This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2014.2300846, IEEE Journal of Biomedical and Health Informatics

A Review on the State-of-the-Art Privacy Preserving Approaches in the e-Health Clouds

Assad Abbas, Samee U. Khan, Senior *Member, IEEE*

***Abstract*—Cloud computing is emerging as a new computing paradigm in the healthcare sector besides other business domains. Large numbers of health organizations have started shifting the electronic health information to the cloud environment. Introducing the cloud services in the health sector not only facilitates the exchange of electronic medical records among the hospitals and clinics, but also enables the cloud to act as a medical record storage center. Moreover, shifting to the cloud environment relieves the healthcare organizations of the tedious tasks of infrastructure management and also minimizes development and maintenance costs. Nonetheless, storing the patient health data in the third-party servers also entails serious threats to data privacy. Because of probable disclosure of medical records stored and exchanged in the cloud, the patients' privacy concerns should essentially be considered when designing the security and privacy mechanisms. Various approaches have been used to preserve the privacy of the health information in the cloud environment. This survey aims to encompass the state-of-the-art privacy preserving approaches employed in the e-Health clouds. Moreover, the privacy preserving approaches are classified into cryptographic and non-cryptographic approaches and taxonomy of the approaches is also presented. Furthermore, the strengths and weaknesses of the presented approaches are reported and some open issues are highlighted.**

***Index Terms*—Privacy preserving, e-Health cloud, access control, security.**

I. Introduction

THE development of new technologies has deeply influenced the traditional healthcare practices. Since the last few decades, technology has seamlessly been integrated into our lives and has elevated the need for the development of socio-technical systems in the healthcare domain. There has been a lot of research in the electronic healthcare area with focus on utilizing the electronic patient records for patient monitoring and diagnosis. Provision of health services using digital technology has been termed as e-Health [1]. Moreover, traditional clinical settings with paper-based medical records and prescriptions have also advanced to the Personal Health Records (PHRs) and the Electronic Health Records (EHRs). The PHRs and EHRs, both are the electronic versions of patient health information. However, the PHRs are controlled by patients themselves [53]; whereas, the EHRs are managed by the healthcare providers [51]. The e-Health necessitates entire restructuring and digitalization of healthcare infrastructure, including production, supply, and management [5]. The new paradigm, for provision of ubiquitous health services at affordable prices, has been adopted by countries, such as USA [2], Canada [3], UK [4], Korea [5], and European Union [6-8].

Several healthcare providers and insurance companies today use one or the other form of electronic medical record systems. Usually, a patient may have many healthcare service providers, including primary care physicians, specialists, and therapists. In addition, a patient may register with several health insurance companies for different types of insurances, such as medical, dental, and vision [10]. Consequently, the electronic health record of a patient may exist at various locations in the healthcare community networks. From the clinical standpoint, it is important to access the up- to- date integrated patient health information [11]. However, sharing and integration of the EHRs, that are managed by several healthcare providers is slow and costly [10] and requires effective, secure, and low cost mechanisms to share electronic health records among several healthcare providers.

The requirements for storage and continuous availability of e-Health data necessitate the use of the cloud computing services [12]. Cloud computing is emerging as a promising paradigm for computing and is drawing the attention from both academia and industry [13]. The cloud computing model shifts the computing infrastructure to third-party service providers that manage the hardware and software resources with significant cost reductions [28], [31]. Cloud computing has shown great potential to enhance collaboration among different healthcare organizations and to fulfill the common requirements, such as scale, agility, cost effectiveness, and availability [11].Moreover, migration of patient health records to the cloud storage relieves the healthcare providers from the infrastructure management tasks [14], [15]. Although there is no standard definition of the e-Health cloud, it can be considered as a platform that, besides storing gigantic volumes of the health data, also serves as a structured management of the health data across multiple healthcare providers. The health data can further be extracted from different databases for treatments and other analytical purposes [52]. Typically, the cloud consists of layered elements, such as physical storage, service infrastructure, application, and communication infrastructure. Moreover, the e-Health cloud infrastructure may be: **(a)** implemented internally by the healthcare provider (private), **(b)** maintained by some external party (public), **(c)** or is maintained by the healthcare provider and external party together (hybrid) [9]. Ref. [52] uses a private cloud, whereas [47] and [56] use public and hybrid clouds, respectively.

Manuscript received February 14, 2013.
A. Abbas and S. U. Khan are with the Department of Electrical and Computer Engineering, North Dakota State University, Fargo, ND 58108, USA. (E-mail: assad.abbas@my.ndsu.edu, samee.khan@ndsu.edu).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2014.2300846, IEEE Journal of Biomedical and Health Informatics

Nevertheless, automated PHRs are exposed to possible abuse and require security measures based on the identity management, access control, policy integration, and compliance management [16]-[19], [22]. In [20], it is claimed that storing huge volumes of patients' sensitive medical data in third-party cloud storage is susceptible to loss, leakage, or theft. Moreover, traditional network security mechanisms are also not sufficient for the data outsourced for storage [49]. Therefore, confidentiality and integrity of the stored health data is deemed as one of the major challenges elevated by the external storages. Ref. [78] articulates that using cryptographic storage significantly enhances security of the data. Particularly, in the public cloud environment operated by the commercial service providers and shared by several other customers, data privacy and security is the most anticipated requirement.

Various mechanisms have been developed to preserve and enhance privacy of the e-Health systems in the cloud environment. We present an overview of the most common privacy preserving approaches that have been used in the e-Health clouds in particular. To the best of our knowledge, there is no comprehensive survey available focusing solely on privacy issues of the e-Health cloud. Xiao *et al*. [21] and Takabi *et al.* [17] provide an overview of the existing security and privacy issues in the cloud environment with the contemporary privacy measures. Ahuja *et al.* [12] discussed about the current research and trends in the e-Health cloud with a minimal focus on privacy issues. Ref. [81] analyzes properties of the existing PHRs and identifies the particular privacy risks. No thorough discussion on the privacy preserving approaches pertaining to the e-Health cloud is presented. Ref. [82] introduces the cloud architecture for bio-medical applications with discussion on the security and privacy issues. However, Ref. [9] and Ref. [23] have discussed some privacy preserving efforts particular to the e-Health clouds. We present taxonomy of the approaches that have been used to preserve the health data privacy in the cloud. Besides the discussion on the privacy preserving approaches, the survey also highlights the strengths and weaknesses of the presented approaches. Moreover, we discuss the privacy preserving requirements and report what types of requirements are fulfilled by each of the presented approaches and also highlight some open research issues. The rest of the paper is organized as follows. Section II discusses the need and requirements of privacy in the e-Health cloud with the discussion on threat models. The privacy preserving approaches used in the cloud based health systems are presented in Section III. Section IV presents comparison of the presented approaches and Section V concludes the discussion and highlights the open research issues and areas.

II. The need and requirements for privacy in the e-Health cloud

Recent trends in the healthcare, centering on accessing the information anytime and anywhere, encourage moving the healthcare information towards the cloud. Despite the fact that the cloud offers several benefits, it also entails special threats to the health data in terms of privacy and security [24]. The concept of privacy preserving is considerably more than merely maintaining the confidentiality of data. Metri *et al*. [27] argue that threats to the data privacy in the cloud include spoofing identity, tampering with the data, repudiation, and information disclosure. In spoofing identity attack, the attacker pretends to be a valid user whereas data tampering involves malicious alterations and modification of the content. Repudiation threats are concerned with the users who deny after performing an activity with the data. Information disclosure is the exposure of information to the entities having no right to access information [27]. The same threats prevail for the health data stored and transmitted on the third-party cloud servers. Essentially, the cloud service providers should completely recognize as well as deal with the security concerns in the cloud to enhance the trust level of the patients and healthcare organizations [25]. In the United States for example, use and disclosure of the Protected Health Information (PHI) should be in accordance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA). The HIPAA requires that maintaining the confidentiality of the health data is not an option, but an obligation [26].

