Computers in Biology and Medicine 78 (2016) 1–8

Contents lists available at ScienceDirect

Computers in Biology and Medicine

journal homepage: www.elsevier.com/locate/cbm

Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan

Aqeel Sahi [a,b,*], David Lai [a], Yan Li [a]

[a] Department of Math and Computing, University of Southern Queensland, 487/521-535 West St, Darling Heights, QLD 4350, Australia
[b] Computer Center, University of ThiQar, ThiQar, Iraq

ARTICLE INFO

Article history:
Received 27 June 2016
Received in revised form
9 September 2016
Accepted 9 September 2016

Keywords:
Disaster recovery plan
eHealth cloud
EHR
PHR
Privacy
Security

ABSTRACT

Cloud computing was introduced as an alternative storage and computing model in the health sector as well as other sectors to handle large amounts of data. Many healthcare companies have moved their electronic data to the cloud in order to reduce in-house storage, IT development and maintenance costs. However, storing the healthcare records in a third-party server may cause serious storage, security and privacy issues. Therefore, many approaches have been proposed to preserve security as well as privacy in cloud computing projects. Cryptographic-based approaches were presented as one of the best ways to ensure the security and privacy of healthcare data in the cloud. Nevertheless, the cryptographic-based approaches which are used to transfer health records safely remain vulnerable regarding security, privacy, or the lack of any disaster recovery strategy. In this paper, we review the related work on security and privacy preserving as well as disaster recovery in the eHealth cloud domain. Then we propose two approaches, the Security-Preserving approach and the Privacy-Preserving approach, and a disaster recovery plan. The Security-Preserving approach is a robust means of ensuring the security and integrity of Electronic Health Records, and the Privacy-Preserving approach is an efficient authentication approach which protects the privacy of Personal Health Records. Finally, we discuss how the integrated approaches and the disaster recovery plan can ensure the reliability and security of cloud projects.

1. Introduction

The technologies of Cloud Computing (CC) provide simple and easy on-demand network access to a shared group of computing resources, which are simple to install and maintain with minimal effort. They have become an important technology milestone and many scientists and researchers claim that cloud computing has changed the computing processes and IT markets. When access is powered by cloud computing, users can use comprehensive sets of tools for assessing various applications, storage and platforms through the Internet, as well as using the services offered by cloud producers.

The National Institute of Standards and Technology (NIST) stated that CC is a model for using computer resources and other modern technological functionality in the information technology world to provide services such as storage and applications [1]. Users can access and use cloud computing services without the need to acquire knowledge, expertise or even administration of infrastructures that support these services. There are three main types of services offered by the cloud [2]: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [3]. In addition, four deployment models have been identified for cloud architecture solutions, namely Private cloud; Community cloud; Public cloud and Hybrid cloud [4,5]. Since cloud computing shares resources distributed throughout the Internet and among the intranets, security is therefore an important issue.

CC can be applied in many sectors; in this research we will focus on the health sector. CC gives healthcare providers the ability to diagnose and evaluate a patient's health even though the patient is not at the hospital. This requires the patient's medical data to be distributed among physicians, nurses, insurance companies as well as the data owner to deliver flexible and prompt care to patients. The distribution of the patient's medical data raises security and privacy issues. Therefore, in this research we propose two approaches which we designed to preserve privacy and security in the eHealth cloud.

Before we present the approaches, we will define Personal Health Records (PHRs) and Electronic Health Records (EHRs).

* Corresponding author at: Department of Math and Computing, University of Southern Queensland, 487/521-535 West St, Darling Heights, QLD 4350, Australia.
E-mail address: akeel_sahy@yahoo.co.uk (A. Sahi).

http://dx.doi.org/10.1016/j.compbiomed.2016.09.003
0010-4825/

1.1. Personal Health Records (PHRs)

A PHR is medical data owned and managed by the patient himself [6]. A good PHR contains a precise and short record of the patient's medical history data collected from various sources (such as EHRs). These data can be easily reached by everyone having the required authorizations to display the PHR.

1.2. Electronic Health Records (EHRs)

According to Zapata [7], the International Organization for Standardization (ISO) stated that the EHR is a "repository of information regarding the health status of a subject of care, in computer processable form". Using the words of ISO/TS 18308 [8], the main purpose of an EHR is to deliver a registered record of healthcare which supports current and upcoming healthcare received by the patient from various healthcare providers.

Today, cloud computing is used by millions of people around the world. Cloud computing gives users the opportunity to store data in the cloud for easy access anytime and anywhere [9]. However, in the cloud environment, the user's data are controlled by service providers and not by the users themselves. The potential for data leaks is real, either intentionally or accidentally, which is unacceptable [10]. Common problems of security and privacy in the eHealth cloud include: confidentiality, integrity, authentication, access control, and non-repudiation [11].

The overall cloud computing theme is that we should be able to use all kinds of functionality and services provided by the cloud, but we would like to maintain our data privacy and security. Therefore, issues regarding privacy and security of data are the main factors limiting the widespread use of cloud computing. Much research has been done on these issues and several researchers claim that a versatile cryptography system may handle data security and data privacy issues more effectively than other methods [12]. With the use of cryptography systems, our proposed security and privacy approaches can tackle the security and privacy issues. Although security is the most important factor in any cloud project, disaster recovery (DR) planning needs to be considered also. There are three types of disaster that may cause major damage to any system: (1) natural disasters, such as flood, earthquake, and volcano, (2) man-made disasters, such as cybercrime and technological terrorism, and (3) technological accidents, such as infrastructure failure, and transportation failure [13]. In order to overcome these kinds of disaster, a recovery plan needs to be set up.

2. Related work

In this section, we review the related work on the preservation of security and privacy in the eHealth cloud as well as the DR planning.

Users are using CC in various ways, such as checking email by Yahoo, writing documents by Google Docs, and storing data in iCloud. CC delivers numerous benefits, for example, low costs due to the pay-as-you-go model, extraordinary availability as data is commonly distributed between a number of servers, and load balancing [1]. Furthermore, CC is benefiting health organisations [14].

