Computer and Information Science; Vol. 9, No. 4; 2016
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Securing Healthcare Records in the Cloud Using Attribute-Based Encryption

Huda Elmogazy[1] & Omaimah Bamasag[1]

[1] Department of Computer Science, Faculty of Computing and Information Technology, King AbdulAziz University, Saudi Arabia

Correspondence: Omaimah Bamasag, Department of Computer Science, Faculty of Computing and Information Technology, King AbdulAziz University, P.O.Box 42808, Jeddah 21551, Saudi Arabia. E-mail: obamasek@kau.edu.sa

Received: September 6, 2015 Accepted: October 11, 2015 Online Published: November 2, 2016

doi:10.5539/cis.v9n4p60 URL: http://dx.doi.org/10.5539/cis.v9n4p60

Abstract

Cloud Computing has attracted interest as an efficient system for storing and access of data. Sharing of personal electronic health record is an arising concept of exchanging health information for research and other purposes. Cconfidentiality except for authorized users, and access auditability are strong security requirements for health record. This study will examine these requirements and propose a framework for healthcare cloud providers that will assist in securely storing and sharing of patient' data they host. It should also allow only legitimate users to access portion of the records' data they are permitted to. The focus will be on these precise security issues of cloud computing healthcare and how attribute-based encryption can assist in addressing healthcare regulatory requirements. The proposed attribute-based encryption guarantees authentication, data confidentiality, availability, and integrity in a multi-level hierarchical order. This will allow the healthcare provider to easily add/delete any access rule in any order, which is considered beneficial particularly in medical research field.

Keywords: cloud computing, cryptography, threats, attribute-based encryption

1. Introduction

Cloud Computing is an arising technology which revolutionize the use of computing resources. Cloud Computing technology provides users with flexibility, scalability of infrastructure, reliability, sustainability and cost effectiveness. The cloud is defined by google as "the collective power of thousands of computers that serve information to you from far-away rooms distributed around the world."

In current healthcare systems, there is a high demand on establishing a framework that minimizes time-consuming work and expensive procedures to retrieve a patient's medical record and integrating this varying set of medical data consistently to deliver it to the healthcare industry. Electronic health records (EHRs) (DesRoches et al., 2008) (Eichelberg et al., 2005) have been widely accepted to allow patients, insurance companies, and healthcare providers to initiate, control and process patients' healthcare information from any place, and at any time.

Thus, healthcare providers accept moving their data and operations to the clouds that can perform their operations more efficiently and eliminate the physical distance concern between patients and providers. Cloud service enables different doctors to obtain an access to a patient's health record even if they are kilometres apart. There is no need for the doctors to make a phone call to ask for a move of the health records; they will just access them in the clouds.

Despite all the benefits cloud computing provides for healthcare systems, data privacy and security are among the major concerns, which make healthcare move slowly towards the acceptance of these new technologies. Cloud computing benefits come at a price of the emergence of different risks related to information security that must be cautiously addressed. Risks differ according to the criticality of the data to be processed or stored, and how the specific cloud provider has developed their specific cloud services.

In order to be appealing to healthcare community, cloud computing should maintain required guarding to address HIPAA (Health Information Portability and Accountability Act) of U.S. Department of Health and Human Services (2013) and other security and privacy requirements. Although Electronic Health Records (EHRs) has

been regulated in standards, such as HIPAA, several cloud providers are still not compliant with them.

In order to secure healthcare data, the first step to be taken is to categorize the data in the Electronic Health Records (EHRs) in correspondence to its level of security sensitivity. The first category is Personally Identifiable Information (PII), such as patient records, normally saved in a relational database as structured data. The second category is Healthcare data, which is typically consists of large media files such as radiology, CT scan, x-ray, and other types of video and images that conceal patient's identity. Such files are often stored in distributed storage.

A medical record has some components that are classified by both individuals and organizations, such as HIPAA of U.S. Department of Health and Human Services (2005) and HITECH (Health Information Technology, 2009), as highly critical and should be disclosed only to the entities that have an explicit access right to them. This is because revealing such data can lead to unjustly show bias against an individual or refuse them chances that they otherwise entitled to. For example, knowing that a person is diabetic might negatively influence their professional growth, personal relationships, insurance cost, and employment opportunities.