Typical entities in a cloud based health record system are patients, hospital staff, such as doctors, nurses, pharmacies, and laboratory staff, insurance companies, and the cloud service providers. Due to the distributed architecture of the cloud, the patient EHRs are stored at and shared among many third-party providers. Therefore, the data is susceptible to unauthorized access and attacks. Various approaches being used to maintain privacy of the e-Health cloud are based on particular adversarial models. One model assumes the cloud servers as untrusted entities that could possibly disclose the sensitive health information. Moreover, such untrusted cloud servers are vulnerable to threats from the internal and external adversaries. The adversaries may not only attempt to access the encrypted health data through forged credentials but also can gain access to the health data as privileged users. In the second model, threats to the health data stored in the trusted cloud servers can be from the inside adversaries. For instance, parts of the data may be saved by a doctor who could subsequently share the data with unauthorized entities, thereby causing the information disclosure [45]. Moreover, identities of the entities must be kept anonymous and flows of the health data from different sources in the cloud must be intricate enough to infer the linkablity among them. In the third model, the cloud servers are semi-trusted. The semi-trusted cloud servers are usually considered as honest, however, they are curious to obtain as much information about the health data as possible and may collude with some malicious users [14]. In such situations, the adversaries may not only tamper the patient health data but can also share or sell the health information to the unauthorized parties. For example, the medicine prescribed by a doctor may be revealed to the representatives of the pharmaceutical company [24] or the expense information pertaining to the insurance company may be tampered. Therefore, the health data privacy preserving in the cloud has multiple requirements to be fulfilled. The requirements include integrity, confidentiality, authenticity, accountability, audit,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2014.2300846, IEEE Journal of Biomedical and Health Informatics

non-repudiation, anonymity, and unlinkability [9], [70]. Each of the aforementioned requirements is briefly defined blow in context of the e-Health systems.

(a) Integrity – to ensure that the health data captured by a system or provided to any entity is true representation of the intended information and has not been modified in any way [21].

(b) Confidentiality – to ensure that the health data of patients is kept completely undisclosed to the unauthorized entities.

(c) Authenticity– ensures that the entity requesting access is authentic. In the healthcare systems, the information provided by the healthcare providers and the identities of the entities using such information must be verified.

(d) Accountability – an obligation to be responsible in light of the agreed upon expectations. The patients or the entities nominated by the patients should monitor the use of their health information whenever that is accessed at hospitals, pharmacies, insurance companies etc.

(e) Audit –to ensure that all the healthcare data is secure and all the data access activities in the e-Health cloud are being monitored.

(f) Non-Repudiation – repudiation threats are concerned with the users who deny after performing an activity with the data. For instance, in the healthcare scenario neither the patients nor the doctors can deny after misappropriating the health data.

(g) Anonymity – refers to the state where a particular subject cannot be identified. For instance, identities of the patients can be made anonymous when they store their health data on the cloud so that the cloud servers could not learn about the identity.

(h) Unlinkability – refers to the use of resources or items of interest multiple times by a user without other users or subjects being able to interlink the usage of these resources [30]. More specifically, the information obtained from different flows of the health data should not be sufficient to establish linkability by the unauthorized entities.

III. Privacy Preserving Approaches in the e-Health Clouds

Numerous approaches have been proposed to preserve the privacy of the patient health data. However, there is no clear classification of the privacy preserving approaches. Therefore, we classify the privacy preserving approaches used in the e-Health clouds into: **(a)** cryptographic and **(b)** non-cryptographic approaches at top level. The cryptographic approaches to mitigate the privacy risks utilize certain encryption schemes and cryptographic primitives. Conversely, non-cryptographic approaches mainly use policy based authorization infrastructure that allows the data objects to have access control policies. Cryptographic and non-cryptographic privacy preserving approaches are presented in Section *A* and Section *B*.

A. Cryptographic approaches

The cryptographic approaches commonly used in the e-Health cloud based systems to protect data use encryption schemes, such as Public Key Encryption (PKE) and Symmetric Key Encryption (SKE). However, there are some other cryptographic primitives that are also used to preserve privacy of the health data. These primitives include: **(a)** searchable encryption, **(b)** (Hierarchical) Identity-Based Encryption (HIBE), **(c)** Proxy Re-encryption (PRE), **(d)** Predicate/Hierarchical Predicate Encryption (HPE), and **(e)** (Fully) homomorphic encryption. In this section, we briefly define and present the approaches based on the PKE, SKE, and several cryptographic primitives that are used to preserve the privacy of the e-Health cloud. Fig. 1 presents taxonomy of the privacy preserving approaches.

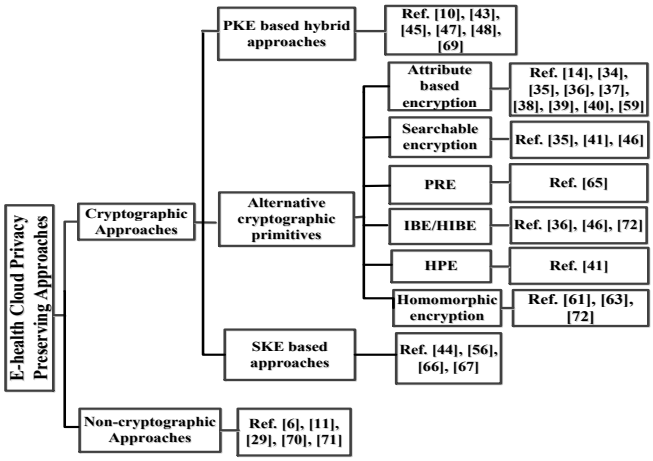

Fig. 1: Taxonomy of the privacy preserving approaches in the e-Health cloud

1) Public Key Encryption (PKE) based hybrid approaches

The PKE technique requires two separate keys; one of the keys is private whereas the other is public. Solutions based on the PKE are secure but using the PKE alone seems computationally less efficient due to the slower operations and the larger key sizes. Therefore, the PKE is used in combination with the SKE where symmetric keys are used to encrypt the contents while public/private keys are used to secure the symmetric keys. Consequently, in this section we term the approaches that use the PKE in conjunction with symmetric cryptographic technique as hybrid approaches. The common public key algorithms use the RSA and Elliptic Curve Cryptography (ECC) techniques for generating public/private parameters used for security services. For instance, the RSA-OAEP [89] and ECIES [90] are based on the RSA and ECC, respectively. The PKE based hybrid approaches to protect the health data in the cloud are presented below.

The authors in [10] presented a reference model for preserving privacy of the healthcare applications in the untrusted cloud. The authors emphasized on a patient centric, role based EHR model that allows the users to maintain anonymity. The model uses an anonymous signature scheme called group signatures [93] for authenticity and integrity of the EHRs. The group signature scheme allows a group member to anonymously sign a message on behalf of all the group members. Moreover, the authors suggested maintaining the logs of all the accesses and modifications to the EHRs.

Jafari *et al.* [43] presented a model to allow such a patient-centric control over the EHRs that restricts the patients

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2014.2300846, IEEE Journal of Biomedical and Health Informatics

to modify the contents authored by other parties, such as doctors and lab staff. The authors used the Digital Rights Management (DRM) based approach for secure management of the health records in the cloud. In the DRM approach, the data is always stored in encrypted form and the license is issued by the owner, whereas the policies expressed in the license are enforced by the agent. The Content Key Encryption (CKE) is used in DRM systems to control the electronic content, and more precisely the CKE relates to a DRM system that employs the user based CKE [42]. The data is encrypted using a content key and only the users having valid license are allowed to decrypt and use the content. The health record service provider acts as the distributor by providing the protected content only to the authorized users. However, the provider cannot access the contents in clear text form. Patients and physicians are assigned the public and the private keys for encryption and decryption.

Mashima *et al.* [45] proposed system architecture and related protocols that enable either explicit or implicit patient control over the heath information. The access control mechanism focuses on when and how the patient health information is accessed. The authors presented the notion of "accountable usage" and the updated health records to enable robust patient centric monitoring. The records are encrypted through the PKE with corresponding hash values. Moreover, to ensure the usage of record by only trusted entities, the concept of Universal Designated Verifier Signatures (UDVS) is introduced. The UDVS function as standard digital signatures that are publicly verifiable. The signatures have additional capability of designating the signature to any designated verifier [50]. However, the proposed scheme exhibits drawback in assuming that the health data is first created by record issuers that have knowledge about the contents of records, hash values, and signatures. If such information is disclosed, then the monitoring system would not be able to effectively manage the access control.