Health organisations have been quick to move to CC for the obvious advantages of data storage and sharing. Those organisations are keen to store and share PHRs and EHRs using the cloud, thereby eliminating the geographical boundaries between health organisations and patients [15]. Sharing data using CC has rapidly become a very important component for healthcare providers and many other organisations. According to Thilakanathan et al. [16], for most organisations, the percentage of the data shared with clients using CC is about 74% and with dealers is about 64%.

On the other hand, it is important for medical data to be safe from unauthorized access and unwanted modifications. CC, however, is vulnerable to various security and privacy attacks. Consequently, many healthcare providers are unwilling to implement CC technologies, as a patient's information privacy may be breached. According to Van et al. [17], the main hurdle delaying the growth and extensive acceptance of CC is privacy and security issues. Actually, most privacy and security attacks are caused by the Cloud Service Providers (CSP) themselves [18] as they commonly have access to the Cloud Storage (CS) and they may also sell the data records to gain profits. Indeed, insider attacks are one of the main problems related to CC, as pointed out by El-Gazzar et al. and Pasupuleti et al. [19,20].

Fujisaki et al. proposed a PKE-based (Public Key Encryption) approach named RSA-OAEP [21]; however, PKE-based approaches are computationally inefficient because of the larger key size and the slower operation.

Jafari et al. introduced an approach which gives the patient the possibility of controlling his EHRs. This approach limits the patient to managing records authored by other parties, such as physicians and nurses [22]. On the other hand, the cloud service provider cannot retrieve the records in plaintext format. The patient himself and data consumers are given the private and public keys for encryption and decryption [23].

Another approach presented by Zhang et al. [24] is a time-based approach. The approach is efficient in ensuring the privacy of the EHRs at the cloud storage and enhances the operation of key distribution between trusted parties. This approach adopts time-bound hierarchical key management [25]. Time-bound hierarchical key management permits trusted parties to gain short-term access to the EHRs, which are encrypted using Symmetric Key Encryption (SKE). However, Zhang's approach is logically inadequate due to the fact that users have to take on multiple roles. Therefore, the users are required to hold and control multiple keys.

Tran et al. [26] proposed an approach based on the proxy re-encryption idea. A trusted user can obtain a data record as the proxy will convert the encrypted data on the data owner side to differently encrypted data which can be decrypted to plain text by the trusted user's key. However, because Tran's approach uses ElGamal public key cryptography, the encryption or decryption of very large data is not practical and unfortunately, very large data is a feature of medical data [16]. In addition, this approach does not solve the situation where a revoked party re-joins using another access key.

Tu et al. presented an approach which adopts Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for data sharing in the situation of a revocation operation, which at the same time allows high flexibility, access control and revocation [27]. However, this approach is also not effective when considering very large data [16].

An Access Control technique is a policy or rule that allows the restriction of access to a cloud project [28]. It also detects unauthorized users who try to access a cloud project. Access Control allows one application to trust the identity of another application [29]. While a robust authentication technique is a compulsory requirement for any cloud project, access control cannot secure data at rest and in transit [30,31], and it is not satisfactory enough to achieve privacy for PHRs [32]. Encryption methods are definitely a better choice for protecting data at rest, as well as the choice for protecting data in transit [30]. In addition, cryptography offers an integrity check to verify that the data is not compromised or corrupted in transit.

Wood et al. presented a DR plan which utilizes three servers and one database, as shown in Fig. 1. One of the servers is

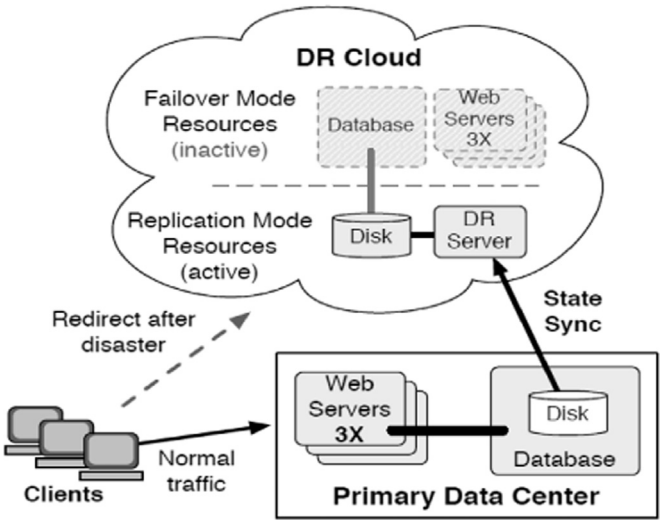

Fig. 1. Wood et al. DR plan [33].

nominated to be used in the event of a disaster, and all users are redirected to that server during the disaster [33]. However, the authors did not consider the case in which the disaster also affects the nominated server itself. In addition, the redirecting may influence the performance of the system and all users will be disconnected while they are being redirected to the nominated server.

In this paper, we are concerned with the following issues when strengthening the security and privacy of health records in the cloud:

- How to design compatible security and privacy approaches which can preserve the security of the EHR and the privacy of the PHR at the same time in the eHealth cloud.
  - How the proposed approaches perform in emergency situations.
  - How to revoke old session keys.
  - How to ensure the availability and the continuity of the system during a disaster.

From our point of view, security, privacy, and disaster recovery plans are crucial and need to be designed together to be homogeneous, accurate, and easy to implement. The lack of any one of them will certainly affect the performance of the others. Thus, designing one of them only, as in most of the related studies, is not enough to deal with the real world.

