ADVANCES in NATURAL and APPLIED SCIENCES

ISSN: 1995-0772
EISSN: 1998-1090
2017 January 11(1): pages 99-107

Published BY**AENSI Publication**
http://www.aensiweb.com/ANAS
Open Access Journal

Study on avant-garde Security Techniques in e-Health Clouds

[1]Indra Priyadharshini S and [2]Vigilson Prem M

[1]Assistant Professor, Department of CSE, RMK College of Engineering and Technology, Tamil Nadu.
[2]Professor, Department of CSE, RMD Engineering College, Tamil Nadu.

Received 18 September 2016; Accepted 15January 2017; Available online 29 January 2017

Address For Correspondence:
Indra Priyadharshini S, Assistant Professor, Department of CSE, RMK College of Engineering and Technology, Tamil Nadu.

ABSTRACT

The recent technological unison of cloud computing, big data and Internet of Things has caused a revolutionary swing in the field of health care. The term 'e-health cloud' becomes a buzz word today, as many health care organizations and hospitals are moving the electronic health information into cloud environment. This movement helps in exchange of medical records among doctors, hospitals and health care centers. e-health cloud acts as a Medical record repository and exchange center facilitating quality medical service and reliable analysis of diseases. Cloud computing is an emerging paradigm providing on-demand access of data, but still security and anonymity is the major hassle to be dealt with. This paper presents a survey about the security techniques and approaches to preserve privacy in e-health clouds. The paper expounds by categorizing the approaches as two divisions, cryptographic techniques and Access control Policies.

KEYWORDS: e-health, Encryption, security, Access Control, Privacy, Anonymity

INTRODUCTION

The healthcare industry is experiencing a paradigm shift largely due to the increasing infrastructure maintenance costs. Healthcare organizations are expected to offer patient care capabilities while simultaneously limiting the increasing cost. The emerging computing model cloud systems can be used to implement the health care solutions. Cloud Standards Customer Council states that Cloud computing offers significant benefits to the health care sector: entities of the e- health cloud requires quick access to large infrastructure facilities which can't be provided with traditional computing. These requirements can be fulfilled only by cloud computing systems.

Big IT giants like [2] Amazon, Infosys, Cisco, CSC, Salesforce and many more are offering health care services through clouds.

NIST defines Cloud Computing as "A model for enabling ubiquitous, convenient, on demand network access to shared pool of configurable computing resources (e.g., networks, servers, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

IBM, a major player in cloud computing, has defined it as follows, "A cloud is a pool of virtualized computer resources. A cloud [1] can host a variety of different workloads ranging from batch processing jobs to interactive user mode jobs".

Union Of Cloud Computing And Health Care Services:

The health care services provided through electronic medium is called as "e-health". Paper based medical records are improved to Patient Health Records (PHRs) and Electronic Health Records (EHRs). PHRs are maintained by the individuals for their reference and EHRs are maintained by health centers for better analysis and diagnosis of diseases and for further treatment. In addition to the analysis by the doctor, he might share the EHRs to his peers or seniors belonging to other hospitals and health centers for discussion and examination. Electronic Medical Records (EMRs) is another category of health information in electronic version similar to EHRs is maintained and it is not shared to outsiders, kept within the hospital or health center where the data is generated.

The hospitals or health centers moving their traditional medical data to clouds has the liberty of choosing their deployment model in clouds.

1) Deployment of e-health cloud in the health center / hospital premises – private e-health cloud.

2) Deployment of e-health cloud in the Cloud Service Provider Network – Public e-health cloud.

3) Deployment of e-health cloud solution is combined with a group of other health organizations and CSPs – Hybrid e-health cloud.

Cloud computing [1] is on demand provisioning of resources (Data, storage, network, Memory, CPU capacity or even I/O). Cloud offers services to users anywhere, anytime through internet. So, any user with an internet connection can access health related information when provided with an internet connection. This sounds like a boon to health care industry where diagnosis, life saving criticality can be easily handled through cloud computing.