Kaletsch *et al*. [47] proposed a framework called Online Referral and Appointment Planer (ORAP) to support secure exchange of the EHRs from general health practitioners to specialist doctors. In the ORAP security model, the EHRs are only stored at the physicians' practice places, that are considered as the only trusted environment. The EHRs are encrypted and signed before transmission to the central cloud storage and can be decrypted by the receiving specialists only. The ORAP uses German Healthcare Telematics Infrastructure (HTI) components to provide the secure encryption and signatures for all documents transferred particular to the patients' health. The framework uses Amazon's S3 Cloud for temporary storage of large scaled attachments that are obviously considered as encrypted. However, the ORAP lacks in integration of patient centric functions that makes it less flexible in providing role based access.

A solution to address the security issues particular to the end-user platforms and external storage is presented in [48]. The presented architecture consists of Trusted Virtual Domains (TVD) to establish the access control. The TVDs are combinations of different virtual machines that trust on each other and have common security policies. The TVD platforms contain the security kernel and other physical components that virtual machines may utilize to enforce the policies [68]. A major advantage of using the TVD approach is its flexibility of integration with the legacy systems. In the proposed approach, the data that needs to be transmitted and stored on the external storages is automatically encrypted through the PKE. When a client machine wants to connect with the TVD, the underlying infrastructure authenticates the integrity of the client platform. However, deploying the TVD based solutions may result in increased complexity and scalability issues in the situations where the security domains are implemented on each client machine.

Pecarina *et al.* [69] presented the PKE based architecture to ensure enhanced control through anonymity and unlinkability in a semi-trusted health cloud. The approach introduces the anonymity boundaries between the Cloud Service Provider (CSP) and the users to ensure the selective anonymity of the PHRs while submitting the health records to the cloud. Patients encrypt their PHRs using the public key of the CSP before storing at the cloud. The CSP decrypts the records using the private key, stores the PHR and location, and encrypts them through the SKE. Pairing the patients' master key and the encrypted location permits the CSP to preserve the administrative control on the cloud storage.

2) Approaches based on Symmetric Key Encryption (SKE)

The SKE uses the same keys for encryption and decryption. The SKE based schemes are effective in securing the data but introduce additional complexity in the EHR systems as they may require additional procedures to implement the access control [40]. The SKE based algorithm currently in use and acting as standard is the Advanced Encryption Standard (AES). The AES was recommended as a standard by the National Institute of Standards and Technology (NIST) after the limitations of the Data Encryption Standard (DES) were exposed [91]. Moreover, there are also some commonly used stream ciphers, such as RC4and A5/1. The SKE based approaches to protect the health data in the cloud are presented below.

A mechanism for unlinkability between the patients and electronic medical records in the cloud environment is presented by Li *et al.* [44]. The patients' electronic medical records are encrypted through the SKE and are stored in an anonymous way. The doctors use digital signatures to process the patient health records after the treatment for storage at the cloud. The Electronic Medical Record number (PID), identity seed stored inside the Patients' Health Card (SID), a random value (R), and a serial number for treatment (SN) are required to access the patients' electronic medical record. Moreover, to access the heath data, a smart card is required that contains the SID. Furthermore, the PID is stored in two parts separately that restricts the illegitimate access over the patient data.

Chen *et al.* [56] used the SKE to encrypt the patient health data file in normal and emergency situations. The approach ensures data privacy in a hybrid cloud for sharing the EHRs. The patients' health data is stored on the hospital's private

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2014.2300846, IEEE Journal of Biomedical and Health Informatics

cloud as well as on the public cloud of the healthcare provider. The patients' medical records can only be decrypted through the private content key that is split randomly and stored in two different parts. One of the keys is escrowed at the hospital server while the other is stored at the smart card owned by the patient. Therefore, only the authorized users can have access to the patient EHRs.

A dynamic access structure to enforce precise access control over the PHRs in multiuser cloud environment is introduced by Chen *et al*. [66]. The health records are encrypted and decrypted through Lagrange multipliers using the SKE. The approach allows the data owners to generate and share the keys. An important feature of the approach is automatic revocation of the users. However, the task is costly in terms of computations. The complexities of key management to grant access dynamically over the PHRs are reduced by managing a partial order relationship among the users.

A role based and time based access control approach is introduced by Zhang *et al.* [67]. The approach is effective in storing the encrypted EHRs on the untrusted clouds and solves the issues of key distribution among the legitimate users. The approach applies time bound hierarchical key management that allows the legitimate users to access the EHRs for a specific period of time, based on their access roles. For time bound hierarchical key management, interested readers are referred to [83].The EHRs are encrypted through the SKE. However, the approach is limited in the sense that it requires a user to work in multiple roles. Consequently, the users have to possess and manage multiple keys.

3) Approaches based on Alternative Cryptographic Primitives

In this section, we present the privacy preserving approaches based on cryptographic primitives mentioned earlier.

a) Attribute-Based Encryption (ABE) approaches

Attribute-Based Encryption (ABE) –introduced by Sahai *et al.* [32], the ABE is a cryptographic primitive based on the PKE where the messages can be encrypted and decrypted on the basis of user attributes. A ciphertext can be decrypted only when the attributes and the decryption keys are available. The ABE enables the users to selectively share the encrypted data and also provides a fine-grained access [33]. Usually, the attribute based approaches are considered as costly in terms of decryption because of bilinear computation steps [72]. The variants of the ABE are briefly presented below.

Ciphertext Policy Attribute Based Encryption (CP-ABE) – first introduced in [80], a message in the CP-ABE is encrypted under an access policy that defines the access structure, whereas the users' private keys are associated with a set of attributes. Later, Zhou and Huang [54] in their construction reduced the size of ciphertext from the linear to a constant size. However, the CP-ABE is limited in terms of specifying the access policies and management of the user attributes.

Key Policy Attribute Based Encryption (KP-ABE) – in contrast to the CP-ABE, the access policies in the KP-ABE are associated with the private key whereas a set of descriptive attributes is used to label the ciphertext [33]. A user can decrypt the ciphertext only if the data attributes satisfy the defined access structure. However, the KP-ABE is limited in allowing the encryptor to decide about the decryptor of the data.

Multi-Authority Attribute Based Encryption (MA-ABE) – allows the users' keys to be collectively generated by multiple trusted authorities that are responsible for governing the subsets of the users' attributes. The user obtains a part of the secret key from each trusted authority, thereby preventing collusion [55]. For situations that require access rights based on identities, the ABE is considered as an inefficient technique.

Broadcast ciphertext-policy Attribute Based Encryption (bABE) – is effective in direct revocation of the user keys without the need of refreshing system parameters or data re-encryption. Although, the bABE ensures the health data confidentiality, it causes increased computational overheads in enforcing the access policies.

Some of the privacy preserving approaches based on the ABE and its variations, used in the e-Health cloud systems are presented below. Table I presents the attributes that are used to specify the access policies.

The issues of concurrently achieving the fine-grained access, scalability, and confidentiality of the outsourced data are addressed by Yu *et al.* [14]. The data encrypted by a single owner is subsequently shared with multiple users by distributing the keys. To enable data owner to delegate the computational tasks to the untrusted cloud servers, the access policies based on the attributes are enforced. The approach ensures the accountability of the users' secret keys. In the proposed approach the tasks of re-encrypting the data files and updating of the secrete keys are delegated to the cloud servers. To deal with the heavy computation overheads caused by re-encryption of data files and update of secret key, the KP-ABE, PRE, and lazy re-encryption are combined. The purpose of lazy re-encryption is to restrict the revoked users from learning the updated contents and keys if the file contents have been modified after user revocation.