To build a better cryptography cloud project, four requirements need to be satisfied: authentication, non-repudiation, integrity, and confidentiality [4]. Most of the previous studies focused on either the security of the EHR or the privacy of PHR, which is not enough to achieve the requirements. Many researchers proposed good security approaches to ensure confidentiality, while others proposed good privacy approaches to ensure authentication. However, those approaches may not integrate seamlessly. Besides, non-repudiation and integrity need to be provided by the same system. Therefore, we were motivated to propose approaches that can be easily implemented and integrated in any distributed system to cover the requirements for both security and privacy. Moreover, on top of security of the EHR and privacy of the PHR, we designed our disaster recovery plan to guarantee the availability and the continuity of the system during a time of disaster. While disaster recovery is not considered by most of the studies in the eHealth domain, our approaches and the disaster recovery plan will enable data owners and patients to have full and safe control over their records.

In addition, our contributions:

- Proposed a security-preserving approach which can ensure the security and integrity of Electronic Health Records.
- Proposed a privacy-preserving approach which can ensure the privacy of Personal Health Records.
- Provided a break-glass access feature to be used in emergency situations. A revocation feature is also provided.
- Designed our disaster recovery plan to guarantee the availability and the continuity of the system during a disaster.

3. Preliminaries

3.1. PEM-AES

The Parallel Encryption Mode (PEM) was first introduced by Sahi et al. [34] as a block cipher mode of operation. The PEM adopted the Advanced Encryption Standards (AES) as an encryption algorithm. The PEM mode significantly enhances the encryption process in terms of speed and provides a data integrity check. In the PEM, each block uses the hash value of the shared data to ensure that the key stream has a very good randomness. Fast parallel processes and integrity checks are the reasons for choosing the PEM-AES. Fig. 2. together with Eqs. (1)–(5) briefly describe the process of the algorithm.

Encryption:

$$W = E_{(K \oplus IV)}(H(X_i)) \tag{1}$$

$$Y_i = E_{(K \oplus IV) \oplus H(X_i)}(X_i) \tag{2}$$

$$C_i = W + Y_i \tag{3}$$

Decryption:

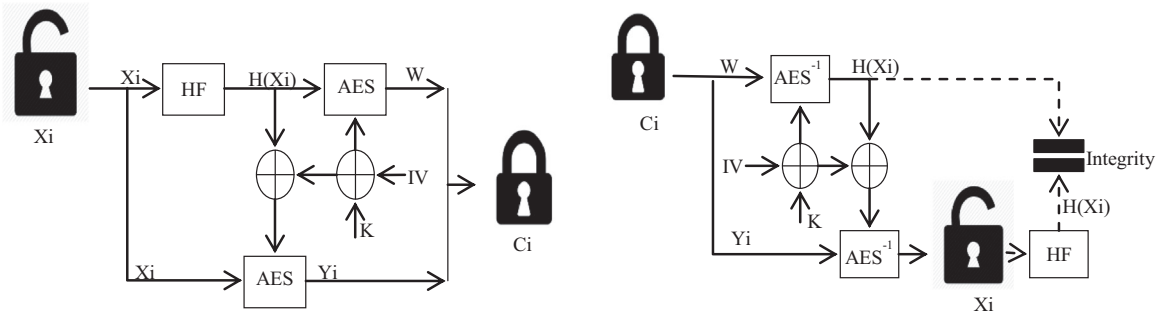

Fig. 2. PEM-AES processes [34].

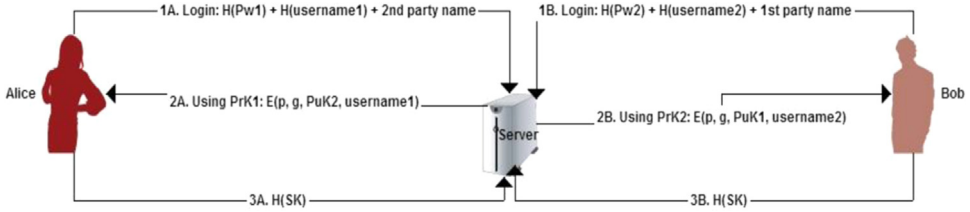

Fig. 3. Key exchange protocol [35].

$$H(X_i)=D_{(K\oplus IV)}(W) \quad (4)$$

$$X_i = D_{H(X_i)\oplus(K\oplus IV)}(Y_i) \quad (5)$$

3.2. Key exchange protocol

In order to ensure the privacy of the users, we adopt a three-party password-based authenticated key exchange protocol (3PAKE), which was introduced in [35]. This protocol ensures both authentication and non-repudiation features. A Geffe generator is used to produce a pseudorandom binary sequence. The resulting sequence is tested using statistical tests including a frequency test, serial test and poker test. Private keys are then generated from the success sequence. In this protocol, data will have a non-repudiation property and no clear data will be sent via the channel (Fig. 3).

4. The proposed approaches

While CC is facing numerous privacy and security issues, and despite the fact that most of these issues are caused by CSPs themselves, all data in CSPs and CSs must be encrypted. In other words, all medical records including PHRs and EHRs must be encrypted before CC stores and shares it. This will resist any attacks from outsiders as well as from insiders (the CSPs themselves) trying to obtain any valuable data without permission [35]. The patient's privacy needs to be ensured on top of the security for medical records.

The proposed approaches are shown in Figs. 4 and 5. They consist of data consumers, trusted party, patients, and cloud, which are defined as follows:

Data consumers: Data consumers are people or companies which are interested in using PHR or EHR data. In other words, data consumers are the healthcare providers, including physicians and nurses.

Controller: The controller is responsible for negotiating and generating session keys in order for them to be used by parties.

Data owner: The data owner is the owner of the data in our system, and is the only party who has full access to the EHR data.

Trusted party: The controller and data owner are trusted by all parties in our proposed approaches.

Patients: The patient is the owner of his PHR and has complete control over the privacy of his PHR information. He can delegate his patient role to other parties, such as a family member or friend in order to access his PHR in an emergency situation.

Cloud: The cloud consists of the cloud service provider and cloud storage. The cloud service provider responds to the demands from the data consumers and provides corresponding services. The cloud storage is used to store the shared encrypted data from the data owner.