Hospitals and health organizations shifting to the cloud-style computing have freedom of choosing the service layer according to their needs.

1) Infrastructure as Service (IaaS):

The health organizations can rent processing capacity, storage capacity, networks and other resources to build their infrastructure to maintain the back office operations to provide e-health service round the cloth. They are relieved from the tedious task of infrastructure maintenance which in turn decreases the cost.

2) Platform as Service (PaaS):

In case if the health organization or hospital has the infrastructure facility to implement the health care solutions or if they have built their infrastructure over cloud using IaaS, they can host and deploy their solutions using PaaS on top of IaaS.

3) Software as Service (SaaS):

This model offers the flexibility of using the browser intiated applications by the users. Services and tools offered by PaaS are utilized in construction of application and management of their deployment on resources offered by IaaS providers.

A Personal Health record is a collection of health related information that is documented and maintained by the individual it pertains to. The idea of maintaining PHRs is to provide a complete and accurate summary of an individual's medical history, which helps the physicians in the diagnosis and analysis of the patient. It includes the observations of physicians as reported by the patient, data from devices like scanners and 3D imagers, lab results and data collected from smart phone sensors.

Electronically stored PHRs are called EHRs. An electronic health record is an electronic version of PHR, that is maintained by the Health Organizations or Hospitals and includes all necessary information for the diagnosis and treatment. EHRs are shared among Health centers, Doctors and Hospitals which helps the medication process by reducing the duplication of tests, reducing delays in treatment and reducing medical error by improving the clarity of medical records.

Cloud based Medical Image Exchange:

In addition to the storage of electronic medical records, a different perspective is that the clouds can be visualized as a platform to exchange medical images among various entities like hospitals, Health organizations, Medical Practioniers, Patients etc., The explosive growth of medical images has led to a challenging situation for the health organizations [7] to store, manage, secure and process the data as it involves increased operating cost. Massive improvement in the invention of medical equipments like MRI scanners, Ultrasound scanners, CT 3D imagers, led to the increase of medical image data.

Cloud based Patient Monitoring:

The union of technologies like IoT, Wireless Body Area Networks, Wearable Medical devices and Cloud Computing has risen the usage of e-healthcare services by public. This convergence of technologies with wearable medical devices or monitoring devices (e.g. Smart Phone Sensors which records psychological signals like ECG, heart beat rate, body temperature, posture, skin allergic resistance etc.,) has become a crucial application as it provides observation & check of chronic diseases, protection of human life in critical situations and 24X7 inspection on the patient.

Need For Security and Privacy Preservation In E-Health Clouds:

Patients are uncertain about the privacy protection of their sensitive data when they rely on third-party cloud service provider for storage. The public can't rely on third party service providers for their sensitive EHR data because they are unaware of how this data can be handled by the Cloud Service Providers (CSPs) and how the access control be established on the EHRs. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 provide regulatory guidance on how to use and protect the health information of a patient. Though the e-health cloud solutions are expected to provide services as per HIPAA, it is not that all cloud providers are covering them. Moreover the observant health records stored on third party cloud providers are prone to attacks by the insider itself. To handle these privacy and security preserving hindrances, encrypting the Patient's EHR before we move them to the cloud.

Entities involved in e-health clouds are patients, hospital employees like doctors, nurses, laboratory staff, pharmaceutical staff, insurance providers and the cloud service providers. The ultimate challenge in the e-health cloud is data level security and sensitive data like EHRs must be within the health provider (hospital or health centers) and not with the CSPs. Identification Access management (IAM) also plays a major role in privacy preserving. These challenges can be met by traditional cryptographic mechanisms. Other non cryptographic mechanisms are used to enforce Access Control in the health clouds.

In general, researchers have exploited the measures of enforcing security to the health clouds with the help of adversary models. The adversary models assume the following,

1) The CSPs are untrusted entities where EHRs are stored. The EHRs are being shared among other hospitals and health centers, so it is vulnerable to attackers. Unauthorized users can try to access the data which they are not intended to.