Outsourcing the storage of unencrypted information in the cloud, is of a high danger. For a highly sensitive data, such as Electronic Health Records (EHRs), locating them unencrypted, out of site, is considered against the law. However, to access data stored on a distance server, the Cloud providers need to access the primitive, i.e. un-encrypted, data. Most people do not have full confident on the Cloud providers for their sensitive healthcare data because there is no law regulating how they use this data and whether the patients have control over them. On the other hand, data encryption might counteract the advantages of cloud computing, unless the cloud service providers get the secret decryption key. Traditional cryptography is not a solution in this situation (Alomgazi & Bamasak, 2013).

Patients may only want portions of their record made available to all doctors and specific portions to be available to specific users, i.e. insurance company. Patients can be given maximum control over their data by encrypting each portion of a patient's record under a different policy. Access control policies should be active to ensure that accessing sensitive information is restricted only to parties that have a valid privilege. This feature can be provided by Attribute-Based encryption.

The rest of this paper is organized as follows: in Section 2, we introduce the concept of cloud computing. Section 3 discusses background technologies on using cryptography to secure cloud computing. In section 4, we outline the security issues surrounding healthcare application in the cloud. Section 5 proposes secure healthcare cloud computing framework. Finally, Section 6 concludes this paper and discusses our future direction.

2. Background

The National Institute of Standards and Technology (NIST) (Mell & Grance, 2009) has defined Cloud Computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". The cloud framework consists of five important components, four deployment models and three service models (Alomgazi & Bamasak, 2013).

2.1 Cloud Computing Characteristics

Cloud Computing has many essential characteristics and features. Cloud service users benefit from many features: cost-effectiveness, variability of resources, seamless self-service, flexibility and elasticity, reliability, location independence, and broad network access (Peng et al., 2009). Cloud providers also gain the advantages of scalability of infrastructure, cost-effectiveness, and sustainability (Zissis & Lekkas, 2012).

- *Cost-effectiveness*: One of the major benefits that are offered to both the clients and providers of cloud computing is cost-effectiveness. For clients, it allows the allocation of as much or as little resources necessary for accomplishing the tasks at hand. It also spares the client from the cost of actually allocating the resources on-site when they are not highly utilized (Peng et al., 2009). Furthermore, it saves the maintenance cost of resources. For service providers, it allows for locating resources in an inexpensive real-estate and/or close to cheap power source (Zissis & Lekkas, 2012).

- *Resource utilization*: Cloud Computing service paradigm is centred around better resource utilization leading to long-term sustainability for the resource owner (Zissis & Lekkas, 2012). With different modes of delivery, Cloud Computing allows the client to access varying types of services. Clients can easily demand basic infrastructure services such as power or network, or deployment platform to run their application such as Java or Python, or rented application.

- *Self*-service: Seamless self-service is yet another remarkable feature of Cloud Computing. Clients of cloud services are able to allocate the necessary resources automatically without requiring manual interaction with the cloud service providers via simple user interfaces.
- *Flexibility and elasticity*: Cloud Computing also offers clients great flexibility and elasticity of service according to demand. Clients of cloud services can swiftly benefit from allocated resources. Services can be scaled up by allowing clients to acquire more resources as they progress in their task without additional effort. Scaling down of service is also accomplished seamlessly by releasing unnecessary resources automatically. Hence, resources seem unlimited to clients of cloud services.
- *Reliability*: Reliability is an important feature to the cloud service client which is usually accomplished through the use of multiple redundant service sites providing business continuity and easier recovery in case of disaster (Zissis & Lekkas, 2012).
- *Location independence*: Another feature of Cloud Computing is location independence. Clients need not be aware of the exact location of resources, nor do they need to control it. Still, they are able to specify an abstract location such as a country or city if it is needed (Zissis & Lekkas, 2012).
- *Broad network access*: Cloud services offer broad network access to its clients. Service clients benefit from the standard mechanisms employed by the providers, allowing for diverse access platforms such as, PDA's, laptops or mobile phones (Zissis & Lekkas, 2012). Cloud service providers benefit from scalability of infrastructure. It allows the network to grow or shrink by adding or dropping nodes or servers to the network with minimal modifications at the infrastructure level as well as at the software level (Zissis & Lekkas, 2012). These key features are what make Cloud Computing a promising technology for providing computing resources.