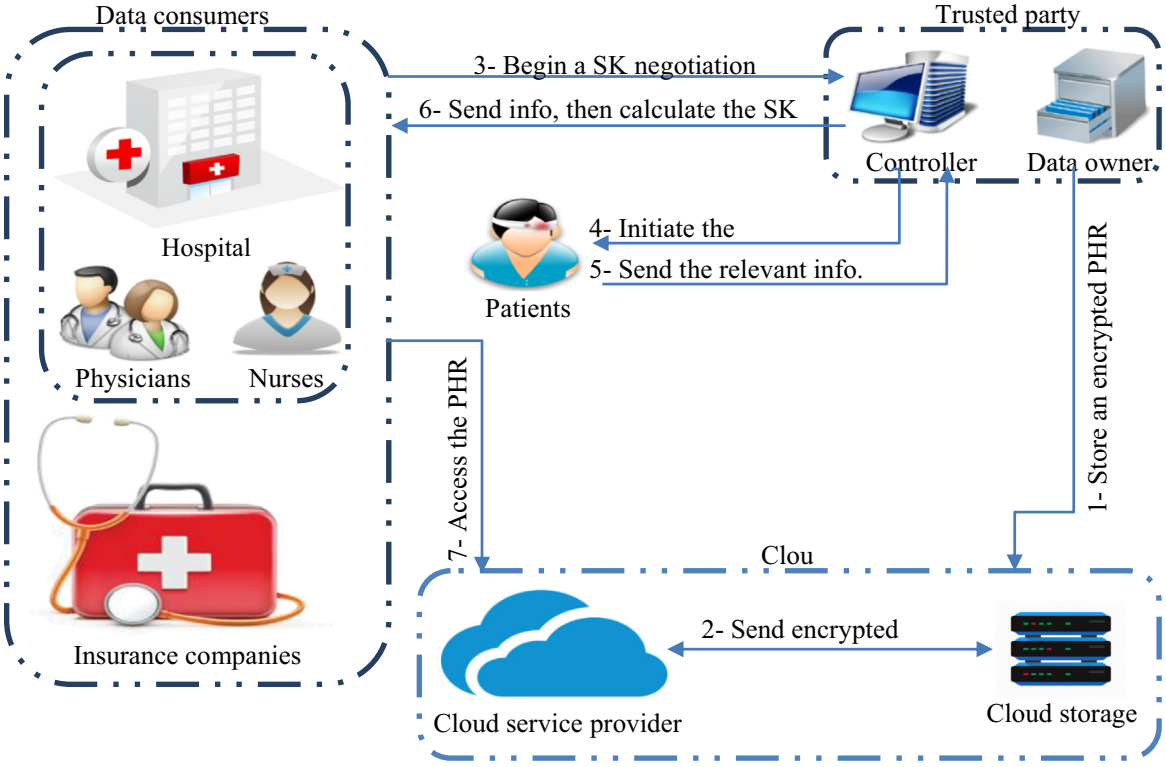

Fig. 4. Privacy-preserving approach.

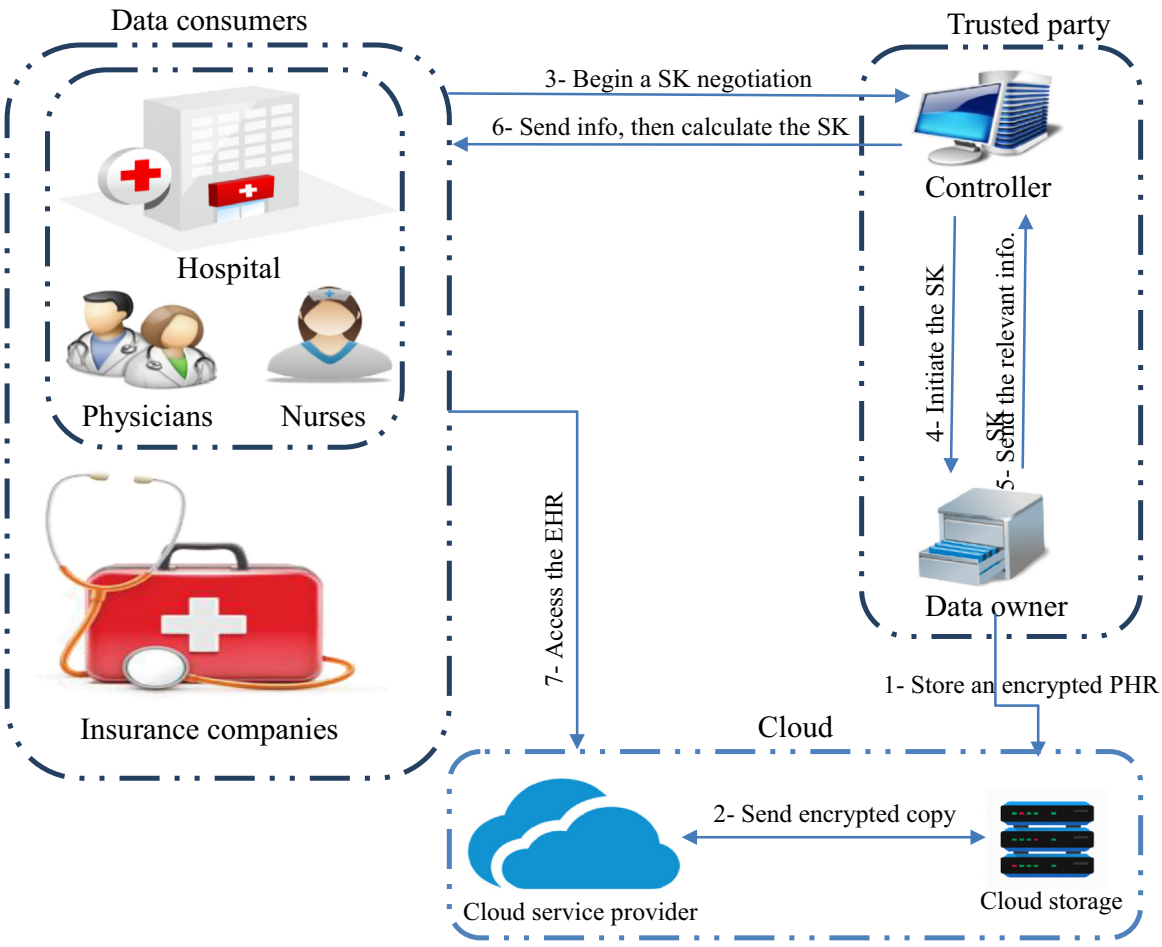

Fig. 5. Security-preserving approach.