2) It is possible for an insider (resides in the enterprise) may try to misuse the data to which he is authorized to access. For e.g., a nurse may disclose the laboratory test results of a patient to public. An article says that 32% of security violations in health care industry between January 2007 and June 2009 were due to insider attacks [3], and the incident rate of insider attacks is rapidly increasing [3]. The insider attacks have caused more damage to the affected organizations more than what outsider attacks have caused.

3) Even if the CSPs [4] are semi trusted servers (honest but curious about the content stored), the attackers not only try to disclose or tamper the data but also tries to use the data in a malicious way by selling the sensitive information to others.

The initiative taken by the project Medical Information Privacy Assurance (MIPA) [5] has listed the unique challenges of maintaining privacy in health data, and the devastating privacy breach facts that resulted from untrusted public or hybrid clouds. MIPA was one of the first few projects that developed frameworks to enforce security and preserve privacy of EHRs stored in cloud.

The general requirements of the e-health cloud solutions are 1) Reliability 2) Authorization 3) Availability 4) Fault Tolerance 5) Resilience 6) Data sharing and aggregation and 7) Emulation/isolation. The specific requirements pertaining to privacy preserving are

1) Integrity:

It refers to the trustworthiness of data. It deals with prevention of unauthorized modification or tampering of data. Integrity suffers with active attacks like masquerading, modification or alteration of sensitive data etc.,

2) Confidentiality:

It refers to the concealment of the resources or information. It deals with unauthorized disclosure of sensitive information. Confidentiality suffers with passive attacks like replay attacks, snooping, passive wire tapping etc.,

3) Accountability:

It refers to the responsibility of an entity to agree on the actions carried out by it. Accountability suffers if there is lack of proper identity management or presence of poor access control policies.

4) Audit:

It refers to the flexibility of checking the health cloud architecture to ensure that the HER stored in the health cloud is error free and secure.

5) Non-Repudiation:

It refers to the protection against denial of the actions done by the entities. Denial of Service and Denial of Receipt attacks damages Non-Repudiation.

6) Unlinkability:

The ability of the framework to achieve the flow of information to multiple paths but the adversary or the authorized users can't create any link among the multiple access of same EHRs.

7) Authenticity and Authorization:

Proper access control mechanisms are provided in the system to ensure that authorized users are authenticated for access.

8) Anonymity:

It refers to the property when EHRs stored in the cloud can't be matched with the identity of the patients by unauthorized users.

Security Techniques In E-Health Clouds:

There are many techniques available to enforce security and preserve privacy in e-health clouds. The major security concerns in the health clouds focuses on a) Confidentiality and Integrity over the data and b) Access control policies. Several techniques available makes use of traditional cryptographic mechanisms and hybrid approaches of cryptography mechanisms and authorization mechanisms to achieve the above said security concerns.

A) Traditional Cryptographic Techniques:

Conventional Cryptographic mechanisms popularly used to maintain confidentiality are Symmetric Key Encryption and Public Key Encryption.

Symmetric Key Encryption:

Symmetric key encryption is the simple to use. It uses same secret key for both encryption and decryption. There must be some secure way to share the secret key between the sender and receiver. The popular symmetric key encryption techniques are Data Encryption Standard (DES), Advance Encryption Standard (AES) etc. The most widely used encryption scheme is DES. In DES, data are encrypted in 64-bit blocks using a 56-bit key. The strength of DES lies in a) 56 bit key, b)S-box Design and c) resistance to timing attacks. DES has variations like Double DES and Triple DES.

NIST has evaluated the AES cipher in various criteria and chosen it as a strongest algorithm. AES has key sizes of 128, 192 and 256 bits. Data block is of size 128 bit. It has 10 to 14 rounds of identical processing. Each round has the following sub stages, a) Substitute bytes, b) shift rows, c) Mix Columns and d) Add round key. Both AES and DES have been proved that it can stand against Brute Force attacks.

