Research Journal of Applied Sciences, Engineering and Technology 15(9): 344-355, 2018
DOI:10.19026/rjaset.15.5925
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: May 22, 2018 Accepted: July 6, 2018 Published: September 15, 2018

Research Article

Introducing Usage-Based Encryption for a Secure and Versatile Access Control Scheme of Electronic Health Records on Cloud

[1]Marie Khair, [2]Chady El Moucary and [2]Walid Zakhem
[1]Department of Computer Science, Notre Dame University-Louaize
[2]Department of Electrical, Computer and Communication Engineering, North Lebanon Campus,
Barsa-El Koura, Lebanon

Abstract: In this study, we introduce Usage-Based Encryption (UBE) approach for a secure, efficient, ubiquitous and versatile management of Electronic Health Records (EHRs) on cloud. The primordial feature lies in delegating the fundamental security guidelines and procedures to the patient in terms of encryption, access control and digital signatures. In contrast with other frequently used approaches, the proposed scheme grants the patient enhanced independence from cloud providers' policies and thus, renders increased administrative authority while sustaining a highly flexible and resourceful configuration. A comprehensive scheme is painstakingly detailed to encompass all tangible situations pertaining to a highly effective control of the EHR in a platform-free sphere. As a matter of fact, encryption and hashing modi operandi are scrupulously and relevantly fixed on to guarantee Confidentiality, Integrity and Availability (CIA). Furthermore, privileges and revocation of access are discussed in their minutiae from a usage perspective to provide patients broader maneuverability of their health records prior to housing them on clouds.

Keywords: Access control, CIA, cloud, Electronic Health Record (EHR), Usage Based Encryption (UBE)

INTRODUCTION

P4 medicine or what is referred to as "Personalized, Predictive, Preventive and Participatory medicine" seems to pave a new age for an ever evolving and more daring approach to healthcare, worldwide. Promising measurement-and-diagnosis emerging technologies, almost-application-unlimited computational capabilities and ubiquitous access and/or transfer of information online using either internet or outernet infrastructures, have invigorated this promising avenue to start infiltrating into the medical system for numerous pertinent and relevant reasons. Examinations need no more take place at hospitals or clinics, but can be done "anywhere" and specialists or even intelligent expert systems would instantaneously analyze and make decisions in terms of prescriptions, medical conditions, prognosis, emergency alerts, etc. On the other hand, accessibility of patients' medical records might unveil hidden snags and pitfalls and seems to turn into a source of dilemmas and controversies regarding who should own the "medical data"; the use of connectivity for data availability and transmission can be easily intercepted and meddled for nefarious purposes. Issues of privacy and legal facets just add to the challenge but would certainly not hinder throwing down the gauntlet of traditional medicine, at least not for a long time, before witnessing the transformation of the entire process toward a more effective and somehow unavoidable path (Hood and Friend, 2011; Hood and Flores, 2012; Flores *et al.*, 2013; Younesi and Hofmann-Apitius, 2013; Topol, 2015; Pack, 2016; Shortliffe and Cimino, 2013).

Recently, up-and-coming various strains and conundrums defy CDCs (Center for Disease Control), welfare and Businesses at large such as impending pandemics and their sequelae, safety and security repercussions associated with key personnel working in public enterprises such as nurses, doctors, aircraft crews, teachers and many other sensitive vocations and professions, etc., and which all endorse the idea of having some medical data obtainable within certain frameworks. Paper charts still exist in clinician offices, medical centers and hospitals; nonetheless, Electronic Medical Records (EMRs) and which are the digital versions of such information, reveal more beneficial and advantageous because they empower healthcare providers and officials with the capacity of tracking, identifying and preventing the aforementioned related issues; they are more legible, of course, as well. Furthermore, Electronic Health Records (EHRs) are

Corresponding Author: Marie Khair, Department of Computer Science, Notre Dame University-Louaize

devised now to be more broad and comprehensive hence, encompassing contact information, historical figures and mostly all relevant details to patients and their families, collected from healthcare providers of all kind and aim at sharing that information with authorized agencies and stakeholders such as laboratories, specialists, diagnosticians, legal experts, etc., across patients' country and sometimes beyond borders. EHRs can be used for quality improvement, population reporting, clinical research, health statistics, standardization, etc., (Bresó *et al*., 2015; Alyass *et al*., 2015; Ball and Lillis, 2001; Shortliffe and Cimino, 2013; Bates *et al*., 2001; Dolin, 1997).

EHRs are even inclusive of conditions of being sound in body, mind or spirit, freedom from physical disease or pain, etc., encapsulating the fact that the word "health" ranges more in sphere than the word "medical". This is in contrast with Personal Health Records (PHRs) which are privately managed by patients to follow up on their own health information yielding no public interest and/or concern in any way, shape or form. This raises the vital question of how to protect data from intruders and malicious attackers if we were to implement rife and omnipresent online medical databases and platform-independent applications (Dolin, 1997; Iakovidis, 1998; Papagounos and Spyropoulos, 1999; Garets and Davis, 2006).

In this study, we propose a quite outright stratagem that efficiently achieves bridling the setbacks and hitches of a "traditional" platform in order to secure the two paramount objectives of autonomy and non-maleficence. Our promising approach relies on segregating EHRs into four primary segments based on a combination of parameters such as content, usage-purpose and sensitivity. Furthermore, different concomitant management subsystems in terms of encryption, access control and revocation, are used to ultimately and eventually provide a secure encapsulation of data onto cloud. Not only data will be encrypted when stored, but during upload/retrieval to/from cloud, as well. Besides, those actions shall be carried out while sustaining an optimal use of resources such as computational cost, management and storage space (Garets and Davis, 2006; Morton and Wiedenbeck, 2009; Collins *et al*., 2011; Kluge, 2004).

Usage-Based Encryption (UBE) will primarily depend on three variants of Federal Information Processing Standards (FIPS): the Advanced Encryption Standard (AES), the Rivest-Shamir-Adleman (RSA) and the Secure Hash Algorithm (SHA), which have been broadly adopted in innumerable applications because of their multifaceted virtues. Access control and revocation, privileges and other relevant security issues are devised in the context of securing the three main CIA components of a sound and sustainable EHR.

Furthermore, the entire EHR will be hosted on cloud which offers a ubiquitous and unlimited platform with a multitude of advantages when compared to other more traditional ones. Nonetheless, hosting information on cloud comes with a price: security is not absolutely guaranteed. Particularly, two critical and fundamental issues constitute imminent trust issues and risks: immunity of the algorithms used against attacks and administration. Our strategy includes tackling those major setbacks by giving the hand to the patient for optimal customization. This would remarkably find applications in developing countries where no structures for secure platforms exist to begin with (Bahga and Madisetti, 2013; Narayan *et al*., 2010; Zhang and Liu, 2010; Basu *et al*., 2012; Löhr *et al*., 2010; Xavier and Chandrasekar, 2015).