To achieve the goals of the proposed approaches, two main points must be satisfied. Since the patient is the only one with full control over the access to his PHR information, the patient's privacy must be ensured in the first place. Secondly, all data consumers must be able to access an up-to-date version of their EHRs in the cloud at any time and in a secure manner, hence data security must be guaranteed.

In the following sections, we will explain the privacy-preserving approach, which can be used to ensure the privacy of the PHRs in the eHealth clouds. We then describe the security-preserving approach, which can be applied to ensure the security of the EHRs in the eHealth clouds.

4.1. *Privacy-preserving approach*

Authentication is vital for archiving and retrieving information from PHRs [36]. Since PHRs are controlled by patients themselves [6], an efficient authentication approach which ensures the privacy of PHRs is required.

In order to ensure the PHRs' privacy, we have adopted a three-party password-based authenticated key exchange protocol (3PAKE) based on the computational Diffie-Hellman assumption by Khader and Lai [35].

According to the 3PAKE protocol, the primitive root (p) and the generator (g) should be changed in each communication session [35]. This suits our approach to ensure that the patient is the only one who has complete access to his PHR, and all data consumers will be revoked after the session. Otherwise, if p and g are not changed, data consumers will be able to access the patient's PHRs using an old session key.

The privacy-preserving approach works as follows:

1. The data owner stores an encrypted PHR at the Cloud Storage (CS). The data are stored according to the disaster recovery plan in Section 6.
2. Therefore, the Cloud Service Provider (CSP) has a copy of the PHR. However, this copy is encrypted and the privacy of the PHR is secured. To make any modification to the PHR, the patient's permission is required. Data are retrieved according to the disaster recovery plan in Section 6.
3. Data consumers ask the controller to begin a Session Key (SK) negotiation in order to access the PHR.
4. The controller will control the communication between the data consumers and the patient. In this step, the controller will ask the patient to initiate the SK agreement.
5. The patient will then send the relevant information through the channel back to the controller in order to authorize the data consumer to gain access to his PHR.
6. The data consumer calculates the SK using the information received from the controller.
7. Data consumers can access the PHR at the CSP once they get the permissions.

4.2. *Security-preserving approach*

EHRs are managed by healthcare providers [6,37] (in our system, healthcare providers are data consumers). However, patients may have to follow various policies, such as medical, dental, and vision, registered with different insurance companies which make

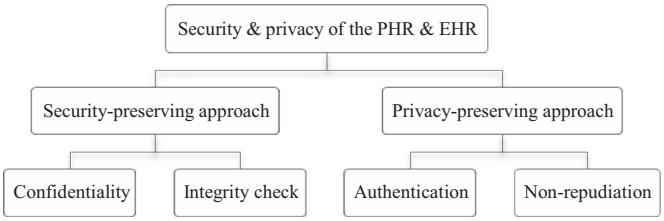

Fig. 6. Security and privacy of the PHR and the HER.

it hard for all parties to access up-to-date EHR records every time. Therefore, we have shifted the management of the data to the data owner or his delegate to ensure that all the consumers can access an up-to-date version of the EHR in the cloud at any time and in a secure manner.

The data owner stores the EHRs at their own preferred CC storage servers, and cloud projects must retrieve the EHRs from these servers. Therefore a robust approach which can ensure the security of the EHRs is required.

The AES encryption algorithm with the PEM block cipher mode was adopted to secure the data at the data owner database as well as at the cloud storage [34].

The security-preserving approach works as follows:

1. The data owner stores encrypted EHRs at the Cloud Storage (CS). Data are stored according to the disaster recovery plan in Section 6.
2. Therefore, the Cloud Service Provider (CSP) has a copy of the EHRs. However, this copy is encrypted to ensure the security of the EHRs. To use the EHRs, the CSP needs the data owner's permission to do so. Data are retrieved according to the disaster recovery plan in Section 6.
3. Data consumers ask the controller to begin the Session Key (SK) negotiation in order to access the EHRs.
4. The controller will control the communication between the data consumers with the data owner. In this step, the controller will ask the data owner to initiate the SK agreement.
5. The data owner will send the relevant information through the channel back to the controller in order to authorize the data consumer to gain access to the EHR.
6. The data consumer calculates the SK using the information received from the controller.
7. Data consumers can access the EHR at the CSP once they get permission.

4.3. Break-glass access

In an emergency situation, such as in a life-threatening situation for an unconscious patient, healthcare providers may require temporary access to a patient's PHR. Those staff members must have a temporary authorisation to decipher the PHR information. While the patient is the only one in our system who has complete control of his PHR, as we mentioned earlier the patient can also delegate the role to a family member or friend. Therefore, a family member or friend can play a patient role in order to authorize the data consumers to access the patient's PHR. In our approaches this can be achieved by encouraging a patient to delegate an emergency key to a family member or friend when the patient registers for the first time in the system. He will be asked to provide an emergency contact detail for a family member or friend, and to assign an emergency key to this person.

5. Discussion

To ensure the security and the privacy of any cryptography-based system, four requirements need to be considered: authentication, non-repudiation, integrity, and confidentiality [4]. In this section, we will analyse and evaluate the security of our proposed approaches from three different perspectives: security requirements, comparison with existing work, and when under several kinds of attacks.