Public Key Encryption:

Public key cryptosystems works on a pair of related keys, one used for encryption (Public key) and the other for decryption (Private Key). The pair of keys is related but can't deduce one key from the other. It is computationally infeasible for an adversary, knowing the public key and the cipher text, to recover the original plain text. RSA algorithm is a widely accepted scheme using public key encryption. RSA is a block cipher in which messages and scrambled outcomes are integers, the computation involves exponentiation of prime numbers in modular arithmetic. RSA can defend against Brute Force attacks, Mathematical attacks, Timing attacks and Chosen Ciphertext attacks. Diffie-Hellman is another public key algorithm which enables users to share secret keys in a secured manner. Elliptic Curve Arithmetic is a popular multipurpose public key algorithm used for key exchange, encryption and digital signature. ECC offers equal security like RSA even with smaller key sizes comparatively.

Conditional Proxy Re-Encryption:

Kuo-Husuan Tang et al. proposed a patient-centric access control scheme for PHRs [25] in the cloud. The authors used the combination of AES and RSA encryption schemes for the process. They enforce access control policies to be assigned by the patient, where conditional proxy re-encryption is used for encrypting the encryption keys.

Huang Lin et al. described a model based on a new variant of key private proxy re-encryption [6] scheme, in which the health centers or hospitals only needs to accomplish encryption once at the setup phase while altering the remaining computational tasks to the cloud without compromising privacy, further reducing the computational and communication burden on clients and the cloud. The CSPs can't obtain any information on the individual user's query or the health provider's communication due to the semantic security of private proxy re-encryption scheme and symmetric key encryption.

Proxy Re-Encryption (PRE) with Public Keyword Search:

Yang Yang [16] et al. discusses about Proxy re-encryption (PRE) which employs a proxy with a re-encryption key for decryption of ciphertext encrypted by user's public key into those that can be decrypted by user's private key. The users with a keyword trapdoor can search the ciphertext while the hidden keywords are unknown to the proxy. The limitation on the schemes in is that only one keyword will be allowed to search in the encrypted documents.

Attribute based Enryption (ABE):

ABE also makes use of public key encryption, it allows multiple users to share the data. Data is encrypted based on the attributes of the user. Attributes pertains to the secret credentials or specific properties of the user. These attributes define the access policies of the user. Users only with access policies satisfying the credentials (attributes) are allowed to decrypt the data.

Yue Tong et al. presented a privacy preserving mobile access health data system implemented in cloud. The authors provide protection against the search keyword patterns presented by the health cloud consumers, through which the adversaries find meaningful information to play attacks. The model also provides an auditability [29] scheme to keep track of the actions. A heuristic approach is used for hiding the search and access patterns instead of relying on relatively heavy cryptographic techniques. This approach slightly increases the computation and storage cost. The authors tested their implementation in private cloud. Unlinkability is focused as the primary concern. Unlike symmetric encryption different data is encrypted with different keys or key combinations. Key management is done using a pseudorandom number generator for unlinkability. The concept of attribute based encryption with threshold signing for providing role-based access control with auditability to prevent misbehavior of intruders in all situations (normal or emergency access).

Yang Tang et al. presents a framework called 'FADE' [10] which achieves both access control and assured deletion. FADE is implemented using ABE for access control and a quorum of key managers with threshold signing for assured deletion of files using access policies. This model is suitable for environments where large data files are archived. FADE provides fine grained access control with time based file assured deletion in which data files are deleted when the associated file access policies are revoked.

Cipher Text Policy Attribute based Encryption (CP-ABE):

CP-ABE has an authority which is responsible for the attribute generation and policy creation. Users has to register with this authority for getting the secret key for decryption. Similar to ABE, the secret key is issued based on the credentials of the user. Two flavours of CP-ABE is available based on the authority implementation. 1) Attributes are managed by single authority 2) Attributes are governed by multiple authorities from different domains.