TABLE I
ATTRIBUTES IN ATTRIBUTE-BASED ENCRYPTION APPROACHES

Work	Attributes in Attribute-Based Encryption
[35]	Type identifier : (patient, doctor, pharmacy) Attributes encrypted: patient's attributes not specified Role attributes: name, id, location, specialization
[34]	Not Specified
[36]	Location, gender, medication details, date of birth, social identification number, health record number
[38]	Role attributes: physician Data attributes: basic profile, history, allergies, and prescriptions
[14]	Attributes: illness, hospital, race
[39]	Not specified
[40]	Not specified
[59]	Record type, patient age
[37]	Not specified

Thomas *et al.* [34] proposed an ABE based architecture to preserve the confidentiality of the EHRs. The authors used the ABE and the PKE for scalable authorization secrets. The patient's smart card and PIN are used for authorization and authentication using the PKE. The patient is provided with a Transaction Access Code (TAC) that may be sent to physician

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2014.2300846, IEEE Journal of Biomedical and Health Informatics

via telephone or through any other remote mechanism. The physician in turn creates an EHR and once the TAC is verified, the EHR is encrypted and sent to the storage provider. The decryption operation requires the health professional to obtain the TAC and acquire authentication from the Private Key Generator (PKG). Ruj *et al.* [37] also proposed an ABE based access control mechanism to maintain anonymity of the users storing the PHRs on the cloud. Although, the identity of the entities storing the data is hidden, their credentials are verified. The approach is resistant to replay attacks and accomplishes the distribution of the keys in a decentralized fashion.

An attribute based infrastructure for the EHRs where the patients encrypt their EHR files using the bABE is presented by Nararyan *et al.* [35]. The bABE effectively makes plaintext accessible to the users satisfying the policies attached to the ciphertext, with an additional functionality of user revocation. The approach solves the key management issues by using the users' attributes for data encryption thereby, allowing every user to have only one private key for their attribute set for decryption. The approach also allows users to carry out private searches for the corresponding keywords over the encrypted data without revealing the keywords or partial matches to the cloud system. Moreover, the system permits the healthcare providers to perform keyword based searches on the patients' records. The keyword search functionality is provided by combining the bABE and the Public-Key Encryption with Keyword Search (PEKS) approach originally presented by Boneh *et al.* [85].

Li *et al.* [38] used the ABE to manage the access control over the health data in multi-owner, multi-authority, and multi-user cloud environment. The patients are capable of setting their own preferences, generating the decryption keys using the MA-ABE, and subsequently distributing the keys to the authorized users. Moreover, the attributes are managed in distributed fashion by each authority. To minimize the complexity of key distribution, the system has been divided into multiple security domains and each domain is responsible for managing only a limited set of users. The proposed scheme is claimed to be flexible in supporting efficient and on-demand revocation of the user access rights. Nevertheless, the proposed approach suffers from excessive computational overhead at the data owner side. Li *et al.* [39] extended the work presented in [38] and proposed another framework for secure sharing of the PHRs in multi-owner environment that divides the PHRs into different sub-domains. The use of the MA-ABE is extended to the public domains. The approach minimizes the intricacies and costs of key management for users and data owners while augmenting the privacy guarantees. To encrypt the patient health record, the ABE is used. Moreover, the approach presented in [38] is improved in terms of efficient management and on-demand user/attribute revocation. Although the approach enhances the scalability of the system, it is unable to efficiently handle the situations where data access rights are granted based on the users' identities instead of the attributes. Another MA-ABE based framework to offer patient centric access over the PHRs is presented in [77]. The framework assumes multiple owners of the PHRs and divides the entire system into different security domains and personal domains.

An approach called Efficient and Secure Patient-centric Access Control Scheme (ESPAC) for the cloud storage using the CP-ABE is presented by Barua et al. [36]. The scheme permits access to the health data based on access privileges. The ESPAC uses the IBE for secure transmission of the data between the remote patient and the e-Health cloud provider; whereas, the access control is realized by using the CP-ABE. The performance results show that the ESPAC scheme is applicable to resist the DOS attacks in a dual server mode. However, lack of dynamicity and flexibility in patient data attainment and then transmitting to the hospital servers makes this approach inefficient. Suhair *et al.* [40] also used the CP-ABE to encrypt the EHRs based on the healthcare providers' attributes or credentials in a multi-owner cloud setting. The healthcare providers share one public key for the EHR encryption and consequently, avoid the distribution and management overheads of the public keys. Akinyele *et al.* [59] also proposed a flexible approach using the ABE to offer a secure encryption of the electronic health data when it is being transferred to the storage outside the trust boundaries of the healthcare organization. The approach allows generation of the self-protected electronic medical records that can be stored at the cloud servers as well as cell phones to ensure availability when the provider is offline. A policy engine generates the access policies over the medical record(s) according to the user types (physician, patient, and insurance agent). Moreover, the policy engine identifies a set of attributes, such as record type, patient age, and date to encrypt the records using the CP-ABE. Likewise, the CP-ABE has also been used in [55], [73], [74], [75], and [76] for secure storage and exchange of the PHRs on the cloud.

b) Approaches based on miscellaneous cryptographic primitives

In this section, we present the privacy preserving approaches based on the cryptographic primitives other than the ABE.

Searchable Encryption – is an important cryptographic primitive that permits to perform search operations over the encrypted data without revealing the information about the contents and the user query to the untrusted servers [60]. The first practical approach using searchable encryption based on symmetric key cryptography was introduced in [60], whereas the authors in [85] were the first to introduce the public key searchable encryption. However, the searchable encryption techniques suffer from issues of functional usability and computational inefficiencies. The approaches presented in [35], [41], and [46] allow searching over the encrypted EHRs.

Predicate Encryption and Hierarchical Predicate Encryption (HPE) –Predicate encryption is a PKE based paradigm used to offer fine-grained access control over the encrypted data. In predicate encryption, the secret keys correspond to the predicates and these secret keys are used to decrypt the ciphertext associated with the attributes corresponding to the predicate [84]. The HPE is a cryptographic primitive that facilitates the delegation of the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2014.2300846, IEEE Journal of Biomedical and Health Informatics

search capabilities. However, the delegated users have more restrictive capabilities as compared to the delegating user [41], [57]. The HPE based schemes can be used to realize the searchable encryption.

Identity Based Encryption– Shamir [88] first introduced the notion of identity based cryptography. However, a fully functional Identity Based Encryption (IBE) scheme was introduced by Boneh and Franklin [64]. The IBE uses any string for instance, a name or an email address as the public key and the corresponding decryption keys are issued by a trusted party. A variant of the IBE called the Hierarchical IBE (HIBE) allows multiple PKGs arranged in a hierarchical form to easily handle the task of private key generation [87]. An HIBE approach to protect the EHRs is presented in [46].

Proxy-re encryption (PRE) –is a cryptographic primitive that allows a semi-trusted proxy to convert theciphertext encrypted under the public key of one user into a ciphertext that can be decrypted through the other user's private key [58].

(Fully)Homomorphic Encryption (FHE) – homomorphic encryption is a particular type of encryption that permits computations on ciphertexts and also results are obtained in encrypted form. The concept of FHE presented by Gentry [86] allows evaluating arbitrary number of additions and multiplications over the encrypted data without being able to decrypt. Another homomorphic scheme called "Somewhat Homomorphic Encryption (SwHE)" performs limited numbers of homomorphic operations by evaluating circuits of some specified depth. The FHE based solutions seem less practical because of their inefficiency. However, Lauter *et al*. [63] argue that the SwHE in some scenarios, such as medical and financial has proved really practical.

Li *et al.* [41] addressed the issues associated with Authorized Private Keyword Searches (APKS) on the encrypted EHRs in the cloud environment under the authorization of local trusted authorities. The threat model assumes that the cloud server is honest but curious to learn the data contents by honestly following the protocol. The authors proposed solution for the APKS based on the cryptographic primitive called the HPE. Besides documents and query privacy, the proposed scheme supports 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.