5.1. Security requirements

CSP should utilize a robust authentication and non-repudiation technique to guarantee authentication and non-repudiation. According to Khader and Lai in [35], these two features are ensured by the 3PKAE key exchange protocol. Since we employed the protocol in this paper, our proposed privacy-preserving approach inherited the authentication and non-repudiation features from the adopted 3PAKE protocol.

In addition, the PEM-AES can check the integrity of the message by comparing the hash of the copy of the original data with the hash received from the other party. It has a concept similar to Chaining Blocks Cipher (CBC) in terms of confidentiality. It connects all the blocks by the hash value of the plaintext. Hence, if one cipher block is corrupted, then the corresponding plaintext block will also be corrupted. Since the CBC mode is considered to be secure against many attacks, we can claim that the PEM-AES mode is also secure against these attacks. In addition, it provides integrity on top of the confidentiality [34]. As we adopted the PEM-AES in our approaches, they too can provide these two features.

Fig. 6 illustrates the security and privacy features that can be provided by combining the privacy-preserving approach with the security-preserving approach in the cloud environment.

5.2. Comparison with existing work

In this section, we compare our proposed approaches with several existing approaches in terms of security, privacy, revocation, break-glass access and DR plan.

Table 1 shows the comparison. As shown in the table, our proposed approaches together with the disaster recovery plan achieved all the listed features, whereas some vital features are missing in other approaches. On top of that, some of those approaches have limitations in various aspects. In the RBTBAC approach [24], each user is required to hold and control multiple keys, which is logically inadequate. The approach by Tran et al. and the new CP-ABPRE approach [26,27] are not effective when considering very large data, and unfortunately very large data is a feature of medical data [16]. Furthermore, the approach by Fabian et al. is not well-suited for emergency cases, as stated by the authors themselves [39]. Finally, the approach of Chen et al. gives the ability of managing the PHR to every healthcare staff member in addition to patients and doctors; yet the PHR needs to remain safe at all times and be able to be managed by the patient himself and his doctor (even for the doctor, a revocation feature is needed to cancel his managing right later) [40].

Table 1
Comparison of delivered security features.

	Proposed approaches	Security	Privacy	Revocation	Break-glass	DR plan
1	Jafari et al. [22]	×	√	×	√	×
2	RBTBAC [24]	√	√	×	×	×
3	Tran et al. [26]	√	×	√	×	×
4	New CP-ABPRE [27]	√	×	√	×	×
5	Wang et al. [38]	×	√	×	×	×
6	Fabian et al. [39]	√	√	×	×	×
7	Chen et al. [40]	×	√	√	×	×
8	CP-ABE [41]	√	√	×	×	×
9	Zheng [42]	×	√	√	×	×
10	Our approaches	√	√	√	√	√

5.3. When under attack

When the PHR and EHR are under different attacks, we will show how the proposed approaches can mitigate the effects of some of these attacks.

5.3.1. Outside attacks

In outside attacks, an adversary attempts to gain electronic records without any identity or access credentials. Let us assume that he can compromise the communication channels and is able to retrieve the PHR/EHR records. However, he can only get the PHR/EHR records in an encrypted format, which he cannot decrypt without an appropriate key. While keys are held only by the patient and the controller, obtaining the correct key is impossible. Thus, we can claim that our approaches can prevent outside attacks.

5.3.2. Man-in-the-middle attacks

In our proposed approaches, it is impossible for an adversary to perform a man in the middle attack. Let us assume that the adversary can compromise the communication channels and retrieve any information sent through this channel. Nevertheless, the adversary needs to know at least the public keys to perform a man in the middle attack, whereas these public keys are encrypted using private user keys according to the adopted 3PAKE protocol [35]. In the 3PAKE protocol, only the user (either the patient or controller) himself can know the public and private keys, so he is the only one who can decrypt the electronic records. Thus, the proposed approaches can prevent man-in-the-middle attacks.

5.3.3. Offline and online dictionary attacks

The 3PAKE protocol can also be secure against offline and online dictionary attacks. For an adversary to perform an offline dictionary attack, he needs to guess the identity credential of the user to calculate the session key. This is going to fail during the verification process due to the fact that the session key is required for verification of the identity credential in advance.

An integrity check is provided in this protocol, and it helps to prevent on-line dictionary attacks using checksum validations. As parties are required to validate one another using a stored checksum, online dictionary attacks can thus be prevented.

6. Disaster recovery plan

In the event of a disaster several questions will need to be answered. For example: do we have a backup server? Where is it? How do we reconnect the client back to the system? How long will the system take to resume service? Therefore, a DR plan must be prepared to answer these and other questions.

We will present our DR plan. First of all, data such as PHRs and EHRs are stored in the cloud storage, which includes a minimum of three nodes or data centres. At the beginning of the process, the data owner will send a heartbeat signal (a heartbeat is a signal sent between the data owner, nodes, and the CSP to check whether those nodes are still in working condition or not) to check the status of the nodes. After that, the data owner asks the controller to break the data records into three partitions (three in our example, but it could be varied), distribute and store them among the nodes. When a client attempts to use the data through the CSP, the CSP will send a heartbeat signal to the nodes, and then ask the controller to retrieve the three partitions from the nodes and combine them in one record file.

The controller is responsible for the number of partitions and the size of each of them. Each partition must be stored in several nodes (in our case, three nodes). The three nodes must be located at three different physical locations in order to ensure that the cloud project can be continued even in a disaster situation.

For example, let us assume that the area where the second node is located has an earthquake, which causes complete damage to this node. The original record can be retrieved immediately from node 1 and node 3 with no time wasted or client disconnected. Therefore, this DR plan can answer the above questions and ensure the continuity of the system, as shown in Fig. 7.