The main forte of the proposed scheme lies in endowing the patient with the lead in managing the EHR which will be fashioned on a usage-based platform rather than attributes or other more advanced parameters, whilst upholding a realistic user-friendly handle. Indeed, patients are becoming more involved in technology, managing smart devices and will inevitably be grasping IoT hence the proposed strategy would indubitably come home to them (Narayan *et al*., 2010; Zhang and Zhang, 2011; Yang *et al*., 2015).

This study will be divided in three sections. In the first one we will recall, validate and highlight the tools used in our platform; the second part will thoroughly encompass the core of the modus operandi which is entailed by the proclaimed lead via a systematic allocation of the tools in corroboration of specific and pertinent EHR component usage. A conclusive third section shall wrap up the presented components with key insights to the advantages and effectiveness of the overall structure.

LITERATURE REVIEW

Cloud computing: Cloud computing or simply cloud, is a physical, yet end-user virtual infrastructure which provides ubiquitous, utilitarian, per-demand access to remote, distributed and shared computing resources such as servers, applications, storage, networks, etc. and which can be swiftly supplied and freed up or idled with marginal supplier interface. According to NSIT, the model is composed of 5 essential characteristics, 3 service models and 4 deployment models. Core and prime interests in this context lie in the fact that cloud offers capabilities that appear both unlimited and omnipresent to the client throughout various physical and virtual resources subtending storage space, computational capabilities, bandwidth, etc., via dynamic allocation, contingent on the setup request. Moreover, the three service models - Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) - as well as the various deployment models (e.g., private, community, public and hybrid) - offer an unprecedented and unequaled platform to deploy applications, memory and connectivity at their finest! Cloud was introduced in the late 2000s to allow for economies of scale over networks thus, granting organizations, companies, institutions, etc., the capability of moving from CAPEX (Capital Expenditures) to OPEX (Operational Expenditures) models of business via delivering maximal efficiency of shared resources and drastically reducing those businesses' infrastructure cost which would then be able to contemplate on their vision and ultimate objectives minus worrying about resource expertise, licensing, management, maintenance, operability, provision, etc., (Deepika *et al*., 2015; Griebel *et al*., 2015; Yang *et al*., 2015; Liu *et al*., 2015b, 2015a).

Cloud is a growing grid witnessing a rapid growth of approximately 50% every year, yet its major setback resides in security and privacy issues. Information belonging to one client could be accidentally delivered to another as well as it might be simply intercepted by malicious attackers with villainous and/or iniquitous schemes. Consequently, even though cloud offers an unquestionably beneficial advantage for application and data storage, information need be protected against both intentional and unintentional misfortune (Jin and Chen, 2015; Ali *et al*., 2015).

Advanced Encryption Standard (AES): The workhorse of our encryption process is the Advanced Encryption Standard (AES), a matrix-based data structure relying primarily on substitution-permutation networks. AES is fast in both software and hardware implementations. AES is interchangeably referred to as the Rijndael Cipher Algorithm which has been selected, after five years of standardization, by the US National Institute of Standards for Technology (NIST) in 2001 amongst fifteen contending algorithms to become the first publicly open cipher symmetric-key algorithm approved by the National Security Agency (NSA) for sensitive information (Rijmen and Daemen, 2001; Daemen and Rijmen, 2002; Standard, 2001; Sanchez-Avila and Sanchez-Reillol, 2001).

AES is in point of fact a variant of the Rijndael algorithm created by two Belgian cryptographers, Joan Daemen and Vincent Rijmen with a family of ciphers of various sizes pertaining to both keys and blocks; NIST selected only 3 different-key length versions but with a fixed block size, however. AES is included in the International Organization for Standardization/ International Electrotechnical Commission ISO/IEC 18033-3 standard where specified-length string-of-bits symmetric systems used to produce ciphertexts, denoted as block ciphers, are stipulated.

AES was designated as the US Federal Information Processing Standard (FIPS) 197; FIPS are specified standards devised for use in computer systems by non-military government agencies or contractors with the aim of establishing requirements affecting computer security and interoperability where apposite conventions do not already exist; they customarily consist of tailored versions of those standards used in technical communities such as the American National Standards Institute (ANSI), the Institute of Electrical and Electronics Engineers (IEEE) and the International Organization for Standardization (ISO). The AES algorithm supplanted the Data Encryption Standard (DES) which was based on Horst Feistel design developed at IBM in 1977 and entitled as the FIPS 46-3 (Rijmen and Daemen, 2001; McLoone and McCanny, 2001; Akkar and Giraud, 2001; Nechvatal *et al*., 2001).

AES is a much more advanced algorithm in comparison with its precursor DES in terms of security and immunity against attacks. AES addressed two fundamental weakness and vulnerability issues; the encryption-key length has been multiplied and 128-, 192- and 256- variants were developed, making the algorithm unbreakable to known practical attacks that would allow anyone to read correctly implemented AES encrypted data. AES also refashioned the design and size of the encrypted block; it doubled its size which drastically augmented the amount of information that can be sent before engendering identical blocks which would probably yield to information leaking; this amount soared from 32 gigabytes to 256 exabytes (or 256 billion gigabytes). Moreover, AES' McCoy banks on a series of substitution and permutation instead of using the balanced Feistel network which renders the entire structure dramatically further immune to attacks. Finally, the U.S. Government announced that AES could be used to protect classified information in June 2003 and in 2011, Bogdanov *et al*. (2011) completed the first key-recovery biclique attack on full AES, which is faster than brute force by a factor of about four and concluded that theoretical attacks have no practical knock-on effect on AES security whatsoever in this context. In fact, the authors were visiting Microsoft Research Redmond while working on the results which proved that it requires 2^126.1 operations to recover an AES-128 key meaning that it would take billions of years for recovery as well as the need for storing 2^88 bits of data equivalent to about 38 trillion terabytes of data-more than all the data stored on all the computers on the planet (Sanchez-Avila and Sanchez-Reillol, 2001; Nechvatal *et al*., 2001; Alanazi *et al*., 2015; Yang *et al*., 2015; Guo and Yau, 2015; Nagaty, 2015; Alshehri *et al*., 2012).