Benaloh *et al.* [46] presented a Patient Controlled Encryption (PCE) based electronic medical record system that allows patients to generate and share the encryption keys for delegation of the access rights. The EHRs are partitioned in a hierarchical structure using the HIBE. Each section of the structure is encrypted with a public key that is managed by the patients. The authors used the PKE to store the data in encrypted form over third-party storage. The decryption operation requires a sub-key that is derived from a master private key. The decryption keys are distributed by the patients to grants access over certain parts of the medical record. Moreover, the approach provides an efficient mechanism for searchability of the encrypted data.

Leng *et al.* [65] proposed an approach that allows the owner of the PHRs to delineate the access control through sticky policies before uploading the PHRs on the cloud. The sticky policies are employed to regulate the access and usage of data and accompany the data. The entities satisfying the access requirements specified in the sticky policies are allowed to access the data. The approach uses a cryptographic primitive called Conditional Proxy Re-encryption (C-PRE) to enforce the fine-grained access over the PHRs. In the C-PRE as compared to the PRE, the delegator categorizes plaintexts into portions and also the permissions to decrypt each portion are delegated through a proxy under the same pair of keys. The approach assumes the presence of multiple trusted authorities in the PHR system. The trusted authorities ensure the enforcement of the sticky policies besides authorizing the users to get the decryption keys for read and write operations. A more practical construction based on the PRE is presented in [92].

Lin *et al.* [72] presented a cloud assisted privacy preserving mobile health monitoring system to preserve privacy of the clients and the mobile health (mHealth) service providers. The adversarial model assumes the honest but curious server. The approach deals with the insiders who commit deliberate or non-intentional attacks to obtain information. The privacy of clients is protected using identity based encryption. Moreover, the approach uses homomorphic encryption while transferring the data from the mobile health provider to the cloud. The homomorphic encryption is effective in performing the meaningful computations over the encrypted data [63]. The decryption complexities of the client or the health provider are alleviated by using the outsourcing decryption technique [62] and the key privacy proxy re-encryption, without compromising on the privacy of the involved parties. Ref. [61] introduced a multiparty computational approach using the homomorphic encryption to process the encrypted ECG signals while preserving the patients' privacy. Lauter *et al.* [63] also applied SwHE to enable the cloud to perform computations over the encrypted patient data on patients' behalf.

B. Non-cryptographic approaches

Quite a few non-cryptographic approaches have been proposed to preserve privacy of the health data in the cloud. The non-cryptographic approaches mainly use certain policy based authorization infrastructure that allows the data objects to have access control policies. Some of the aforementioned systems also use few cryptographic primitives, such as hash functions and digital signature verification. Below, we present the systems that use the non-cryptographic approaches for preserving privacy in the e-Health cloud.

Fan *et al.* [6] developed the Data Capture and Auto Identification Reference (DACAR) platform to deal with the issues of security, integrity, confidentiality, and integration of various health services. The DACAR makes use of the private cloud for data storage and the hybrid cloud for hosting the services. To integrate different health services, the DACAR uses Service Oriented Architecture (SoA). The DACAR architecture consists of three layers. The bottom layer deals with security and confidentiality mechanism. The Single Point

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JBHI.2014.2300846, IEEE Journal of Biomedical and Health Informatics

of Contact (SPoC) is the middle layer used to fulfill the authorization requirements. The top layer has data buckets, ID mapping, and audit trial services. The database level encryption, digital signature verification, hashing, and integrity check-sum are applied on the DACAR platform to grant the access to the trustworthy individuals, roles, and application services.

Wu *et al.* [11] proposed broker-based authorization approach for selective sharing of the composite EHRs from the multiple healthcare service providers. The approach introduces an EHR aggregator for retrieval and aggregation of the distributed EHRs among multiple clouds to construct the virtual composite EHRs. Moreover, a policy manger supports the specification and enforces the access control policies. Based on the composite EHR schema, the EHR instances from different healthcare domains can be integrated. However, the access control policy infrastructure may come across the policy composition issues in case of multiple healthcare providers.

Chadwick *et al.* [29] presented an approach where patients' privacy policies are stuck with the data indicating who could have access to the data. The authors introduced a master policy decision point to support multiple sub-ordinate policy decision points. The cloud application developers use the Application Independent Policy Enforcement Point (AIPEP) to call the authorization services. The AIPEP accepts web service requests from applications and formulates web service decision responses to the application. The authorization infrastructure inquires whether the users have read permissions. If the infrastructure is unable to support a sticky policy, then the sender of the query is informed about the fact as well. The validation tests of infrastructure were conducted by running the authorization services on a small cloud server. Nonetheless, the proposed policy based infrastructure does not obviate the need for trust as the cloud data is still susceptible to disclosure threats by the cloud service providers.

Haas *et al.* [70] presented an approach that not only allows the patients to audit the access over the EHRs but also enables them to identify the sources of data leak. A policy based access structure is introduced that prevents the linking of different data sets for a single patient. The data before writing to the external storage is passed to a pseudonymity service that ensures the anonymity of the data. The data is further encrypted with a unique key before storage on a third-party server. By tracing the data flows the approach ensures the auditing of the health data.

A cloud based PHR system called MyPHRMachines that allows patients build their personal health data repository is presented in [71]. After upload the PHRs on MyPHRMachine, the patient can access the PHRs through Virtual Machine (VM) to delegate the access rights selectively to individual caregivers (general physician, hospital, and insurance companies).The caregivers are provided access to VMs through a ciphered VM identifier via email. The patients can monitor the PHRs through the remote desktop protocol and shutdown the VM session if they realize a misuse of PHR data. All of the communication is protected using the SSH protocol that besides others, effectively counters the Man-In-The-Middle attacks.

IV. Comparison of the Privacy Preserving Approaches

A detailed comparison of the presented approaches in terms of the privacy requirements is provided in Table II. As can be observed that majority of the presented techniques fulfill the privacy preserving requirements, such as integrity, confidentiality, authenticity, accountability, and audit. However, the requirements, such as non-repudiation, anonymity, and unlinkability are met by only a few techniques. There appears an important relationship between the anonymity and unlinkability and most of the presented approaches maintain unlinkability through anonymity. Another important observation is particular to the ABE based approaches. The ABE approaches may propagate the keys to the unwanted users having attributes similar to the legitimate users. Nonetheless, the ABE approaches have been quite effectively utilized to achieve a desired level of privacy. We also observe that most of the presented cryptographic techniques have successfully been able to minimize the key management overheads despite of their inherent complexities. For instance, the public key encryption is considered as less efficient in terms of computation whereas the ABE has a standing of costly decryption primitive because of bilinear computations. However, the presented schemes in this survey based on the aforementioned cryptographic schemes sufficiently minimized the key management overhead. The non-cryptographic approaches can never be truly secure in public clouds because they are susceptible to information disclosure by some insiders or the other hackers. However, non-cryptographic approaches when used only in private clouds preserve the privacy to a desired level because the infrastructure in such cases is trusted. Therefore, for systems operating in public or hybrid clouds, using reasonably strong cryptography is highly important.

In Table II, "✓" and "✗"symbols represent whether a particular privacy preserving requirement is fulfilled or not, respectively whereas "-" represents that a particular requirement is not discussed. Moreover, in Table II, due to space limitations, the privacy preserving requirements are abbreviated as follows:

Integrity: IN, Confidentiality: CO, Authenticity: AU, Accountability: AC, Audit: AT, Non-repudiation: NR, Anonymity: AN, Unlinkability: UN.

V. Conclusions and Open Research Issues

The privacy of the electronic health data in the cloud computing environment is a serious issue that requires special considerations. We have presented a state-of-the-art review on the approaches and methodologies that are currently being used to deal with the important issue of privacy. We have categorized the privacy preserving approaches into cryptographic and non-cryptographic approaches. Moreover, we have developed taxonomy of the techniques that have been applied to preserve the privacy of the existing data. We also presented a detailed comparison of the privacy preserving approaches from the perspective of the fulfillment of the

privacy preserving requirements and key management overhead. Despite all the efforts made to enhance the privacy of the electronic health data, there are certain areas and issues still open and need more attention. We briefly highlight the issues as under:

An important issue that arises due to the nature of the cloud is secure provenance. Generally, the provenance may include tracking and monitoring of: (a) actions taken, (b) the entities taking the actions, (c) the location of the actions, and (d) the reason for action [79]. Although the health cloud environment is protected against the privacy threats, still provenance of the health data may reveal sensitive information to the unauthorized individuals by monitoring the sequence of the events. Therefore, it is highly desirable that the mechanisms should be developed to deploy efficient auditing and accountability mechanisms that anonymously monitor the utilization of health records and track the provenance to ensure the confidentiality of the data.

