the same method can be extended for large medical distributed system.

REFERENCES

1. Kaitai Liang, Liming Fang, Duncan S. Wong and Willy Susilo, 2013. A Ciphertext-Policy Attribute-Based Proxy Re-Encryption with Chosen-Ciphertext Security, pp: 552-559.
2. Luan Ibraimi, Qiang Tang, Pieter Hartel and Willem Jonker 2008, A Type-and-Identity-based Proxy Re-Encryption Scheme and its Application in Healthcare, pp: 185-198.
3. Matthew Green and Giuseppe Ateniese 2007, Identity-Based Proxy Re-Encryption, ACNS, pp: 288-306.
4. Benoit Libert and Damien Vergnaud 2011, Unidirectional Chosen-Ciphertext Secure Proxy Re-Encryption, IEEE, 57(3).
5. Qin Liua, B., GuojunWanga and JieWub 2012. Time-Based Proxy Re-encryption Scheme for Secure Data Sharing in a Cloud Environment, Elsevier Information Sciences.
6. Sharon Inbarani, W., G. Shenbagamoorthy and C. Kumar Charlie Paul, 2013. Proxy Re-encryption Schemes for Data Storage Security in Cloud- A Survey, International Journal of Engineering Research & Technology (IJERT), 2(1).
7. Luan Ibraimi, Qiang Tang, Pieter Hartel and Willem Jonker, 2012. Exploring Type-and-Identity- Based Proxy Re-Encryption Scheme to Securely Manage Personal Health Records.

8. Giuseppe Ateniese, Kevin Fu. Matthew Green and Susan Hohenberger, 2006. Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage, ACM Transactions on Information and System Security (TISSEC), 9(1): 1-30.
9. Snehal Pise and Pramod Mali, 2014. Security of Personal Health Records through Attribute Based Encryption in Cloud Computing, International Journal of Engineering Research & Technology (IJERT), 3(1).
10. Ms. Disha H. Parekh and R. Sridaran, 2013. An Analysis of Security Challenges in Cloud Computing, (IJACSA) International Journal of Advanced Computer Science and Applications, 4(1).
11. Kuyoro, S.O., F. Ibikunle and O. Awodele, 2011. Cloud Computing Security Issues and Challenges, International Journal of Computer Networks (IJCN), 3(5).
12. ANSI, ISO/TS 18308 Health Informatics-Requirements for an Electronic Health Record Architecture, ISO 2003.
13. Bakker, R., B. Barber, R. Tervo-Pellikka and A. Treacher, (eds.) 1995. Communicating Health Information in an Insecure World, in Proceedings of the Helsinki Working Conference, 43: 1-2.
14. Barber, B., D. Garwood and P. Skerman, 1994. In: Security in Hospital Information Systems, Security and data protection programme presented at the IMIA WH10 Working conference, Durham.
15. Furnell, S.M. and P.W. Sanders, XXXX. Security management in the health-care environment, in: R.A. Greenes, H.E. Peterson, D.J. Protti, (eds.), MEDINFO '95, Proceedings of the eighth World Congress on Medical Informatics. Canada, pp: 675-678.
16. Patel, A. and I. Kantzavelou, XXXX. Implementing network security guidelines in health-care information systems. In: MEDINFO '95. Proceedings of the eighth World Congress on Medical Informatics. Vancouver Trade and Convention Centre, Canada, pp: 671-674.
17. Henry, H. Chang, Paul B. Chou and Sreeram Ramakrishnan, 2009. An Ecosystem Approach for Healthcare Services Cloud"2009 IEEE International Conference on e-Business Engineering
18. Nkosi, M.T. and F. Mekuria SM, XXXX. Cloud Computing for Enhanced Mobile Health" 2nd IEEE International Conference on Cloud Computing Technology and Science Applications.
19. Cong Wang, Kui Ren, Wenjing Lou and Jin Li, 2010. Toward Publicly Auditable Secure Cloud Data Storage Services, IEEE Network - July/August 2010
20. Kevin Hamlen, Murat Kantarcioglu, Latifur Khan and Bhavani Thuraisingham, 2010. Security Issues for Cloud Computing, International Journal of Information Security and Privacy, 4(2): 39-51, April-June 2010
21. Shaftab Ahmed Azween Abdullah, 2011. Telemedicine in a cloud - A Review, 2011 IEEE Symposium on Computers & Informatics.
22. Ekonomou, E., L. Fan, W. Buchanan and C. Thüemmler, 2011. An Integrated Cloud-based Healthcare Infrastructure, 2011 Third IEEE International Conference on Coud Computing Technology and Science.