Rivest-Shamir-Adleman (RSA): In symmetric-key cryptography, every partaker has an identical private key. As the number of stakeholders increases, the transaction in question becomes more in jeopardy. An additional downside of symmetric-key cryptography is that the process is drastically slowed down (about thousand times) for every encryption/decryption maneuver compared to Public-Key Cryptosystems (PKCS). In the latter configuration, the key distribution is much easier since only the private key must remain confidential and thus, fewer keys need be generated - O (n) compared to O (n^2) (Thakur and Kumar, 2011;

Burnett and Paine, 2001; Grollmann and Selman, 1988; Pointcheval, 1999; Cramer and Shoup, 1998; Wang *et al*., 2008; Wander *et al*., 2005; Gaubatz *et al*., 2004).

RSA (R. Rivest, A. Shamir and L. Adleman) is one of the earliest functional public-key cryptosystems introduced in 1977 and is extensively utilized for secure data communication. As such, the encryption key is public and differs from the decryption key which is privately retained. In this context, public-key cryptography is commonly referred to as asymmetric. RSA is based on the complexity of factoring the product of two large prime numbers and is believed to be an exponential-time problem since to be cracked, solving discrete logarithm or factoring is required; it is a generalization of the Fermat's theorem in modular arithmetic. Most configurations use RSA-1024 for it is practically unbreakable due to relatively-limited existing computational scopes; at the present, new standards employ RSA-2048 keys which are as challenging to hack as AES-128 - this is due to the fact that asymmetric keys need be much lengthier than their symmetric counterparts to accomplish a comparable shield.

Furthermore, since public-key systems have interchangeable keys, RSA offers the feature of digital signatures which can be implanted by hashing the message prior to encrypting it with the private key; the recipient would then be able to uniquely ascertain the authenticity/identity of the sender whilst verifying the integrity of the received hashed/signed message, as well; this inhibits intercepting listeners from deceiving the partakers in communication. The glaring setback of symmetric-key approach in terms of figuring out a secure manner to swap keys becomes in fact a dominating strength of PKCS (Somani *et al*., 2010; Cao and Fu, 2008; Negi *et al*., 2015).

Digital certificate and Secure Hash Algorithm (SHA): Digital certificates are obtained to create trustworthy communication channels. Digital certificate or public key certificate allows proving ownership of a public key via a document purchased from a certificate authority which typically comprises a serial number, the name of the certificate holder, a time-period validity, the public key of the certificate holder (to which a corresponding private key is securely kept) and the digital signature of the certifying agency (so that any recipient can validate the authenticity of this certificate), as well. Digital certificates matchlessly bind an identity with a public key.

Hashing uses asymmetric encryption algorithms in order to verify the validity, legitimacy and genuineness of digital data in the context of communication - it constitutes a valid tool to ascertain of the authenticity of the sender by revealing the identity of the owner of the original data and the integrity of the data by unquestionably signaling a likelihood of tampering. Moreover, it is endowed and vested with non-repudiating features meaning that the sender cannot disclaim sending that received data in any way, shape, or form.

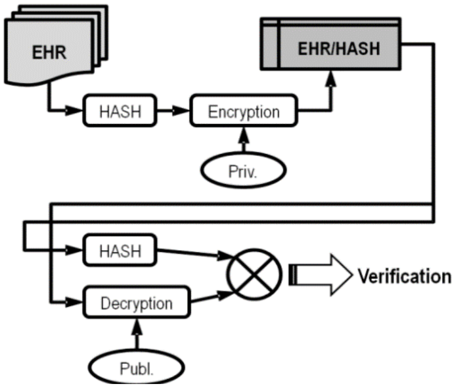


Fig. 1: Hashing algorithm

One of the most widely employed and effective protocols for hashing uses cryptographic hash functions which guarantee 4 ultimate features: simplicity, irreversibility, uniqueness and avalanche effect. The Secure Hash Algorithm (SHA) is a family of cryptographic hash functions distributed by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS) and which allows signing such a hash instead of the whole document and generating fixed string messages of 128 or 160 bits long; the input data is referred to as the message and the hash value is called the digest (Eastlake and Jones, 2001; Sklavos and Koufopavlou, 2003; McEvoy *et al*., 2006; Gilbert and Handschuh, 2003).

Figure 1 below depicts the hashing process employed in our configuration; public key is used for encryption with hashing whilst decryption is accomplished via private key.

In this context, various SHA algorithms will be used for digital signature in our scheme; the outcome is, as it is already known, data that cannot be possibly forged; verification is in fact incontestable.

MATERIALS AND METHODS

This study has been the subject of student's projects, thesis and collaborative research work amongst the authors.

Whilst healthcare industries, media and official/governmental organizations frequently use the terms Electronic Medical Record (EMR) and Electronic Health Record (EHR) interchangeably, it is important at this stage to state that there is a clear difference between the two concepts. As a matter of fact, the EMR is the lawful account/documentation created in hospitals and/or ambulatory contexts and constitutes the source of data for the EHR which establishes the platform to share medical information amongst pertinent stakeholders subtending patients, healthcare providers, insurers, governmental organizations, etc., (Garets and Davis, 2006).

Generally, medical (or health) records can be segregated into various and well-diversified sections

Table 1: Below incorporates the details of the proposed method in encrypting/accessing the before mentioned EHR constituents in terms of policies, specification requirements and deemed actions