Likewise, searchable encryption approaches based on public key encryption presented are computationally far less efficient as compared to symmetric key approaches [72]. Consequently, there is a significant need to devise more usable and efficient data search strategies without compromising on privacy of the cloud environment in general and the e-Health clouds in particular.

Another important issue worth investigating is determining and verifying the integrity of the health data in the cloud environment. Although existing privacy preserving mechanisms offer support to maintain the integrity of data in the cloud, assimilating the integrity verification mechanism with the existing solutions will offer the patients and the data owners to realize an increased sense of control over the data.

ACKNOWLEDGMENT

The authors are thankful to Usman Shahid Khan, Mazhar Ali, Saif-ur-Rehman Malik, Kashif Bilal, and Neelam Jabeen for the valuable reviews, suggestions, and comments.

REFERENCES

[1] D. Slamanig and C. Stingl, "Privacy aspects of e-Health," *3rd IEEE international Conference on Availability, Reliability and Security, (ARES '08)*, March 2008, pp.1226-1233.

[2] "Federal Health IT Initiatives," http://www.hhs.gov , accessed December 24, 2012.

[3] "Canada Health Infoway," http://www.infoway-inforoute.ca, accessed December 24, 2012.

[4] J. Dzenowagis and G. Kernen, "Connecting for health: Global vision, local insight," *World Health Organization Press, Report for the World Summit on the Information Society*, 2005, pp. 1-36.

[5] H. J. Cheong, N. Y. Shin, and Y. B. Joeng, "Improving Korean service delivery system in health care: focusing on national e-health system," in *IEEE International conference on e-Health, Telemedicine and Social Medicine (TELEMED '09)*, February 2009, pp. 263–268.

[6] L. Fan, W. Buchanan, C. Thummler, O. Lo, A. Khedim, O. Uthmani, A. Lawson, and D. Bell, "DACAR platform for e-Health services cloud," in *4th IEEE International Conference on Cloud Computing*, July 2011, pp. 219-226.

[7] P. G. Goldschmidt, "HIT and MIS: Implications of health information technology and medical information system," *Communication of the ACM,* Vol. 48, No. 10, October 2005, pp. 69–74.

[8] E. Davidson, and D. Heslinga, "Bridging the IT adoption gap for small physician practices: An action research study on electronic health records," *ACM Journal of Information Systems Management*, Vol. 24, No. 1, January 2007, pp. 15-28.

[9] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, "E-Health Cloud: Opportunities and challenges," *Future Internet*, Vol. 4, No. 3, July 2012, pp. 621-645.

[10] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," *3rd IEEE International Conference on Cloud Computing*, Miami, FL, USA, July 2010, pp.268–275.

[11] R. Wu, G.-J. Ahn, and H. Hu, "Secure sharing of electronic health records in clouds," In *8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work-sharing (CollaborateCom)*, 2012, pp. 711-718.

[12] S. P. Ahuja, S. Mani, and J. Zambrano1, "A survey of the state of cloud computing in healthcare," *Network and Communication Technologies,* Vol. 1, No. 2, September 2012, pp. 12-19.

[13] P. Mell and T. Grance, "*The NIST definition of cloud computing*", NIST specialpublication,2011,http://predeveloper.att.com/home/learn/enabling technologies/The_NIST_Definition_of_Cloud_Computing.pdf, accessed December 14, 2012

[14] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing," *IEEE INFOCOM Proceedings*, March 2010, pp. 1-9.

[15] B. Horowitz, *Cloud Computing Brings Challenges for Health Care Data Storage*, Privacy, *http://www.eweek.com/c/a/Health-Care-IT,* accessed December 20, 2012.

[16] G. Ahn, H. Hu, J. Lee, and Y. Meng, "Representing and reasoning about web access control policies," *34thIEEE Annual Conference on Computer Software and Applications, (COMPSAC '10),* July 2010, pp. 137–146.

[17] H. Takabi, J. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," *Security & Privacy, IEEE*, Vol. 8, No. 6, 2010, pp.24–31.

[18] R. Wu, G.J. Ahn, H. Hu, and M. Singhal, "Information flow control in cloud computing," *6th International Conference on Collaborative Computing: Networking, Applications and Work-sharing (CollaborateCom '10)*, October 2010, pp. 1-7.

[19] R. Wu, G. Ahn, and H. Hu, *Secure Sharing of Electronic Health Records in Clouds*, http://www.public.asu.edu/~hongxinh/papers/TrustCol12.pdf, accessed December 14, 2013.

[20] M. Johnson, "Data hemorrhages in the health-care sector," *Financial Cryptography and Data Security*, April 2009, pp. 71-89.

[21] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," *IEEE Communications Surveys & Tutorials*, July 2012, pp. 1-17.

[22] N. Gonzalez, C. Miers, F. Redígolo, T. Carvalho, M. Simplicio, M. Naslund, and M. Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud computing*," 3rd IEEE International Conference on Cloud Computing Technology and Science (CloudCom '11)*, November 2011, pp. 231-238.

[23] A. J. L. Fernández, I. C. Señor, P. Á.Oliver L., and A. Toval, "Security and privacy in electronic health records: a systematic literature review," Journal of Biomedical Informatics, 2013, pp. 541-562.

[24] N. Dong, J. Hugo, and J Pang, "Challenges in e-health: from enabling to enforcing privacy*," Foundations of Health Informatics Engineering and System*, 2012, pp. 195-206.

[25] S. Allen, *Cloud Computing and Health Care Security,* http://cloudcomputing.syscon.com/node/1796151, 2011, Accessed on December 20, 2012.

[26] *Health Insurance Portability and Accountability Act of 1996 (HIPAA),* http://aspe.hhs.gov/admnsimp/final/pvcpre03.htm, accessed January 4, 2013.

[27] P. Metri and G. Sarote, "Privacy issues and challenges in cloud computing," *International Journal of Advanced Engineering Sciences and Technologies*, Vol. 5, No. 1, 2011, pp. 001– 006.

[28] B. Grobauer, T. Walloschek, E. Stocker, "Understanding cloud computing vulnerabilities," *IEEE Security and Privacy*, Vol. 9,No. 2, March 2011, pp. 50–57.

[29] D.W. Chadwick, K. Fatema, "A privacy preserving authorization system for the cloud, "*Journal of Computer and System Sciences*, Vol. 78, December 2011, pp. 1359–1373.

[30] A. Pfitzmann, and M. Hansen, *Anonymity, unlinkability, unobservability, pseudonymity, and identity management – a consolidated proposal for terminology,*http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.154.421&rep=rep1&type=pdf, accessed on September 28, 2013.

[31] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," *ACM Workshop on Cloud Computing Security,* November 2009, pp. 85-90.

[32] A. Sahai and B. Waters, "Fuzzy Identity Based Encryption," in *Advances in Cryptology EUROCRYPT*, May 2005, pp. 457–473.

[33] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," *13th ACM Conference on Computer and Communications Security*, October 2006, pp. 89-98.

[34] H. Thomas, H. Löhr, A.R. Sadeghi, and M. Winandy, "Flexible patient-controlled security for electronic health records," *2nd ACM SIGHT Symposium on International Health Informatics*, January 2012, pp. 727-732.

[35] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving EHR system using attribute-based infrastructure*," The ACM Cloud Computing Security Workshop, (CCSW '10),* October 2010, pp.47–52.

[36] M. Barua, X. Liang, R. Lu, and X. Shen, "ESPAC: Enabling Security and Patient-centric Access Control for e-Health in cloud computing," *International Journal of Security and Networks,* Vol. 6, No. 2, 2011, pp. 67-76.