7. Conclusion

The security and privacy of data are the most important factors in the cloud. Therefore, this research study aims to set up new approaches to harden the security of the EHRs and the privacy of the PHRs in cloud projects, as well as ensuring the continuity of the projects during a time of disaster. A privacy-preserving approach was proposed based on a key exchange protocol, which can ensure the privacy of the PHRs. Also, a security-preserving approach was proposed based on the PEM-AES, which can ensure the security of the EHRs. These two approaches are able to provide the most important requirements in each cryptosystem, such as authentication, non-repudiation, integrity, and confidentiality. In addition, a DR plan was proposed to enable a client to connect to its system at any time, even at a time of disaster. The two approaches and the DR plan all together provide a private, secure and robust CC environment for the health sector.

Conflicts of interest

None declared.

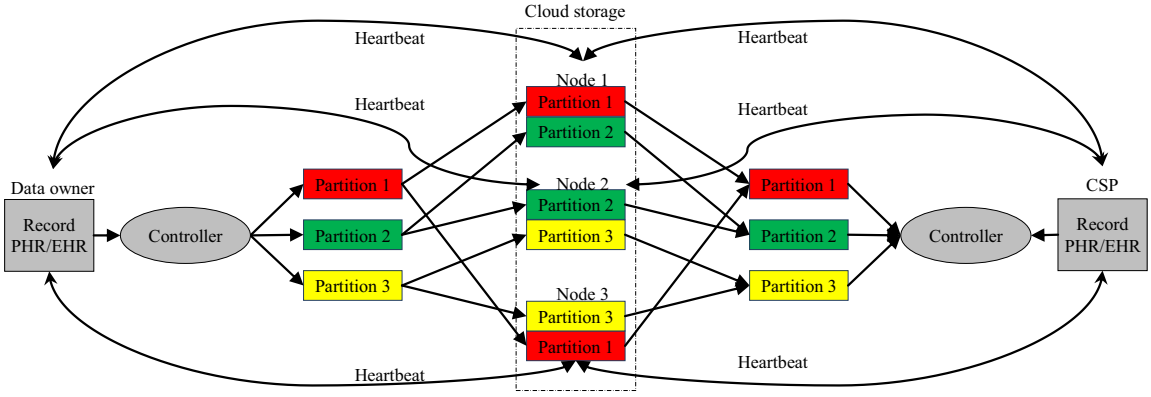

Fig. 7. The proposed DR plan.

Acknowledgements

This research did not receive any specific Grant from funding agencies in the public, commercial, or not-for-profit sectors. The constructive comments from the anonymous reviewers are greatly appreciated. Professor Barbara Harmes is gratefully acknowledged for her help and support.