Publ-ER	Prvt-ER	Prvt-MED	Prvt-No MeD
Posting the data on the cloud			
The owner hashes and then uses his private key to sign the hash of the Publ-ER.	The owner chooses the persons or institutions he wishes to grant privileges to for each of the Prvt-ER, Say for example U1, U2, … Ui. The owner gets the public keys of the users so he will have kU1pub, KU2Pub, ... KUiPub.	The owner chooses the persons or institutions he wishes to grant privileges to for each of the Prvt-Med, Say for example G1, G2, …Gj. The owner divides his data into subgroups D1, D2, … Dn where each subgroup is of a specific nature for example labs, x-ray, prescription…	The owner chooses the persons or institutions he wishes to grant privileges to for each of the Prvt-NoMed Say for example R1, R2, ... Rk. The owner gets their public keys by using their certificates so he will have KR1pub, KR2Pub, ... KRkPub.
	The owner encrypts the emergency data using these different public keys. So he applies: E (Prvt-ER, Ku1pub), E (Prvt-ER, Ku2Pub), E (Prvt-ER, KUnPub).	The owner fills in the matrix: $\begin{array}{ccccc} & G1 & G2 & …. & Gj \\ D1 & 1 & 0 & & 1 \\ D2 & 0 & 1 & & 1 \\ Dn & 1 & 1 & & 0 \end{array}$ 1 is used when the owner wants to give privilege to the user for the group of data, 0 is used otherwise. A clustering algorithm is be used on the matrix. Such as cl1: (D1, D3), cl2 (D3, D6.), cl3… For each cluster the owner create a common symmetric master key MasterKey1, MasterKey2 and MasterKey3. The owner sends the masterKey1 to the all users in the group encrypted by their Public Key, For example send MasterKey1 as follows: E (Masterkey1, KG1Pub) to G1, E (Masterkey2, KG2Pub) to G2…	The owner chooses different symmetric keys K1, K2, … Kk and applies E (K1, KR1pub) and sends to the user R1 same for all the other users. who are usually few.
The owner posts the public data in addition to its signed hashing on the cloud.	The owner posts all of this data on the cloud.	Apply E (cl1, MasterKey1), E (cl2, MasterKey2), E (cl3, MasterKey3) and post on the cloud.	The owner encrypts the data for example D1. By applying E (D1, K1) and posts on the cloud. Same for the rest.
Accessing data by legitimate users			
Any user can read the above data. In addition, any user, having the public key of the owner can verify the integrity of the data.	Any user Ui who wishes to have access to this data can use his private key to apply E (E (Prvt-ER, KUipub), KUipriv) and accesses the data.	Any user who wishes to access the data can apply E (E (Masterkey1, KG1Public), KG1Priv) and obtain masterkey1. Then, the user can use the Masterkey1 to apply D (E (cl1, MasterKey1), Masterkrey1) and have access to the data in the cluster.	Any user Ri who wishes to have access to this data can use his private key to apply E (E (K1, KRipub), KRipriv) and accesses K1. Later he can use K1 to apply D (E (D1, K1), K1) and accesses the data.
Revocation of access			
No revocation is needed.		In case of revocation of access the data is re-encrypted with a new master symmetric key.	

based on two ultimate and fundamental properties: document-centric and data-centric.

A typical medical record embraces elements such as a document header where rather conventional demographic data are established - for instance, patient name, gender, address, date of birth, identity card number, patient health number, some relevant dates of admission/discharge, etc. History, physical and consultation reports constitute another element which subtend information pertaining to history of present illness, past medical history, medications, physical examination in terms of vital signs (heart rate, pulse, blood pressure and body temperature), diagnostics, assessment and prescriptions, procedure history and results, allergies and adverse reactions, social and family history in terms of risk factors, marital status, psychological health, genetics, etc. Finally, operative and discharge reports constitute an additional and essential element in case the patient had undergone surgeries with the aim of underlying diagnoses prior and post procedures including looming complications.

Be that as it may, EHR will be viewed differently from the patient’s perspective in terms of privacy and secrecy of information and thus, will be accordingly segregated and divided to reflect specific requirements when sharing information is on the Table 1. The proposed scheme spares the patient from digging into advanced concepts and offers a user-friendly platform to manage access control, encryption level and revocation of privileges; it rather subdivides data based on its usage. Additionally, it offers an effective tool for patients to preserve their right to privacy, particularly in countries or environments where no systematic policies are implemented in the context of a typical EHR and where no security/privacy legislation are in place, such as HIPAA in the United States.

Our method is founded on dividing EHRs into the following 4 components:

- A public component designated by Publ-ER and which is related to impromptu and urgent situations such as when patients are administrated by ER medical personnel; this component shall comprise data such as contact information, blood type and other records that are purposely chosen by patients such as allergies and the like.
- A private component designated by Prvt-ER that resembles the previous component with the main difference lies in the content; data is more sensitive and patients shall specify the type of information and the users who would be allowed to access and/or transfer them. The content is truly broad and subtends information such as pieces or entirety of their chronological records in terms of illnesses, treatment, prescriptions, surgery, etc.
- A private component designated by Prvt-MED and which refers to more specific, case-dependent, targeted and/or personal information that is shared by a patient with doctors and diagnosticians whether those are specialists, generalists, or family doctors and thus, information here shall consist of diversified medical data in terms of laboratory tests, all kind of medical imaging and radiography (X-rays, MRI, CT-scan, fluoroscopy, etc.), chronic diseases, illnesses, procedures, other health issues (mental, psychological, etc.), therapies, medications, etc.
- A private component designated by Prvt-NoMeD and which refers to rather non but related to, medical information such as insurance- and financial- related data, subject matters pertaining to family/friends/acquaintance, etc.

RESULTS AND DISCUSSION

As mentioned before, Fig. 2 shows complete setup of the EHR which is divided in our simulation into 4 parts and are fully controlled by the patient.

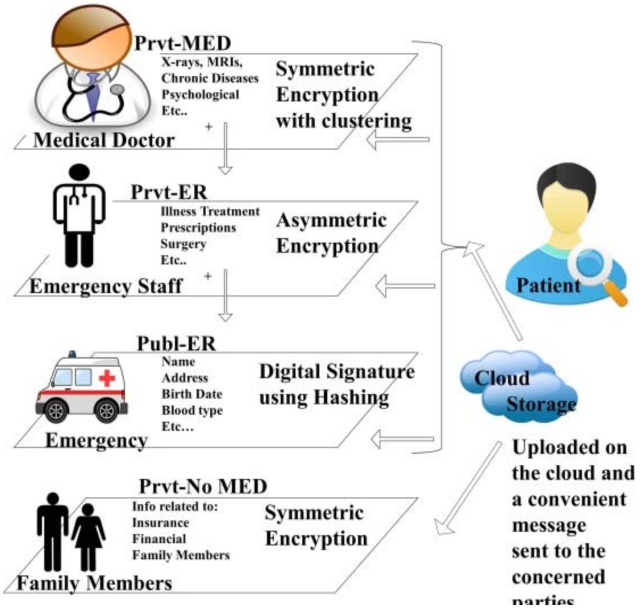


Fig. 2: Complete setup

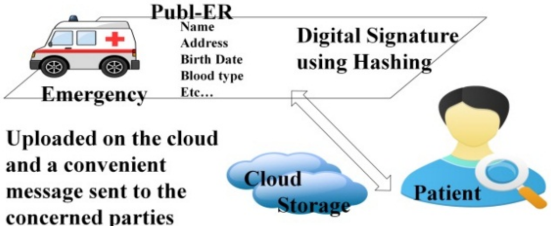

Publ-ER
Name
Address
Birth Date
Blood type
Etc…
Digital Signature using Hashing
Emergency
Uploaded on the cloud and a convenient message sent to the concerned parties
Cloud Storage
Patient