2.2 Deployment Models

There are different ways to deploy and manage service deliveries to Cloud clients. The different ways (also referred to as deployment models) dictate the disposition of resources and the relationships between cloud providers and clients. There are four deployment models: public, private, community and hybrid clouds.

- *Public Cloud*: In the public cloud, Infrastructure and computational resources are owned and operated by a cloud provider, offering to render services to the public over the Internet. Presumably, the provider is an external entity from all the clients.
- *Private cloud*: a private cloud is owned and operated by the organization itself for exclusive resource provision. The organization may also hand cloud management to a third party. In this case, the cloud may be hosted either within the organization's data center or outside of it (Jansen & Grance, 2011). For private clouds, the organization has more control over the infrastructure, the clients, and the services provided.
- *Community cloud*: In the middle between public and private clouds is the community cloud. For this model, the cloud infrastructure and services are customized to a community of clients. The community of clients belong to organizations who share the same policy and security requirements among other considerations (Jansen & Grance, 2011). Cloud infrastructure may be owned and operated by a third party, or one or more of the organizations within the community.
- *Hybrid cloud*: The more complex cloud deployment model is the hybrid model. Hybrid clouds are composed of more than one type, perceived as separate entities while being combined via a set of standards and rules, allowing them to share data and applications among them (Peng et al., 2009).

Different cloud deployment models have different implications on the provision of security and client privacy in the cloud. For private clouds, security provision stays within the organization since it owns the cloud facility or rents it exclusively. However, for public clouds, security provision is managed by service providers leading to challenging circumstances. As for community and hybrid clouds, security provision has the same circumstances as public clouds only for data and processes handled by public facilities.

2.3 Service Models

While deployment models define resource disposition and cloud management, service models define control and level of service abstraction. Most literature identifies three service models: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) (Peng et al., 2009).

IaaS refers to hard-core infrastructure capabilities rendered to the client such as storage space, network bandwidth, power for processing, or any basic computing resource. These resources are obtained by clients as virtualized objects controlled via a service interface, giving clients the freedom to choose the operating system and development environment hosted on these resources (Zissis & Lekkas, 2012). PaaS model allows clients to

develop and deploy their applications on programming platforms rented by the provider such as Python or Java. This model can help the client reduce resource allocation cost and simplify the development and deployment process. It will also allow the client to control applications and application environment settings of the platform (Zissis & Lekkas, 2012). The cloud provider will spare the client the expense and hassle of purchasing, hosting, and controlling underlying hardware and software components, as well as program and database development tools. In the SaaS model, services rendered are applications running on the cloud infrastructure and platform of the service provider via a browser interface or any other thin client. It decreases the cost of software and hardware development, maintenance, and operations for the client. In this case, the client does not have any control over the underlying cloud infrastructure or individual applications, except for selecting usage preference and some administrative settings (Zissis & Lekkas, 2012).

3. **Literature Review**

For access control of patients' EHR outsourced to cloud providers, we assume that they are partially trusted. The goal of cryptographic techniques is to administer who has 'read' access to which portion of a patient's EHR in a detailed way. Three types of cryptography are commonly used to secure EHR records: symmetric key cryptography, public key cryptography, and attribute-based encryption, explained in the following (Madnani & Sreedevi, 2013).

3.1 Symmetric Key Cryptography- Based Solutions

Symmetric-key algorithms belong to a category of cryptography algorithms that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The encryption and decryption keys are equal. A solution for protecting off-site data on semi-trusted clouds was proposed by Vimercati et.al.(di Vimercati, Foresti, Jajodia, Paraboschi & Samarati 2007). Using symmetric-key algorithms, it was able to achieve fine-grained access control. However, the challenges in file creation and the operations of user grant/revocation are in-line with the number of authorized users, which is not scalable.