Kan Yang et al. [8] presents an efficient data access model for multi authority cloud storage. The authors describes this model which suits for e-health cloud where users have multiple roles (e.g. A person may be assigned 'doctor' role in hospital and 'researcher' role in 'medical college'). The model also focuses on attribute revocation, which is done when any authority cancels or deletes the attribute or role of any user. A version number is assigned for each attribute of any user. When an attribute revocation happens, the secret keys and ciphertexts corresponding to that particular attribute need to be updated. When an attribute of a user is revoked from its corresponding attribute authority, [6] the attribute authority generates a new version key for this revoked attribute and generates an update key. All other users except the revoked user can update their respective keys with the newly generated update key. The cipher text is also updated with the update key. This cipher text updation is shifted to the server by using proxy re-encryption method. All the users must hold the recently updated secret key to decrypt the data because the cipher text is constantly updated according to the attribute revocation.

Hierarchical Predicate Encryption (HBE):

HBE is based on public key encryption and it is used to offer fine grained access policies. Private keys are generated based on the predicates and these private keys are used for decryption.

Ming Li *et al.* [14] discussed the issues on Authorized Private Keyword Searches (APKS) on the encrypted EHRs in the cloud environment with the help of local trusted authorities. The environment has three entities namely data owner, trusted authorities and the cloud owner. To guard against the curiosity of cloud server, the authors proposed a solution based on HPE. The model provides query privacy, multi-dimensional multiple keyword searches, delegation and revocation of search capabilities. By using the attribute hierarchy, the technique not only enhances the search efficiency but also improves the query privacy.

Homomorphic Encryption:

This type of encryption allows computations to be performed on cipher texts, that is it works on encrypted text and the output is also in encrypted form. Gentry et al. presented a privacy preserving multi cloud architecture which makes use of fully homomorphic encryption. Here the key is shared between the cloud where the entity with the private key resides and other participating clouds. Multi party communication is assisted with a threshold encryption scheme.

Jun zhou [13] proposed a secure and efficient privacy-preserving dynamic medical text mining and image feature extraction scheme PPDM for cloud-assisted e-healthcare environment. An efficient privacy-preserving fully homomorphism data aggregation is used. This framework achieves an outsourced disease modeling achieved by developing an efficient privacy-preserving function correlation matching PPDM1 from dynamic medical text mining and designing a privacy-preserving medical image feature extraction PPDM2. The cloud server performs privacy-preserving function correlation matching for medical text mining and SIFT for image feature extraction in the encrypted domain.

Dynamic Broadcast Encryption:

Broadcast encryption is fast as it uses simple symmetric encryptions for computations. It is scalable and keys are distributed in such a way that broadcasts can made to m users, where m is a subset of n users.

Xuefeng Li et al. presents architecture called Mona [22] for secure data sharing between multiowners of data in a cloud. This can be correlated with a situation where doctors of same department want to share the same PHR of a patient to a class of students for demonstration purpose. Such kind of private communication is implemented with dynamic broadcast encryption, where a trusted entity called group manger is allowed to dynamically enroll/revoke registers and maintains secret keys. Group members have to be registered with group manager to participate in communication. This secure data sharing is done in a dynamic user group in a untrusted cloud.

B) Access Control Techniques:

Policy based Access Control:

Sourya Joyee De et al. proposed a policy-based security framework [12] for outsourcing company's data for computations in a very secured manner. It considers about changing user perceptions, gathered in a decentralized way directly from the users, about trustworthiness of CSPs and data security requirements. Based on these perceptions secure data policies which consist of storage security policies, upload security policies and computation security policies are formulated which is used for taking decisions by the company.

Mandatory Access Control:

This method allocated rights to data owners based on the access of objects to number of subjects. Each object and every subject is assigned with particular security level. This plays a major role in assigning rights of objects to corresponding subjects. Access to particular object by a subject is allowed only when certain relationship is met [26]. This method classifies the objects in cloud environment hierarchical manner.

Attribute based Access Control:

Chen Yanli et al. [19] presents an Attribute – based Access control method for multi authority system which solves the collusion problem in multi-authority cloud architecture systems where we can't trust a single machine as a central authority which can tie different components of any user's private key. This implementation model allows any user to act as an authority thereby eliminating the central authority scheme. Different parties can act as different authorities and function independently and therefore no global commitment is required. It also eliminates Single Point of Failure.