Fig. 3: Publ-ER

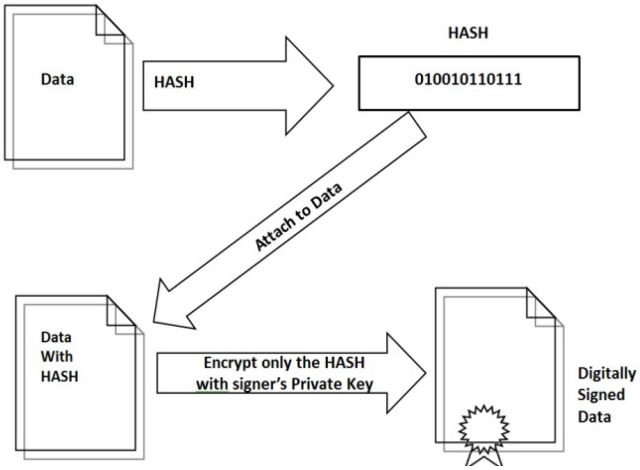


Fig. 4: Hash

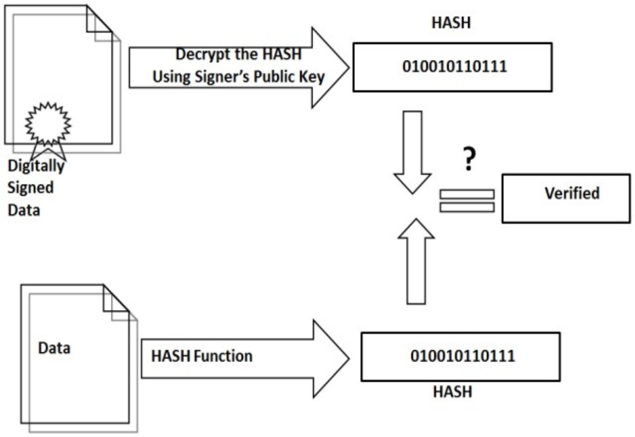


Fig. 5: Hash check

Publ-ER part of the HER: The first part, as in Fig. 3, called Publ-ER, contains any data that the patient judges is necessary to be accessed during emergency cases. This data is hashed first using a hashing algorithm and then the hash is encrypted with digital signature using the private key of the patient. This data is uploaded to the cloud and either a convenient message sent to the concerned party (ies) or carried on with the patient himself.

Hashing algorithm, as in Fig. 4, should only be used for verification of integrity. The data could be Hashed using SHA256 algorithm, a 256 character is created. The Hash is then encrypted using signer's private key.

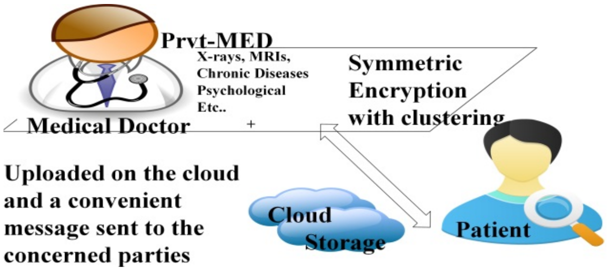
The patient should choose to have his Name, Date of Birth, Blood type, any organ donation if exist and any information should he chose to have access to any emergency team.

The emergency team could have access to all chosen data available for them but the first they should check its integrity and authenticity, as in Fig. 5, to make sure that the data is not altered in any way or form. While the data is available as text format with its Encrypted HASH character, the team could decrypt the HASH using the signer's Public Key and compare it to the HASH of the data itself, if it matches then the data is authenticated and verified.

Prvt-MED and Prvt-No MED parts of the EHR: For the 2nd and 3rd parts, Prvt-MED, as in Fig. 6 and Prvt-No MED, as in Fig. 7, the patient uses Symmetric encryption and uploaded to the cloud, but with one key shared between both parties the patient from one side and his family members from the other side.

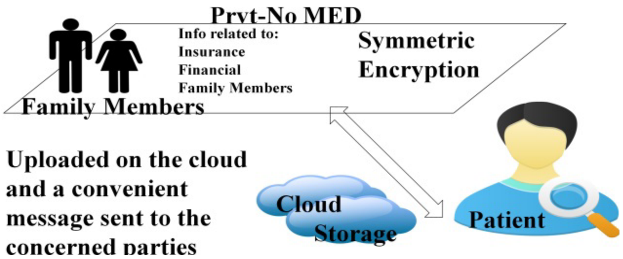
The Symmetric encryption used can be simulated using Matlab GUI, as in Fig. 8, it can encrypt a text file as well as an image sourced from for example sourced from an X-Ray machine. That same GUI is simulated so that both encryption and decryption are both tested.

The Matlab GUI will create a security code to be initialized and saved for later use for the decryption to recreate the image as in Fig. 9. It will also input the