[37] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy preserving access control with authentication for securing data in clouds," In *12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid)*, 2012, pp. 556-563.

[38] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in *Security and Privacy in Communication Networks,* September 2010, pp. 89-106

[39] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, January 2013, pp. 131-143.

[40] A. Suhair, S. Radziszowski, and R.K. Raj, *Designing a Secure Cloud-Based EHR System using Ciphertext-Policy Attribute-Based Encryption,* http://www.cs.rit.edu/~spr/PUBL/ehr11.pdf, accessed December 20, 2012.

[41] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," *31st International Conference on Distributed Computing Systems (ICDCS '11),* June 2011, pp. 383-392

[42] A. V. Loenen "User Based Content Key Encryption for a DRM System," *WIPO Patent, WO/2006/038204*, issued April 13, 2006.

[43] M. Jafari, R. S. Naini, and N. P. Sheppard, "A rights management approach to protection of privacy in a cloud of electronic health records," *11th annual ACM workshop on Digital rights management,* October 2011, pp. 23-30.

[44] Z. R. Li, E.C. Chang, K.H. Huang, and F. Lai, "A secure electronic medical record sharing mechanism in the cloud computing platform," *15th IEEE International Symposium on Consumer Electronics (ISCE '2011)*, June 2011, pp. 98-103.

[45] D. Mashima and M. Ahamad, "Enhancing accountability of electronic health record usage via patient-centric monitoring," *2nd ACM SIGHIT Symposium on International Health Informatics*, January 2012, pp. 409-418.

[46] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," *ACM workshop on Cloud Computing Security,* November 2009, pp.103-114.

[47] A. Kaletsch and A. Sunyaev, A, "Privacy Engineering: Personal Health Records in Cloud Computing Environments," *32nd International Conference on Information Systems (ICIS '2011)*, December 2011, pp. 1–11.

[48] L. Hans, A.R. Sadeghi, and M. Winandy, "Securing the e-Health cloud," in *1st ACM International Health Informatics Symposium*, November 2010, pp. 220-229.

[49] M. Kallahalla, E. Riedel, R. waminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage, "in *Fast*, vol. 3, pp. 29-42. 2003.

[50] R. Steinfeld, L. Bull, H. Wang, and J. Pieprzyk, "Universal designated-verifier signatures," In *Advances in Cryptology-Asiacrypt* 2003, pp. 523-542. Springer Berlin Heidelberg, 2003.

[51] L. C. Huang, H. C. Chu, C. Y. Lien, C. H. Hsiao, and T. Kao, "Privacy preservation and information security protection for patients' portable electronic health records," *Computers in Biology and Medicine* 39, no. 9, 2009, pp. 743-750.

[52] J. Vilaplana, F. Solsona, F. Abella, R. Filgueira, and J. Rius, "The cloud paradigm applied to e-Health," *BMC Med. Inf. & Decision Making* 13, 2013, pp. 35.

[53] D. C. Kaelber, A.K. Jha, D. Johnston, B. Middleton, and D.W. Bates, "A research agenda for personal health records (PHRs)," *Journal of the American Medical Informatics Association,* 15(6), 2008, pp.729-736.

[54] Z. Zhou, and D. Huang, "On efficient ciphertext-policy attribute based encryption and broadcast encryption," *In Proceedings of the 17th ACM conference on Computer and communications security*, 2010, pp. 753-755.

[55] M. Chase and S.S. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in *Proceedings of 16th ACM Conference on Computer and Comm. Security (CCS '09),* 2009, pp. 121-130.

[56] Y. Y. Chen,J. C. Lu, and J. K. Jan, "A secure EHR system based on hybrid clouds," *Journal of medical systems* 36, no. 5, 2012, pp.3375-3384.

[57] E. Shi, and B. Waters, "Delegating capabilities in predicate encryption systems," In *Automata, Languages and Programming*, pp. 560-578. Springer Berlin Heidelberg, 2008.

[58] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," In *Advances in Cryptology—EUROCRYPT'98*, pp. 127-144. Springer Berlin Heidelberg, 1998.

[59] J. A. Akinyele, C. U. Lehmann, M. D. Green, M. W.Pagano, Z. N. J. Peterson, and A. D. Rubin, "Self-protecting electronic medical records using attribute-based encryption," *Cryptology e-Print Archive*, Report 2010/565, 2010.

[60] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," In *IEEE Symposium on Security and Privacy*, 2000 pp. 44-55.

[61] M. Barni, P. Failla, R. Lazzeretti, A-R. Sadeghi, and T. Schneider, "Privacy-preserving ECG classification with branching programs and neural networks," *IEEE Transactions on Information Forensics and Security*, 6, no. 2, 2011, pp. 452-468.

[62] M. Green, S. Hohenberger, and B.Waters, "Outsourcing the decryption of ABE ciphertexts," in *Proceedings of Usenix Security*, San Francisco, CA, USA, Aug. 8–12, 2011, pp. 34–49.

[63] K. Lauter, M. Naehrig, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*, 2011, pp. 113-124.

[64] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proc. CRYPTO*, 2001, pp. 213–229.

[65] C. Leng, H. Yu, J. Wang, and J. Huang, "Securing Personal Health Records in the Cloud by Enforcing Sticky Policies," *TELKOMNIKA Indonesian Journal of Electrical Engineering* 11, no. 4, 2013, pp. 2200-2208.

[66] T. S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau, and T.C. Lin, "Secure Dynamic access control scheme of PHR in cloud computing," *Journal of Medical Systems*, vol. 36, no. 6, pp. 4005–4020, 2012.

[67] R. Zhang, L. Liu, and R. Xue, "Role-based and time- bound access and management of EHR data," *Security and Communication Networks*, 2013, DOI: 10.1002/sec.

[68] J. L. Griffin, T. Jaeger, R. Perez, R. Sailer, L. Van Doorn, and R. Cáceres, "Trusted virtual domains: Toward secure distributed services," In *Proceedings of the 1st IEEE Workshop on Hot Topics in System Dependability (HotDep'05),* 2005, pp. 1-6.

[69] J. Pecarina, S. Pu, and J.-C. Liu, "SAPPHIRE: Anonymity for enhanced control and private collaboration in healthcare clouds," In *IEEE 4th International Conference Cloud Computing Technology and Science (CloudCom)*, 2012 on, pp. 99-106. IEEE, 2012

[70] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, and G. Müller, "Aspects of privacy for electronic health records," *International journal of medical informatics* 80, no. 2, 2011, pp. e26-e31.

[71] P. V. Gorp, and M. Comuzzi, "Lifelong Personal Health Data and Application Software via Virtual Machines in the Cloud,"2013, *IEEE Journal of Biomedical and Health Informatics*, January, 2012, pp. 1-10.

[72] H. Lin,J. Shao, C. Zhang, and Y. Fang, "CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring,", *IEEE Transactions On Information Forensics And Security*, Vol. 8, NO. 6, 2013 2013, pp. 985-997.

[73] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, 2010, pp. 261-270.

[74] L. Ibraimi, M. Asim, M. Petkovic, *Secure Management of Personal Health Records by Applying Attribute-Based Encryption*, University of Twente, Technical Report, 2009.

[75] C. Wang, X. Liu, and W. Li, "Design and implementation of a secure cloud–based personal health record system using ciphertext–policy attribute–based encryption," *International Journal of Intelligent Information and Database Systems* 7, no. 5, 2013, pp. 389-399.

[76] G. Hsieh, and R. J. Chen, "Design for a secure interoperable cloud-based Personal Health Record service," *In 4th IEEE International Conference on Cloud Computing Technology and Science (CloudCom),* 2012, pp. 472-479.

[77] M. Irfan, and S. Yasin, "A Novel Framework for Securing Medical Records in Cloud Computing" *International Journal of Modern Engineering Research (IJMER)*, Vol. 3, Issue, 2013, pp-2697-2699.