Ciphertext Policy Attribute based Access Control:

Zhijie Wang et al. achieves an efficient access control mechanism using Constant-size Ciphertext Policy Comparative Attribute-Based Encryption (CCP-CABE) with the support of negative attributes and wildcards. The CCP-CABE [20] framework comprises of a central Trust Authority (TA), e.g., the government health agency, a trusted third party server which provides security services, a Cloud Provider, data owners (e.g., patients, doctors) and data users (e.g., healthcare professionals , doctors, etc.,). The Trust Authority issues public and private keys to data users through secure channels and publishes global parameters. The framework keeps the computational overhead constant over the different user roles in spite of any number of involved attributes through batch processing technique of various encryption or decryption techniques.

Ciphertext Policy Attribute based Access Control for Revocation:

Kan Yang and Xiaohua Jia proposed a revocable multi-authority CP-ABE scheme that can support efficient attribute revocation. The paper discusses about a variation of CP-ABE scheme primarily focusing on revocation

[8]. The scheme provides efficient and revocable data access control scheme for multi-authority cloud storage systems, where multiple authorities coexist and work independently. The revocation feature achieves both forward security and backward security.

Xiaoyu Li et al. proposed a scheme called TFDAC-MACS [21] which provides two-factor data encryption protection for multi-authority cloud storage systems. The user need to go through two level check before accessing the stored data. The first level check include the user specific attributes and the final check is done with authorization keys. The author kept both the size of ciphertext and the number of pairing operations in decryption to be constant, thereby reducing the communication overhead and computation cost of the system.

Dynamic Risk based Access Control:

The DRAC scheme effectively implements access control by accentuate on risk measurement for taking up a decision on access rights. Aiguo Chen et al. combines the traditional author defined access models like ABE with risk assessment [28] to measure the uncertainty of a user behavior. The framework has various modules for setting up rules, assessing the risk, setting up dynamic threshold and integrated decision making. As the cloud environment is itself dynamic in nature, the DRAC model which comprises the features of Attribute based Access control and threshold policies achieves dynamic decision making in access control with improved scalability and accuracy.

Role based Access Control:

The RBAC schemes in cloud storage systems allows a data owner to encrypt their data based on role, and only the users who have been granted the membership to the corresponding role or the ancestor role of that role can decrypt. These trust models helps the data owners and the associated roles to create flexible access policies. These trust models [23] prevents the owners from allowing the roles with bad historical behaviour in terms of poor track record in carrying out their functions properly and also assist the roles to identify the malicious users who is responsible for the roles' trustworthiness.

Comparison Table:

Paper	Technique	Strength	Weakness
Security Techniques			
[11]	Symmetric Key Encryption	• Can't determine the relationship among the Patient records • Strongly secured ownership for data owners • Simultaneous access of data	• Service Provider can access the data • Key distribution is complex • Overheads due to cloud access • Scalability and Portability issues • Difficult to implement user with different roles
[9]	Public Key Encryption	• Accountability is achieved • Multiuser roles can be handled with secure access control • Access levels are introduced by hierarchical ownership rights	• Security is declined when records are accessed through referrals • Relationships are determined among patient records • Weakly secured Identity of Patient records • Increased overhead for data owners
[25], [29], [10]	Conditional Proxy Re-encryption	• Allows units of data for access • Fine grained Access Control • Unlinkability is achieved	• Cancellations of access rights is tedious
[6], [8]	Cipher Text Policy Attribute Encryption (CP-ABE)	• Flexible control over data by data owners • Key distribution made easy	• Key Escrow Problem • Limited number of access policy implementation
[14]	Hierarchical Predicate Encryption (HBE)	• Multidimensional Keyword searches • Delegation and revocation of rights is easy	• Lack of Access Control
[13]	Homomorphic Encryption	• Multi Party Communication • Privacy Preserving • Computation on encrypted data	• Complex implementation causes overheads
[22]	Dynamic Broadcast Encryption	• Fast, simple computations • Multiple ownership	• Revocation Issues • Group communication overhead