Uploaded on the cloud and a convenient message sent to the concerned parties

Fig. 6: Prvt-MED



Uploaded on the cloud and a convenient message sent to the concerned parties

Fig. 7: Prvt-No MED

Fig. 8: AES GUI

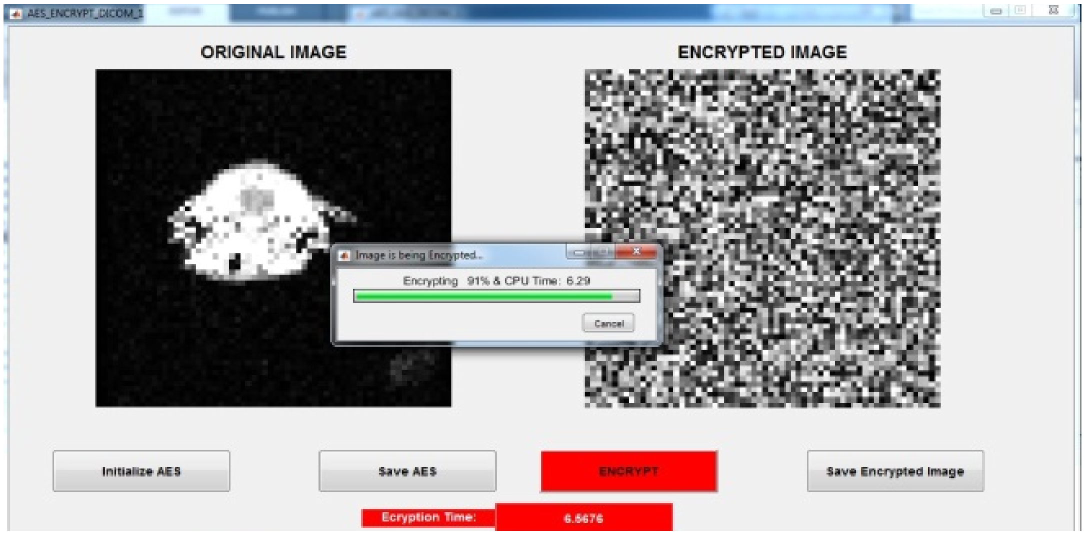
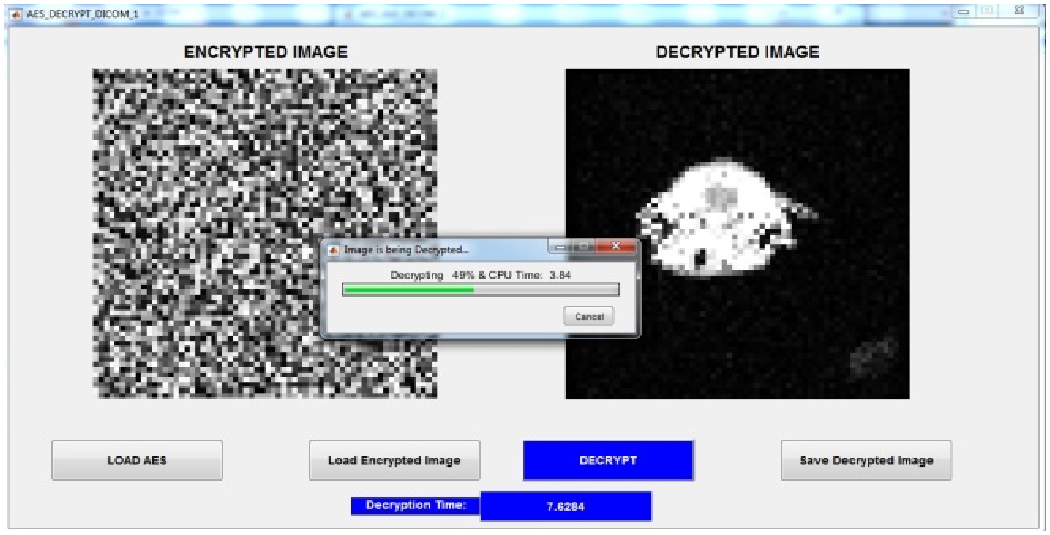


Image is being Encrypted..

Encrypting 91% & CPU Time: 6.29

Ecryption Time: 6.5676

Fig. 9: AES encryption process



Decrypting 49% & CPU Time: 3.84

Decryption Time: 7.6284

Fig. 10: AES decryption process

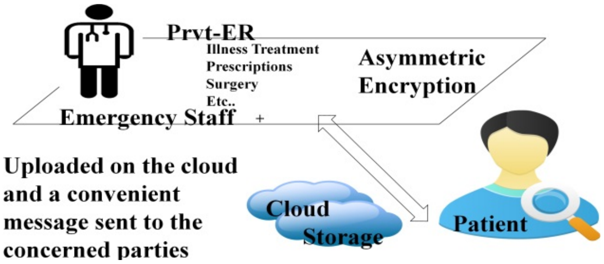


Fig. 11: Prvt-ER

desired image show the original image, its encrypted one as well as the time taken for encryption.

While on the other side, the second part of MATLAB GUI, as in Fig. 10, will be required to decrypt the encrypted image.

The MATLAB GUI will use the same security code required to decrypt the image, will show the encrypted image, its decrypted image as well as the time taken for the system to decrypt.

The AES Symmetric encryption takes a readable data, whether a plaintext or image, scrambles it and transfers it to unreadable, then transfers it again to readable when needed. It is generally fast. The most important thing to remember is that both sides-the patient and the hospital/doctor need access to the same key.

Prvt-ER parts of the EHR: The last part of the EHR, Prvt-ER, as in Fig. 11, uses Asymmetric encryption, uploaded to the cloud and a convenient message is sent to the concerned parties for pre-visit discussion as it is slow to decrypt.

The asymmetric encryption method (RSA) transfers the raw data also from readable to unreadable but with a twist of having 2 keys called public and private where the patient will have his private key stored in a private place for encrypting his data while having his public key known to all for decrypting. This same process was simulated using MATLAB RSA tools having images as well as text.

The objective of this study is to shed the light on a comprehensive structure for an innovative approach in dealing with patient, medical and health records. The idea is to incorporate the advantages of each of the aforementioned records' skeleton and curb the drawbacks of those existing platforms in the frame of a free, autonomous, versatile and omnipresent system that could be managed by patients and/or other "authorities". In few words, the main objective is to create a system that secures autonomy and non-maleficence in handling those records. The system relies on what we referred to as UBE or Usage-Based Encryption where three variants of FIPS standards are adopted to accomplish the acclaimed goals. Furthermore, a nifty modus operandi has been sketched to wittingly organize/command access control and revocation, specific privileges and security issues, at large. As a matter of fact, since those records are intended to be stored on cloud, our innovative approach knits all those loops of interest together by administering the upper hand in this structure to the patient with an advanced level of flexibility in customizing all pertinent and relevant aspects.

The outcomes are beyond satisfactory since the devised system allowed the patient to fully and successfully control his/her health records by choosing the ultimate scheme which is deemed as best fit for the third party that is meant to have access to it. It also allowed faultless yet smooth revocation of access when the patient deems it necessary to abolish the contact in question. Furthermore, the testing results demonstrated high level of security in terms of storage on cloud since the protocols are under the patient's full supervision and choice. In this sense, those principles applied in this case truly constitute a most general system that is ideal fit for health care applications at large. The relationships that interrelate all modi operandi adopted are indeed versatile since they can also be seen as a library where one could select the most appropriate organigram for the application in question under the umbrella of health care environment. Particularly and as a matter of fact, this approach could ultimately fit as an ideal solution for the management of health records in developing countries where governmental initiatives are extremely limited if not totally absent and where coping with the digital age requirements are still being significantly hindered by the infrastructure whether social, financial, or economic.

Moreover, the proposed scheme decisively offers significantly enhanced capabilities and features in contrast with most of the frequently used systems for a multitude of reasons and rationales. First and foremost, it is not frigid in terms of the tree of choices regarding the access control and type given to a third party involved in the sphere of the patient's medical and/or health records; the patient enjoys a flexible pattern out of which he/she can select and/or later modify the type of access to be granted. Second, the encryption algorithms used constitute an ideal basis to optimize space, computational time and practicality - the number of keys that is produced is reduced to the minimum required. Third, the system's structure allows to secure the data before sending it onto cloud which optimizes resources and prevent raw information from being intercepted by maleficent intruders or hackers - here also policies and protocols are monitored by the user and not left to cloud providers; all of this presented in a highly user-friendly graphical user interface with all options required to manage the entirety of the patient's records inclusive of all types such as lab-test results, images, diagnosis reports, prescriptions, medications, etc. Finally, yet importantly, the presented system indubitably establishes a comprehensive, powerful, secure, ubiquitous and versatile setting for the healthcare globe.