3.2 Public key cryptography (PKC) based solutions

Public-key based solutions were proposed as it is able to set apart read and write privileges. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter (Benaloh et al., 2009) proposed a public-key based encryption scheme that solved the issue of implementing fine-grained access control. However, this work suffers from high overhead of key management.

A hybrid encryption scheme that integrates RSA, 3- DES and Random Number generator algorithm, is proposed in (Kaur & Bhardwaj, 2012) to improve the security of cloud data storage. This scheme offers the adaptability in sequence and range to the user's selection. This is due to a user may choose to perform all of the three encryption methods or cancel any in any order. The default is applying the random number generator algorithm despite the user not selecting any encryption method, hence, ensuring at least a single layer of security. The selected sequence will also be saved in the database for decryption purpose. The downside of this system is that it heavy on the query performance due to the layered nature of encryption and decryption. In addition, the computation time goes up linearly with the size of data.

3.3 Attribute-Based Encryption solutions

The authors in (Kaur, 2012) described Attribute-Based Encryption ABE as it links both the attributes and policies with the encrypted message. The user then decides which entity, according to the defined attributes, can decrypt the ciphertext. Secret keys for the users are created by a central authority based on attributes/policies specified for each user. Each user in the system is linked with attributes; he receives a key ("or group of keys") from a trusted authority corresponding to his set of attributes. Ciphertext embeds a policy in the form of Boolean predicate over the attribute space. A user can use his group of keys to decrypt the ciphertext only if his attribute set comply with the policy.

Authors in (Akinyele et al., 2010) described ABE in two formulations: ciphertext policy ABE and key policy ABE, explained in the following.

- *Ciphertext policy ABE*: a ciphertext is coupled with a policy specifying which entity is authorized to decrypt it. These policies are generally described as boolean formulae showing a list of attributes that are enclosed into the secret key of the encryptor. As an example, given the attributes: Doctor, Nurse, Massachusetts General Hospital (MGH), InsureCo, the following example policy represents a record that can be read by an MGH doctor or nurse or an insurance agent:

  ((Doctor _ Nurse) ^ MGH) _ ((InsureCo ^ Agent)

- *Key policy ABE*: reverses the relationship between ciphertext and key so that each record is labeled with its corresponding attributes, e.g. Lab Result (record), Cardio (attribute). In order to get access to portion of a record, the record owner, i.e. patient, generates unique key comprising the policy formulae that decides on which entity can access which records.

Collusion resistance is a basic feature of ABE systems (Akinyele et al., 2010). This feature is about individuals who are not able to integrate attributes with their secret keys to fulfill a given policy. For instance, the following policy might denote that only the insurance agent, associated with either the billing company or MGH, can read the patient's prescriptions:

(Billing _ MGH) ^ (InsureCo ^ Agent)

The insurance agent's key associated with the attribute InsureCo cannot be integrated with the billing company's key (i.e., Billing attributes) or with the Doctor's key (i.e, MGH attribute) to fulfill the policy. In this example, a trust relationship has to be established between the insurance agent and the hospital so as to obtain the MGH or Billing attributes. Each symmetric key is generated with a different random initial value, therefore, integrating keys cannot generate a new relevant one (Akinyele et al., 2010).

The depiction of the policy access formulae is considered the strong point of ABE. Access policies can be articulated with AND, OR, and other boolean operators such as <, _, >, and _. Binary numbers typically represents numerical values used in boolean operators so that each bit in the number relates to a non-numerical attribute. A mixture of OR and AND gates are employed to construct a binary tree that depicts contrasting over the non-numerical attributes similar to the ciphertext policy employment of Bethencourt, Sahai and Waters (Goyal, Pandey, Sahai & Waters, 2006). Therefore, ABE enables indicative access control that is cumbersome to achieve with classical access control parameters.