• ACCESS CONTROL			
[12]	Policy based Access Control	• Sticky Policies	• Veracity and Reliability issues
[26]	Mandatory Access Control	• Conditional Access rights given • Predefined rights at the time of record creation	• Delegation may cause confusion
[20], [8], [21]	Ciphertext Policy Attribute based Access Control	• Supports multiauthority cloud storage • Primarily focuses on Revocation	• Central authority may get compromised
[28]	Dynamic Risk based Access Control	• Scalable and accurate, as it works on risk assessment • Dynamic as the nature of cloud	• Inside attacks can't be determined
[23]	Role based Access Control	• Auditing & Logging	• Complex

Conclusion:

The paper examines about the various techniques and approaches towards e-health cloud security. In precise, the need and importance behind the union of cloud into health care systems, the design challenges and issues of e-health cloud is reviewed. Then the state of art analysis of security techniques is analyzed by classifying them into cryptographical approaches and access control policies. In addition to security and privacy preserving, there are still more issues for research. Integrity of the medical data stored in cloud, tracking and logging of actions in the health cloud, efficient data search mechanisms, anonymity in multi authority cloud and efficient key management can be considered for research. This paper serves as the outline for our future work of building a secure and fault tolerant framework for e-health cloud.

REFERENCES

1. e-Health Cloud: 2012. Opportunities and Challenges Eman AbuKhousa, Nader Mohamed and Jameela Al-Jaroodi Future Internet, 4: 621-645; doi:10.3390/fi4030621
2. Key Challenges in Cloud Computing Enabling the Future Internet of Services Rafael Moreno- Vozmediano, Rubén S. Montero,and Ignacio M. Llorente IEEE Computer Society 1089-7801/13/ © 2013 IEEE INTERNET COMPUTING
3. Emam, K.E. and M. King, 2009. The Data Breach Analyzer [Online]. Available: http://www.ehealthinformation.ca/dataloss
4. Shaw, E., K. Ruby and J. Post, 1998. "The insider threat to information systems: The psychology of the dangerous insider," Security Awareness Bull., 2(98): 1-10.
5. Ateniese, G., R. Curtmola, B. de Medeiros and D. Davis, 2002. "Medical information privacy assurance: Cryptographic and system aspects," presentedat the 3rd Conf. Security Commun. Netw., Amalfi, Italy, Sep.
6. CAM: 2013. Cloud-Assisted Privacy Preserving Mobile Health Monitoring Huang Lin, Jun Shao, Chi Zhang, and Yuguang Fang, IEEE Transactions on Information Forensics and Security, 8: 6.
7. Cloud Based Medical Image Exchange-Security Challenges, Shini. S.G, Dr. Tony Thomas, Chithraranjan, K, Procedia Engineering, 2012 . 3454 – 3461 1877-7058 © 2012 Published by Elsevier Ltd.
8. Expressive, 2014. Efficient and Revocable Data Access Control for Multi-Authority Cloud Storage Kan Yang, and Xiaohua Jia, IEEE Transactions on Parallel and Distributed Systems, 25(7).
9. Emerging Security Mechanisms for Medical Cyber Physical Systems Ovunc Kocabas, Tolga Soyata, Member, IEEE, and K. Mehmet 2015. Aktas IEEE/ACM Transactions on Computational Biology and Bioinformatics.
10. Secure Overlay Cloud Storage with Access Control and Assured Deletion Yang Tang, Patrick P.C. Lee, John C.S. Lui and Radia Perlman, 2012. IEEE Transactions on Dependable and Secure Computing, 9: 6.
11. Lifelong Personal Health Data and Application Software via Virtual Machines in the Cloud, Pieter Van Gorp and Marco Comuzzi IEEE 2014. Journal of Biomedical and Health Informatics, 18: 1.
12. A Policy-based Security Framework for Storage and Computation on Enterprise Data in the Cloud, Sourya Joyee De, Asim K. Pal, 2014. 47th Hawaii International Conference on System Science
13. PPDM: 2015. Privacy-preserving Protocol for Dynamic Medical Text Mining and Image Feature Extraction from Secure Data Aggregation in Cloud-assisted e-Healthcare Systems Jun Zhou, Zhenfu Cao, Xiaolei Dong, Xiaodong Lin Ieee Journal of Selected Topics in Signal Processing.
14. Li, M., S. Yu, N. Cao and W. Lou, 2011. "Authorized private keyword search over encrypted data in cloud computing," in Proc. 31st Int. Conf. Distrib. Comput. Syst., pp: 383-392.