CONCLUSION

In this study, we proposed a Usage Based Encryption (UBE) approach that adapts leading standard encryption techniques with cryptographic hashing and digital signatures algorithms to different parts of a typical EHR. The innovative feature of the approach lies in categorizing information based on their usage rather than on advanced concepts which renders the management of the health record fathomable by the patient and most importantly allows for a significantly greater degree of maneuverability in terms of data segregation in the context of access control, encryption and revocation of privileges. Besides, the suggested structure does not rely on security measures provided and/or supplied by cloud providers, but allows a low-level granularity security policy to be implemented and managed by the patient-data is not left or sent raw or plain to cloud providers.

Furthermore, the suggested skeleton offers a versatile platform for the patient to specify and resourcefully reallocate the different parts of the health record via convenient choices of encryption/hashing algorithms. Finally, with the widespread of IaaS, SaaS and PaaS cloud providers and the digitization of almost the entirety of EHRs, the proposed solution allows the patient to safely preserve and easily share data in an efficient way while sustaining the EHR security goals: Confidentiality, Integrity and Availability (CIA).

REFERENCES

Akkar, M.L. and C. Giraud, 2001. An implementation of DES and AES, secure against some attacks. Proceeding of the International Workshop on Cryptographic Hardware and Embedded Systems. Springer-Verlag, Berlin, Heidelberg, New York, pp: 309-318.

Alanazi, H.O., A.A. Zaidan, B.B. Zaidan, M.L.M. Kiah and S.H. Al-Bakri, 2015. Meeting the security requirements of electronic medical records in the ERA of high-speed computing. J. Med. Syst., 39(1): 165.

Ali, M., S.U. Khan and A.V. Vasilakos, 2015. Security in cloud computing: Opportunities and challenges. Inform. Sciences, 305: 357-383.

Alshehri, S., S.P. Radziszowski and R.K. Raj, 2012. Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption. Proceeding of the IEEE 28th International Conference on Data Engineering Workshops (ICDEW), pp: 143-146.

Alyass, A., M. Turcotte and D. Meyre, 2015. From big data analysis to personalized medicine for all: Challenges and opportunities. BMC Med. Genomics, 8(1): 33.

Bahga, A. and V.K. Madisetti, 2013. A cloud-based approach for interoperable Electronic Health Records (EHRs). IEEE J. Biomed. Health Inform., 17(5): 894-906.

Ball, M.J. and J. Lillis, 2001. E-health: Transforming the physician/patient relationship. Int. J. Med. Inform., 61(1): 1-10.

Basu, S., A.H. Karp, J. Li, J. Pruyne, J. Rolia *et al*., 2012. Fusion: Managing healthcare records at cloud scale. Computer, 45(11): 42-49.

Bates, D.W., M. Cohen, L.L. Leape, J.M. Overhage, M.M. Shabot *et al*., 2001. Reducing the frequency of errors in medicine using information technology. J. Am. Med. Inform. Assoc., 8(4): 299-308.

Bogdanov, A., D. Khovratovich and C. Rechberger, 2011. Biclique cryptanalysis of the full AES. Proceeding of the International Conference on the Theory and Application of Cryptology and Information Security, pp: 344-371.

Bresó, A., C. Sáez, J. Vicente, F. Larrinaga, M. Robles and J.M. García-Gómez, 2015. Knowledge-based personal health system to empower outpatients of diabetes mellitus by means of P4 medicine. Methods Mol. Biol., 1246: 237-257.

Burnett, S. and S. Paine, 2001. The RSA Security's Official Guide to Cryptography. Osborne/McGraw-Hill, New York.

Cao, Y.Y. and C. Fu, 2008. An efficient implementation of RSA digital signature algorithm. Proceeding of the IEEE International Conference on Intelligent Computation Technology and Automation (ICICTA), 2: 100-103.

Collins, S.A., S. Bakken, D.K. Vawdrey, E. Coiera and L. Currie, 2011. Model development for EHR interdisciplinary information exchange of ICU common goals. Int. J. Med. Inform., 80(8): e141-e149.

Cramer, R. and V. Shoup, 1998. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. Proceeding of the Annual International Cryptology Conference, pp: 13-25.

Daemen, J. and V. Rijmen, 2002. The Design of Rijndael: AES--the Advanced Encryption Standard. Springer-Verlag, Berlin, Heidelberg, New York.

Deepika, K., N. Naveen Prasad, S. Balamurugan and S. Charanyaa, 2015. Evolution of cloud computing: A state-of-the-art survey. IJIRCCE, 3(1): 174-179.

Dolin, R.H., 1997. Outcome analysis: Considerations for an electronic health record. MD Comput. Comput. Med. Practice, 14(1): 50-56.

Eastlake, D. and P. Jones, 2001. RFC 3174, US Secure Hash Algorithm 1 (SHA1). Retrieved form: https://www.rfc-editor.org/info/rfc3174.

Flores, M., G. Glusman, K. Brogaard, N.D. Price and L. Hood, 2013. P4 medicine: How systems medicine will transform the healthcare sector and society. Per. Med., 10(6): 565-576.

Garets, D. and M. Davis, 2006. Electronic Medical Records vs. Electronic Health Records: Yes, there is a Difference. Policy White Paper, Chicago, HIMSS Analytics, pp: 1-14.

Gaubatz, G., J.P. Kaps and B. Sunar, 2004. Public key cryptography in sensor networks-revisited. Proceeding of the European Workshop on Security in Ad-Hoc and Sensor Networks, pp: 2-18.

Gilbert, H. and H. Handschuh, 2003. Security analysis of SHA-256 and sisters. Proceeding of the International Workshop on Selected Areas in Cryptography. Springer-Verlag, Berlin, Heidelberg, New York, NY., pp: 175-193.

Griebel, L., H.U. Prokosch, F. Köpcke, D. Toddenroth, J. Christoph, I. Leb, I. Engel and M. Sedlmayr, 2015. A scoping review of cloud computing in healthcare. BMC Med. Inform. Decis. Mak., 15(1): 17.

Grollmann, J. and A.L. Selman, 1988. Complexity measures for public-key cryptosystems. SIAM J. Comput., 17(2): 309-335.

Guo, L. and W.C. Yau, 2015. Efficient secure-channel free public key encryption with keyword search for EMRs in cloud storage. J. Med. Syst., 39(2): 11.

Hood, L. and S.H. Friend, 2011. Predictive, personalized, preventive, participatory (P4) cancer medicine. Nat. Rev. Clin. Oncol., 8(3): 184-187.