4. Security Challenges

With the many promises of better resource utilization and client-empowerment in healthcare systems, Cloud Computing also presents many challenges, and one of these challenges lies in the issue of security assurance. Xiaoping claims that security issues in the cloud paradigm present the biggest challenge for service providers (Jansen & Grance, 2011). Zissis and Lekkas identify two main security issues in Cloud Computing, which are placement of trust and identification of security threats (Zissis & Lekkas, 2012). In Cloud Computing, the boundaries separating an organization from outsiders become fuzzy making it more difficult to identify trusted parties and to locate security measures (Zissis & Lekkas, 2012). Identification of security threats is also necessary to implement a security system with the appropriate countermeasures.

The security system of a cloud platform should ensure confidentiality and privacy, service availability, data and application integrity and recovery.

- *Confidentiality* assures that information is not disclosed to unauthorized parties while privacy extends further to assure that individuals control who can collect or store information related to them.
- *Availability* assures that services are not denied to authorized clients.
- *Integrity* ensures that data and software can be modified only by authorized parties and in a specified manner.

Our proposed solution will aim to address the above mentioned security requirements using ABE.

5. ABE-Based EHR Security in the Cloud

We propose a secure centralized data sharing framework for healthcare cloud-based EHR, addressing the security requirements specified in Section 4. We shall assume that we have three basic organizations A, B and C in our healthcare industry, as shown in Figure 1.In this section, an overview of the framework is presented. This is followed by the assumptions considered in the design of the proposed ABE-based solution, then the proposed solution is presented.

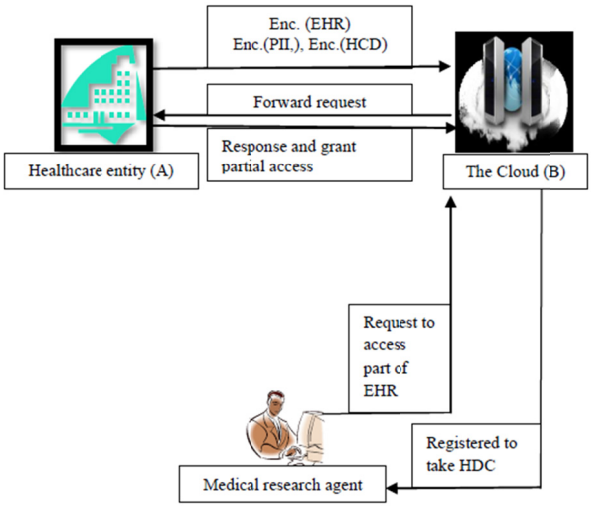

Figure1. A framework for cloud-based secure data sharing

5.1 General Framework

Healthcare entity (A), representing different fields, i.e. primary care, clinical lab, primary, emergency care and pharmacy, host their patients' EHRs in cloud (B). This is to minimize cost of operation and maximize compatibility and seamless delivery of services. Healthcare data can be requested by the research institute (C) for its medical research. EHRs ownership belongs to the healthcare entity (A), which sets policies for access control to enforce which entity/organization can access which fields of its EHRs, with different roles. To address HIPAA and related security and privacy requirements, the medical research institute (C) must not have the right to access Personally Identifiable Information (PII). Administrators carry out management operations, e.g. turning users on or off, and enrolling or de-enrolling medical research institute.

The PII consists of record owner's (patient) type-identifier, e.g. doctor, patient, pharmacy, and attributes that define the identity and specifications of the record owner, e.g. ID, name, specialization, location, etc. In our EHR suggested framework, the patient specifies the entities that can access the data in his medical record and, therefore, decides on the attribute set under which the record is encrypted

The access policies for our proposed solution comprise boolean formulas that employs logical AND and logical OR, on the attributes. For example, the policy ‘ ID999 ∧ doctor' indicates that only an entity who owns the attributes 'ID999' and 'doctor' is allowed access. Our scheme assumes that there is a trusted authority for key generation, which validates the entity's attributes prior to issuing the secret key. The patient can trust that his record can be accessed by user 999 only if he is a doctor by specifying the above access policy (Narayan, Gagne & Naini, 2010).