15. PPM-HDA: 2015. Privacy-preserving and multifunctional health data aggregation with fault tolerance Song Han, Shuai Zhao, Qinghua Li, Chun-Hua Ju and Wanlei Zhou IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.
16. Conjunctive Keyword Search With Designated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds Yang Yang and Maode Ma 746 IEEE Transactions on Information Forensics and Security, 2016. 11(4).
17. Security and Privacy in Cloud Computing, Zhifeng Xiao and Yang Xiao IEEE Communications Surveys & Tutorials, 2013. 15(2).
18. A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding Hsiao-Ying Lin, Member and Wen-Guey Tzeng IEEE Transactions on Parallel and Distributed Systems, 2012. 23(6).
19. Attribute-Based Access Control for Multi-Authority Systems with constant size ciphertext in cloud Computing, CHEN Yanli, SONG Lingling, YANG Geng, China Communications, 2016.
20. Efficient Attribute-Based Comparable Data Access Control, Zhijie Wang, Dijiang Huang,Yan Zhu, Bing Li, and Chun-Jen Chung, IEEE Transactions on Computers, 2015.
21. Two-factor Data Access Control with Efficient Revocation for Multi-authority Cloud Storage Systems, Xiaoyu Li, Shaohua Tang, Lingling Xu, Huaqun Wang and Jie Chen, Journal of Latex Class Files, 2016.
22. Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud, Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan, Ieee Transactions on Parallel and Distributed Systems, 2013. 24(6).
23. e-Health Cloud Implementation Issues and Efforts Noura Al Nuaimi, Asma AlShamsi, Nader Mohamed, Jameela Al-Jaroodi, Proceedings of the 2015 International Conference on Industrial Engineering and Operations Management Dubai, United Arab Emirates (UAE).
24. Cloud-based Service for Secure Electronic Medical Record Exchange, Asmaa S. Radwan, Ayman A. Abdel-Hamid, Yasser Hanafy, ICCTA 2012, 13-15 October 2012, Alexandria, Egypt Information Security and Privacy of Patient-Centered Health IT Services: What needs to be done? Tobias Dehling, Ali Sunyaev 2014 47th Hawaii International Conference on System Science
25. A Patient-Centric Access Control Scheme for Personal Health Records in the Cloud, Kuo-Husan Hang, En-Chi Chang, Shao-Jui Wang, Fourth International Conference on Networking and Distributed Computing, 2013
26. Survey of Access Control Models for Cloud based Real-time Applications, Balamurugan B, Gnana Shivitha N, Monisha V, Saranya V, 2015 International Conference on Innovation Information in Computing Technologies(ICIICT),,India
27. Toward Energy-Efficient and Trustworthy eHealth Monitoring System Ajmal Sawand1, Soufiene Djahel2, Zonghua Zhang3, Farid Naït-Abdesselam1IEEE/CIC ICCC2014
28. A Dynamic Risk-based Access Control Model for Cloud Computing Aiguo Chen1, Hanwen Xing1, Kun She2, Guiduo Duan, 2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom)
29. Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability, Yue Tong, Jinyuan Sun, Sherman S. M. Chow, and Pan Li, Ieee Journal of Biomedical and Health Informatics, 2014. 18(2).