Hood, L. and M. Flores, 2012. A personal view on systems medicine and the emergence of proactive P4 medicine: Predictive, preventive, personalized and participatory. N. Biotechnol., 29(6): 613-624.

Iakovidis, I., 1998. Towards personal health record: Current situation, obstacles and trends in implementation of electronic healthcare record in Europe. Int. J. Med. Inform., 52(1-3): 105-115.

Jin, Z. and Y. Chen, 2015. Telemedicine in the cloud era: Prospects and challenges. IEEE Pervas. Comput., 14(1): 54-61.

Kluge, E.H.W., 2004. Informed consent and the security of the Electronic Health Record (EHR): Some policy considerations. Int. J. Med. Inform., 73(3): 229-234.

Liu, C., R. Ranjan, X. Zhang, C. Yang and J. Chen, 2015a. A Big Picture of Integrity Verification of Big Data in Cloud Computing. In: Khan, S. and A. Zomaya (Eds.), Handbook on Data Centers, Springer, New York, pp: 631-645.

Liu, J., E. Ahmed, M. Shiraz, A. Gani, R. Buyya and A. Qureshi, 2015b. Application partitioning algorithms in mobile cloud computing: Taxonomy, review and future directions. J. Netw. Comput. Appl., 48: 99-117.

Löhr, H., A.R. Sadeghi and M. Winandy, 2010. Securing the e-health cloud. Proceedings of the 1st ACM International Health Informatics Symposium (IHI '10), pp: 220-229.

McEvoy, R.P., F.M. Crowe, C.C. Murphy and W.P. Marnane, 2006. Optimisation of the SHA-2 family of hash functions on FPGAs. Proceeding of the IEEE Computer Society Annual Symposium on Emerging VLSI Technologies and Architectures (ISVLSI’06), pp: 317-322.

McLoone, M. and J.V. McCanny, 2001. Single-chip FPGA implementation of the advanced encryption standard algorithm. Proceeding of the International Conference on Field Programmable Logic and Applications. Springer-Verlag, Berlin, Heidelberg, New York, pp: 152-161.

Morton, M.E. and S. Wiedenbeck, 2009. A framework for predicting EHR adoption attitudes: A physician survey. Perspect. Health Inf. Manag., 6(Fall): 1a.

Nagaty, K.A., 2015. A Secured Hybrid Cloud Architecture for mHealth Care. In: Adibi, S. (Ed.), Mobile Health. Springer Series in Bio-/Neuroinformatics. Springer, Cham, 5: 541-588.

Narayan, S., M. Gagné and R. Safavi-Naini, 2010. Privacy preserving EHR system using attribute-based infrastructure. Proceeding of the 2010 ACM Workshop on Cloud Computing Security Workshop (CCSW '10), pp: 47-52.

Nechvatal, J., E. Barker, L. Bassham, W. Burr, M. Dworkin *et al*., 2001. Report on the development of the Advanced Encryption Standard (AES). J. Res. Natl. Inst. Stand. Technol., 106(3): 511-577.

Negi, A., P. Sharma, P. Chaudhary and H. Gupta, 2015. New method for obtaining digital signature certificate using proposed RSA algorithm. Int. J. Comput. Appl., 121(23).

Pack, A.I., 2016. Application of personalized, predictive, preventative, and participatory (P4) medicine to obstructive sleep apnea. A roadmap for improving care? Ann. Am. Thorac. Soc., 13(9): 1456-1467.

Papagounos, G. and B. Spyropoulos, 1999. The multifarious function of medical records: Ethical issues. Methods Inf. Med., 38(4-5): 317-320.

Pointcheval, D., 1999. New public key cryptosystems based on the dependent-RSA problems. Proceeding of the International Conference on the Theory and Applications of Cryptographic Techniques, Springer-Verlag, Berlin, Heidelberg, New York, NY., pp: 239-254.

Rijmen, V. and J. Daemen, 2001. Advanced encryption standard. Proceeding of Federal Information Processing Standards Publications, National Institute of Standards and Technology, pp: 19-22.

Sanchez-Avila, C. and R. Sanchez-Reillol, 2001. The Rijndael block cipher (AES proposal): A comparison with DES. Proceeding of the IEEE 35th International Carnahan Conference on Security Technology, pp: 229-234.

Shortliffe, E.H. and J.J. Cimino, 2013. Biomedical Informatics: Computer Applications in Healthcare and Biomedicine. Springer Science+Business Media, LLC, New York.

Sklavos, N. and O. Koufopavlou, 2003. On the hardware implementations of the SHA-2 (256, 384, 512) hash functions. Proceeding of the International Symposium on Circuits and Systems (ISCAS'03).

Somani, U., K. Lakhani and M. Mundra, 2010. Implementing digital signature with RSA encryption algorithm to enhance the data security of cloud in cloud computing. Proceeding of the 1st IEEE International Conference on Parallel Distributed and Grid Computing (PDGC), pp: 211-216.

Standard, F.I.P., 2001. Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication, 197: 1-51.

Thakur, J. and N. Kumar, 2011. DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. Int. J. Emerg. Technol. Adv. Eng., 1(2): 6-12.

Topol, E.J., 2015. The Patient Will See You Now: The Future of Medicine is in Your Hands. Basic Books, New York.

Wander, A.S., N. Gura, H. Eberle, V. Gupta and S.C. Shantz, 2005. Energy analysis of public-key cryptography for wireless sensor networks. Proceeding of the 3rd IEEE International Conference on Pervasive Computing and Communications (PerCom, 2005), pp: 324-328.

Wang, H., B. Sheng, C.C. Tan and Q. Li, 2008. Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control. Proceeding of the 28th International Conference on Distributed Computing Systems (ICDCS'08), pp: 11-18.

Xavier, N. and V. Chandrasekar, 2015. Cloud computing data security for personal health record by using attribute based encryption. Bus. Manage., 7(1).

Yang, J.J., J.Q. Li and Y. Niu, 2015. A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Gener. Comp. Sy., 43-44: 74-86.

Younesi, E. and M. Hofmann-Apitius, 2013. From integrative disease modeling to predictive, preventive, personalized and participatory (P4) medicine. EPMA J., 4(1): 23.

Zhang, R. and L. Liu, 2010. Security models and requirements for healthcare application clouds. Proceeding of the IEEE 3rd International Conference on Cloud Computing (CLOUD), pp: 268-275.

Zhang, X.M. and N. Zhang, 2011. An open, secure and flexible platform based on internet of things and cloud computing for ambient aiding living and telemedicine. Proceeding of the 2011 International Conference on Computer and Management (CAMAN), pp: 1-4.