[78] S. Kamara, K. Lauter, "Cryptographic cloud storage," In *Financial Cryptography and Data Security*, 2010, pp. 136-149.

[79] R. Lu, X. Lin, X. Liang, and X. S. Shen, "Secure provenance: the essential of bread and butter of data forensics in cloud computing," *In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, 2010, pp. 282-292.

[80] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy* SP'07, 2007, pp. 321-334.

[81] J. Li, "Electronic Personal Health Records and the Question of Privacy, *IEEE Computers*, 2013,pp. 1-1.

[82] A. Rosenthal, P. Mork, M. H. Li, J. Stanford, D. Koester, and P. Reynolds, "Cloud computing: A new business paradigm for biomedical information sharing," *Journal of Biomedical Informatics* 43, no. 2, 2010, pp. 342-353.

[83] E. Bertino, N. Shang, and S. S. Wagstaff, "An efficient time-bound hierarchical key management scheme for secure broadcasting," *IEEE Transactions on Dependable and Secure Computing* 5, no. 2, 2008, pp. 65-70.

[84] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," In *Advances in Cryptology–EUROCRYPT* 2008, pp. 146-162.

[85] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," In *Advances in Cryptology-Eurocrypt* 2004, pp. 506-522.

[86] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *ACM Symposium on Theory of Computing STO,C* 2009, pp. 169-178.

[87] C. Gentry, and A. Silverberg, "Hierarchical ID-based cryptography," In *Advances in cryptology—ASIACRYPT*, 2002, pp. 548-566.

[88] A. Shamir, "Identity-based cryptosystems and signature schemes," In *Proceedings of CRYPTO 84 on Advances in cryptology*, Springer-Verlag New York,Inc., 1985, pp. 47–53.

[89] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern, "RSA-OAEP is secure under the RSA assumption," In *Advances in Cryptology—CRYPTO 2001*, pp. 260-274. Springer Berlin Heidelberg, 2001

[90] A. Liu, P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," In *IEEE International Conference on Information Processing in Sensor Networks*, 2008, pp. 245-256.

[91] M. Agrawal, and P. Mishra, "A comparative survey on symmetric key encryption techniques," *International Journal on Computer Science and Engineering (IJCSE)* Vol. 4, 2012, pp. 877-882.

[92] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security (TISSEC)* 9, no. 1, 2006, pp. 1-30.

[93] G. Ateniese, J.Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-resistant group signature scheme," *In Advances in Cryptology—CRYPTO,* 2000, pp. 255-270.

Assad Abbas completed Master of Science in Informatics from University of Skovde, Sweden in 2010. Currently, he is pursuing PhD at Department of Electrical and Computer Engineering, North Dakota State University, USA. He is affiliated with COMSATS Institute of Information Technology, Pakistan since 2004. His research interests are mainly but not limited to Cloud Computing, Information Systems, Knowledge Based Medical Decision Support Systems, and Data Mining.

Samee U. Khan received a BS degree from Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, Topi, Pakistan, and a PhD from the University of Texas, Arlington, TX, USA. Currently, he is Assistant Professor of Electrical and Computer Engineering at the North Dakota State University, Fargo, ND, USA. Prof. Khan's research interests include optimization, robustness, and security of: cloud, grid, cluster and big data computing, social networks, wired and wireless networks, power systems, smart grids, and optical networks. His work has appeared in over 225 publications. He is a Fellow of the Institution of Engineering and Technology (IET, formerly IEE), and a Fellow of the British Computer Society (BCS).

TABLE II

COMPARISON OF PRIVACY PRESERVING APPROACHES

Work	Technique(s)	Strength(s)	Weakness(es)	Adversarial Model Assumption	Privacy Preserving Requirements							
					IN	CO	AU	AC	AT	NR	AN	UN
[10]	Pseudonymity, digital signatures	Ensures all the privacy preserving requirements	Only described through a use case	Untrusted servers	✓	✓	✓	✓	✓	✓	✓	✓
[43]	PKE, CKE	Flexible access control using DRM	Increased overhead at client side	Trusted servers	×	×	✓	×	✓	×	×	×
[45]	PKE, signature verification	Accountable usage	Possibility of misuse by record issuer	Untrusted servers	✓	✓	✓	✓	✓	✓	-	-
[47]	PKE, digital signatures	Secure EHR referral	Insufficient patient centric functions	Semi-trusted servers	✓	×	✓	✓	×	✓	-	-
[48]	PKE , signature verification	TVD utilization	Scalability issues	Untrusted servers	✓	×	✓	-	×	✓	-	-
[69]	PKE,pseudonymity	Introduces anonymity boundaries between the user and provider	The service provider may learn about the health data contents	Semi- trusted servers	✓	✓	✓	×	✓	✓	✓	✓
[44]	SKE	Unlinkability among EHRs	Unfeasible portability mechanism	-	✓	✓	✓	×	×	×	-	-
[56]	SKE	Ensures patients' ownership over data	Emergency access provision is not secure	-	✓	✓	×	✓	✓	✓	×	×
[66]	SKE (DES)	Allows multiusers to access PHRs simultaneously	High implementation overheads in cloud	Semi- trusted servers	✓	✓	✓	✓	×	✓	-	-
[67]	SKE	Solves the issues of key distribution among multiple users	Difficult to manage multiple user roles	Untrusted Servers	✓	✓	✓	×	×		-	-
[14]	KP-ABE, PRE, Lazy re-encryption	Scalable access control	Computational overhead at server	Semi- trusted servers	×	✓	-	✓	✓	×	-	-
[34]	PKE, ABE	Flexible access control	Linkability among EHRs	Semi- trusted servers	×	✓	×	✓	✓	✓	-	-
[35]	bABE, PKE with keyword search	Efficient revocation	Inflexible access control	Semi- trusted servers	×	✓	×	×	×	✓	-	-
[36]	ABE, IBE, digital signatures	Patient centric access policies	Communication delays	Trusted servers	✓	✓	✓	×	×	×	×	×
[37]	ABE	Hides the identities of data storing entities	Cloud is aware of access policy about each record	Semi- trusted servers	×	×	✓	✓	×	×	✓	-
[38]	MA-ABE	Scalable access control	Management overhead	Semi- trusted servers	×	✓	✓	×	×	×	×	×
[39]	MA-ABE	Efficient user revocation	Limited in terms of access policy specification	Semi- trusted servers	×	✓	✓	✓	×	×	-	-
[40]	PKE, CP-ABE	Avoids re-distribution of keys	Limited in terms of access policy specification	Untrusted servers	×	×	✓	×	×	×	×	×
[59]	CP-ABE	Flexible patient control over EHRs	Key escrow problem	Semi- trusted servers	×	×	✓	×	✓	×	×	×
[41]	HPE, searchable encryption	Efficient revocation, search capability	Lack of access control	Semi- trusted servers	✓	×	×	✓	×	×	×	×
[46]	IBE, searchable encryption	Delegation and searchability	Inefficient user revocation	Untrusted servers	×	×	✓	✓	×	✓	-	-
[65]	SKE, C-PRE	Allows access on parts of data	Less flexibility in user revocation	Semi- trusted servers	×	✓	✓	×	×	×	×	×
[72]	IBE, homomorphic encryption	Computations on encrypted data	High implementation overheads	Semi- trusted servers	×	×	×	×	×	✓	✓	✓
[6]	Policy engines, policy repository, and domain ontology	Dissemination of specialized services	Integration issues with cloud	-	✓	✓	✓	×	✓	×	×	×
[11]	Policy manager and broker based authorization	Selective sharing of EHRs	Policy composition issues	-	×	×	✓	×	✓	×	×	×
[29]	Policy based authorization infrastructure	Sticky policies	Integrity issues	-	×	×	✓	✓	✓	×	×	×
[70]	Pseudonymity, policy based authorization	Patients monitor policy compliance	Management overhead in identifying information leakage	Semi trusted	✓	✓	-	×	✓	✓	✓	✓
[71]	Anonymity, SSH protocol	Remote monitoring	Software issues for virtual machines	Trusted server	×	×	✓	×	✓	×	✓	×