A patient grants a subject X access to his medical data by adding the subject ID and type-identifier, and other subject specific features, depending on the access policy specified by the patient. An index set is associated with the ciphertext that consists of the unique subject ID. The access requestor cannot decrypt the data if his subject ID is not in the index set.

5.2 Assumptions

Our proposed solution is built on the following assumptions.

- There exists a trusted authority (TA) who is honoured by all parties in the framework to generate keys for system's users. TA also publishes, in a public directory, the system's public parameters, i.e. public keys, and other data required for cryptographic functions.
- A subject X is coupled with an exclusive identifier (ID), and a set of attributes (ω). Each subject is linked with a public key and a corresponding private key. Both keys are created and released by the TA after authenticating the subject’s attributes.
- The EHR database is located in and stored by a cloud service provider. This provider is trusted by the system's entities to perform the required operations but should not have the ability to perform any operation beyond what was specified.

5.3 Proposed Solution

The attribute-based ciphertext policy encryption scheme, which we will use, inspired by (Narayan, Gagne & Naini, 2010), comprises five algorithms namely: Initialize, Key-Gen, Encrypt, Decrypt, and Revoke.

- *Initialize(y):* having a security parameter y , the algorithm generates the public key *pub-key* and master secret key *Master-sk*. The system public key *pub-key* is a collection of public information.
- *Key-Gen(pub-key, Master-sk, ω, ID)*: having as input an attribute set ω, user-ID *ID*, public key *pub-key*, and the master secret key *Master-sk*, the algorithm generates the private key $pk_{ID,\omega,}$ related to ω.
- *Encrypt(pub-key, M, IS, AS):* Given a message M (EHR), *pub-key*, user-id set *IS* and an access structure *AS*, the encryption algorithm outputs the ciphertext *CT* holding the encrypted message.
- *Decrypt(pub-key,CT,* $pk_{ID,\omega}$*)*: This algorithm's inputs are the ciphertext *CT* and the private key $pk_{ID,\omega}$ for the attribute set ω. It decrypts the ciphertext *CT* if $\omega \in AS$ and $ID \in IS$. If it decrypted successfully, it outputs the plaintext *M*, else outputs 0.
- *Revoke(*HP_i*, CT)*: A user, i.e. a patient, can remove the access of a client HP_i, i.e. healthcare provider, to the encrypted record *CT*.

Here, we will explain the steps of the ABE algorithms in our proposed framework, as shown in Figure 1. The setup step consists of the generation of system's parameters using Initialize(*y*) algorithm. This is followed by generating the private key $pk_{ID,\omega}$ using Key-Gen(*pub-key*, *Master-sk*, *ω, ID*) algorithm. Both steps are performed by the trusted authority TA. The healthcare entity (A) then encrypt EHRs using Encrypt(*pub-key*, *M*, *IS*, *AS*) algorithm. The patient uploads the encrypted record *CT* together with the access policy and search index to the cloud (B). Only approved entities (C) can be granted access to the corresponding parts of the encrypted EHR data by the decryption algorithm Decrypt(*pub-key*, *CT*, $pk_{ID,\omega}$), hence satisfying the confidentiality, availability and integrity requirements mentioned in Section 4. The user will sign in into the system via a web application. The identity of the user will be verified against sign in database, which will perform the check based on attribute authentication system. The medical research agent (C) will ask to access parts of EHRs to conduct their research. This request is forwarded to healthcare entity to get authorization to access specific healthcare data for specific time. After that this access will be invalidated using *Revoke(*HP_i*, CT)* algorithm.

5.4 Security Analysis

Our proposed solution provides confidentiality of EHR through the use of strong attribute-based encryption. The encrypted EHR can be decrypted by an entity with private key $pk_{ID,\omega}$ only if its attribute set ω is in the EHR access structure AS and its ID is in the user-id set IS. Therefore, if the EHR database is attacked, the attacker will not learn anything about the EHR stored in the cloud without the corresponding private keys.

Consequently, only legitimate entities, with the appropriate private keys and access privileges can read, change, or delete EHR from the database in the cloud, hence, ensuring integrity of the EHR.