References

[1] P. Mell, T. Grance, The NIST Definition of Cloud Computing, 2011.
[2] M. Sugumaran, B.B. Murugan, D. Kamalraj, An architecture for data security in cloud computing, in: Proceedings of the 2014 World Congress on Computing and Communication Technologies (WCCCT), 2014, pp. 252–255.
[3] K.E. Kushida, J. Murray, J. Zysman, Cloud Computing: From Scarcity to Abundance, BRIE Working Paper, Springer, 2014.
[4] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Gener. Comput. Syst. 28 (2012) 583–592.
[5] I. Hsu, F.Q. Cheng, SAaaS: a cloud computing service model using semantic-based agent, Expert Syst. 32 (2013) 77–93.
[6] A. Abbas, S.U. Khan, A review on the state-of-the-art privacy-preserving approaches in the e-health clouds, IEEE J. Biomed. Health Inform. 18 (2014) 1431–1441.
[7] B.C. Zapata, A.H. Niñirola, A. Idri, J.L. Fernández-Alemán, A. Toval, Mobile PHRs compliance with Android and iOS usability guidelines, J. Med. Syst. 38 (2014) 1–16.
[8] ANSI, ISO, TS 18308 Health Informatics-Requirements for an Electronic Health Record Architecture, ISO (Ed.), 2003.
[9] M. Carroll, A. Van Der Merwe, P. Kotze, Secure cloud computing: benefits, risks and controls, in: Proceedings of Information Security South Africa (ISSA), 2011, pp. 1–9.
[10] N. Gonzalez, C. Miers, F. Redígolo, M. Simplicio, T. Carvalho, M. Näslund, et al., A quantitative analysis of current security concerns and solutions for cloud computing, J. Cloud Comput. 1 (2012) 1–18.
[11] D.G. Rosado, R. Gómez, D. Mellado, E. Fernández-Medina, Security analysis in the migration to cloud environments, Future Internet 4 (2012) 469–487.
[12] D. Talbot, Security in the Ether, Technol. Rev. 113 (2010) 36–42.
[13] S. Snedaker, Business Continuity and Disaster Recovery Planning for IT Professionals, Newnes, 2013.
[14] E.J. Giniat, Cloud computing: innovating the business of health care, Healthc. Financ. Manag.: J. Healthc. Financ. Manag. Assoc. 65 (2011) 130–131.
[15] R. Wu, Secure Sharing of Electronic Medical Records in Cloud Computing, Arizona State University, 2012.
[16] D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, L. Alem, A platform for secure monitoring and sharing of generic health data in the cloud, Future Gener. Comput. Syst. 35 (2014) 102–113.
[17] P. Van Gorp, M. Comuzzi, A. Jahnen, U. Kaymak, B. Middleton, An open platform for personal health record apps with platform-level privacy protection, Comput. Biol. Med. 51 (2014) 14–23.
[18] F. Rocha, S. Abreu, M. Correia, The final frontier: confidentiality and privacy in the cloud, Computer 44 (9) (2011) 44–50.
[19] R. El-Gazzar, E. Hustad, D.H. Olsen, Understanding cloud computing adoption issues: a Delphi study approach, J. Syst. Softw. 118 (2016) 64–84.
[20] S.K. Pasupuleti, S. Ramalingam, R. Buyya, An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing, J. Netw. Comput. Appl. 64 (2016) 12–22.
[21] E. Fujisaki, T. Okamoto, D. Pointcheval, J. Stern, RSA-OAEP is secure under the RSA assumption, J. Cryptol. 17 (2004) 81–104.
[22] M. Jafari, R. Safavi-Naini, N.P. Sheppard, A rights management approach to protection of privacy in a cloud of electronic health records, in: Proceedings of the 11th Annual ACM Workshop on Digital Rights Management, 2011, pp. 23–30.
[23] I. Khalil, A. Khreishah, M. Azeem, Consolidated identity management system for secure mobile cloud computing, Comput. Netw. 65 (2014) 99–110.
[24] R. Zhang, L. Liu, R. Xue, Role-based and time-bound access and management of EHR data, Secur. Commun. Netw. 7 (2014) 994–1015.
[25] E. Bertino, N. Shang, S.S. Wagstaff Jr., An efficient time-bound hierarchical key management scheme for secure broadcasting, IEEE Trans. Dependable Secur. Comput. 5 (2008) 65–70.
[26] D.H. Tran, H.-L. Nguyen, W. Zha, W.K. Ng, Towards security in sharing data on cloud-based social networks, in: Proceedings of the 2011 8th International Conference On Information, Communications and Signal Processing (ICICS), 2011, pp. 1–5.
[27] K. Liang, M.H. Au, J.K. Liu, W. Susilo, D.S. Wong, G. Yang, Y. Yu, A. Yang, A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing, Future Gener. Comput. Syst. 52 (2015) 95–108.
[28] A.R. Khan, Access control in cloud computing environment, ARPN J. Eng. Appl. Sci. 7 (2012) 613–615.
[29] B. Sosinsky, in: illustrated (Ed.), Cloud Computing Bible, 762, John Wiley & Sons, United States of America, 2010.
[30] J. Sen, Security and privacy issues in cloud computing, Archit. Protoc. Secur. Inf. Technol. Infrastruct. (2013) 1–45.
[31] Y.A. Younis, K. Kifayat, M. Merabti, An access control model for cloud computing, J. Inf. Secur. Appl. 19 (2014) 45–60.
[32] Y. Yang, H. Zhu, H. Lu, J. Weng, Y. Zhang, K.-K.R. Choo, Cloud based data sharing with fine-grained proxy re-encryption, Pervasive Mob. Comput. 28 (2015) 122–134.
[33] T. Wood, E. Cecchet, K.K. Ramakrishnan, P.J. Shenoy, J.E. van der Merwe, A. Venkataramani, Disaster recovery as a cloud service: economic benefits & deployment challenges, in: Proceedings of the HotCloud, vol. 10, 2010, pp. 8–15.
[34] A. Sahi, D. Lai, Y. Li, Parallel encryption mode for probabilistic scheme to secure data in the Cloud, in: Proceedings of the 10th International Conference on Information Technology and Applications (ICITA), Sydney, 2015.
[35] A. S. Khader, D. Lai, Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol, in: Proceedings of the 22nd International Conference on Telecommunications (ICT), 2015, pp. 204–208.
[36] D.C. Kaelber, A.K. Jha, D. Johnston, B. Middleton, D.W. Bates, A research agenda for personal health records (PHRs), J. Am. Med. Inform. Assoc. 15 (2008) 729–736.
[37] L.-C. Huang, H.-C. Chu, C.-Y. Lien, C.-H. Hsiao, T. Kao, Privacy preservation and information security protection for patients' portable electronic health records, Comput. Biol. Med. 39 (2009) 743–750.
[38] C. Wang, X. Liu, W. Li, Implementing a personal health record Cloud platform using ciphertext-policy attribute-based encryption, in: Proceedings of Intelligent Networking and Collaborative Systems (INCoS), 2012, pp. 8–14.
[39] B. Fabian, T. Ermakova, P. Junghanns, Collaborative and secure sharing of healthcare data in multi-clouds, Inf. Syst. 48 (2015) 132–150.
[40] T.-S. Chen, C.-H. Liu, T.-L. Chen, C.-S. Chen, J.-G. Bau, T.-C. Lin, Secure dynamic access control scheme of PHR in cloud computing, J. Med. Syst. 36 (2012) 4005–4020.
[41] L. Ibraimi, M. Asim, M. Petković, Secure management of personal health records by applying attribute-based encryption, in: Proceedings of the 2009 6th International Workshop on Wearable Micro and Nano Technologies for Personalized Health (pHealth), 2009, pp. 71–74.
[42] Y. Zheng, Privacy-Preserving Personal Health Record System using Attribute-based Encryption, Worcester Polytechnic Institute, 2011.

Aqeel Sahi is a Ph.D. student in the Department of Mathematics and Computing, Faculty of Health Engineering and Sciences at University of Southern Queensland, Toowoomba 4350, QLD, Australia. He received a Bachelor degree of Computer Science from Thiqar University, Iraq in 2007, and Master degree of Information Technology from University Utara Malaysia, Malaysia in 2010. His current research interests are in cryptography and parallel processing with a focus on block cipher modes of operation and key exchange protocols.

David Lai is a senior lecturer in the Department of Mathematics and Computing, Faculty of Health Engineering and Sciences at University of Southern Queensland, Toowoomba 4350, QLD, Australia. Qualifications BSc CUHK , PGDipEd CUHK , GDipCompSc VUT , MPhil CUHK , MIT QUT , PhD USQ.

Yan Li is an associate professor in the Department of Mathematics and Computing, Faculty of Health Engineering and Sciences at University of Southern Queensland, Toowoomba 4350, QLD, Australia. Qualifications BEng HUST , MEng HUST , PhD Flinders. Approved research supervisor in the area of: Signal Processing (090609), Computer Communications, Networks (100503), Fields of Research (FoR), Biomedical Engineering, Artificial Intelligence, Image Processing, Signal Processing and Computer Communications Networks. Research interests: Machine Learning Algorithms, Big Data Analytics, Signal/Image Processing, EEG Research, Graph Theory, and Networking Technologies.