Both the cloud service provider and the underlying ABE encryption are assumed to work properly and meet the demand of all system's entities, i.e. A, B, C. Hence, addressing the availability requirement.

6. Conclusion

In this paper, we have explored the use of Attribute-Based encryption to secure EHRs. For future work, we plan to further investigate and implement the proposed system in a suitable simulation platform. We will also evaluate the security and performance of the proposed system after being implemented and compare them with the most related work in the area.

References

Akinyele, J., Lehmann, C., Green, M., Pagno, M., Peterson, Z., & Rubin, A. (2010). Self-Protecting Electronic Medical Records Using Attribute-Based Encryption. *Technical Report 2010/565*, Cryptology e-Print Archive.

Alomgazi, H., & Bamasak, O. (2013). Towards Healthcare Data Security in Cloud Computing, *Proceedings of the International Conference for Internet Technology and Secured Transactions*, IEEE Society, 363-368, http://dx.doi.org/10.1109/ICITST.2013.6750223

Benaloh, J., Chase, M., Horvitz, E., & Lauter, K. (2009). Patient controlled encryption: ensuring privacy of electronic medical records. *Proceedings of the 2009 ACM Workshop on Cloud Computing Security CCSW'09*, 103–114. http://dx.doi.org/10.1145/1655008.1655024

DesRoches, C., Campbell, Rao, E, S., Donelan, K., Ferris, T., Jha, A., Kaushal, R., Levy, D., Rosenbaum, S., &

Shields, A., (2008*).* Electronic health records in ambulatory care - a national survey of physicians. *New England Journal of Medicine, 359*(1), 50-60. http://dx.doi.org/10.1056%2FNEJMsa0802005

Vimercati, S. D. C., Foresti, S., Jajodia, S., Paraboschi, S., & Samarati, P. (2007). Over-encryption: management of access control evolution on outsourced data. *Proceedings of the 33rd International Conference on Very Large Databases VLDB '07*, 123–134.

Eichelberg, M., Aden, T., Riesmeier, J., Dogac, A., & Laleci, G., (2005). A survey and analysis of electronic healthcare record standards. *ACM Computing Surveys (CSUR), 37*(4), 277-315. http://dx.doi.org/10.1145/1118890.1118891

Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM Conference on Computer and Communication Security CCS '06*, 89–98. http://dx.doi.org/10.1145/1180405.1180418

Health Information Technology. (2009). *The Health Information Technology for Economic and Clinical Health (HITECH) Act*, Retrieved from https://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing, *NIST special publication, 800*, p. 144.

Kaur, A., & Bhardwaj, M., (2012). *Hybrid Encryption for Cloud Database Security*, IJESAT, 2(3), 737 – 741, Retrieved from http://www.ijesat.org

Kaur, S., (2012). Cryptography and Encryption In Cloud Computing. *VSRD International Journal of CS & IT, 2*(3), 242-249.

Madnani, B., & Sreedevi, N. (2013). Attribute Based Encryption for Scalable and Secure Sharing of Medical Records in Cloud Computing Design and Implementation. *International Journal of Innovative Research in Computer and Communication Engineering*, 1(3).

Mell, P., & Grance, T., (2009). *The NIST Definition of Cloud Computing*, version 15, National Institute of Standards and Technology (NIST). Retrieved from http://www.csrc.nist.gov

Narayan, S., Gagne, M., & Naini, R. (2010). Privacy Preserving HER System Using Attribute-based Infrastructure. *Proceedings of 2010 ACM Workshop on Cloud Computing Security Workshop CCSW' 10*, 47-52. http://dx.doi.org/10.1145/1866835.1866845

Peng, J., Zhang, X., Lei, Z., Zhang, B., Zhang, W., & Li., Q. (2009). Comparison of several cloud computing platforms. *Proceedings of The Second International Symposium on Information Science and Engineering (ISISE)*, 23-27. http://dx.doi.org/10.1109/ISISE.2009.94

U.S. Department of Health and Human Services. (2013). *The health insurance portability and accountability act*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems,* 28(3), 583-592. http://dx.doi.org/10.1016/j.future.2010.12.006