SN Computer Science (2020) 1:239
https://doi.org/10.1007/s42979-020-00246-4

ORIGINAL RESEARCH

Privacy Enforced Access Control Model for Secured Data Handling in Cloud-Based Pervasive Health Care System

P. Blessed Prince[1] · **S. P. Jeno Lovesum**[1]

Received: 29 May 2020 / Accepted: 27 June 2020 / Published online: 21 July 2020

Abstract
Health care is a significant application of pervasive computing. In recent years, the pervasive health care applications are replaced by cloud-based health care applications thus solving the problem of scalability and computing cost. In a cloud-based pervasive health care data security and privacy becomes a greater concern. The key contribution of this paper is to provide high privacy, data confidentiality, availability against the health data and this is achieved using the proposed access control model which uses a PR based approach for providing access control to various users of the system. Privacy rating (PR) is calculated for both the user and the data to provide access to any data that is being requested by the user. The results achieved shows that the proposed model achieves high level of privacy and security for the data stored in the healthcare system.

Keywords Pervasive · Cloud · Security · Privacy rating · Health data

Introduction

Health care is an important area of pervasive applications. Pervasive means anywhere computing without the intervention of users. When it comes to pervasive systems a group of devices are connected with wired and wireless technology to form an invisible and intelligent computing environment so that the system can work with or without user intervention. These connected devices are capable of functioning independently with each other. All devices connected to the system are embedded with chips to connect the device to a network of other devices, where connectivity is always available [1]. Thus, facilitating its users to use the application of pervasive computing in various fields such as healthcare, homecare, transport, etc.

The main aim of pervasive healthcare is to use pervasive computing technologies to provide healthcare anywhere anytime for its users. It replaces the traditional system of health care which consists of finding the symptoms, visiting a doctor, communicating the symptoms, getting treated. But Pervasive healthcare provides healthcare facilities to individuals anywhere and at any time. It uses the concept of deploying the sensing and communication (wired and wireless) technologies to monitor patient's health continuously by collecting the data through sensors. This helps to communicate accurate health information to a doctor or a medical professional, thereby giving proper and timely diagnosis and treatment for health problems of a patient anywhere. Recent advancements in communication and sensing technologies via cloud has led to the development of intelligent handheld and wearable devices (such as PDAs, cell phones, smart watches, etc.) that have made it possible to implement a large range of advancements in pervasive health care systems. In recent years, the pervasive health care applications are been converted into a cloud-based application, so that it can be provided as a service over the internet by a service provider so that the application could be made more efficient with better scalability. As this health care is being transformed into cloud based the security issue becomes a greater concern. Pervasive health care provides some advantages [1].

This article is part of the topical collection "Advances in Computational Approaches for Artificial Intelligence, Image Processing, IoT and Cloud Applications" guest edited by Bhanu Prakash K. N. and M. Shivakumar.

✉ P. Blessed Prince
blessedprince@gmail.com

S. P. Jeno Lovesum
jenolovesum@gmail.com

[1] CSE Department, Presidency University, Bangalore, India

Mobile Telemedicine

Using this we can monitor, diagnose, and treat patients from anywhere, which in turn reduces the chances of medical errors and aids to the treatment of patients by providing complete health information to the medical professional. Example includes health care in remote rural locations and providing fast response to any medical emergency and providing patient treatment for post operative care.

Pervasive Access to Patient Health Data

The Pervasive healthcare systems are able to collect data from patients across a period of time. These data collected are stored in an organized manner so that they can be retrieved by the patients and doctors to provide better care for his patient. Hence the security, privacy, and confidentiality of the personal health data available in a pervasive health care system is the greatest concern for its users, since it is cloud based and all information are available to a third party [2]. Therefore, the pervasive health care system requires very high level of security as well as privacy.

Related Works

After the first CP-ABE scheme proposed by Bethencourt et al. [3], there have been presented several variants of CP-ABE in order to improve the security of the access structure [4–7]. However, most of the existing CP-ABE schemes are built on the method, where a single KGC has the power to generate the whole private keys of users with its master secret key information. Thus, the key escrow problem is inherent such that the KGC can decrypt every ciphertext in the system by generating every user's secret key at any time.

Zou et al. [8] proposed a reliable and secure access control scheme for the medical information system. In this scheme, the data that is being transferred between various medical devices is temporarily stored in the memory to find the reliable communication in the presence of the third party and unreliable network connection. The access policy is enforced by the polynomial function, which delivers data encryption keys to receivers. However, the size of the rekeying message increases in proportion to the number of receivers, because the polynomial function is linearly constructed using all the attributes of receivers by the key management server. Thus, this scheme lacks efficiency in terms of the scalability in a large-scaled medical information system, and key escrow is also inherent. In addition, this scheme is not appropriate to define and enforce fine-grained access policy, since the access structure can be expressed with only 'OR' logic.

Bobba et al. [9] proposed a policy-based encryption scheme for data sharing. In this approach, a sender can encrypt the data encryption key with the attribute-based access policy, and can store it in an external storage area together with the encrypted data. When a receiver obtains the encrypted data and key encryption message from the storage node, the receiver forwards the key encryption message to the KGC. Then, the KGC decrypts the encryption key and sends it to the receiver if the receiver's attributes satisfy the policy. The main problems of this approach are the key escrow to the KGC and the communication overhead. Since all entities in the system should ask the KGC to decrypt every ciphertext (that is, key encryption message), not only the key escrow to the KGC is inherent but also additional communication cost is required, which is linear to O(d), where d is the number of decryption queries in the system. Even worse, even if the authors did not address it.

David et al. 2014 [10] proposed an utility preserving protection of textual healthcare documents. It provides an automatic protection of individual health records in the textual format. In addition, semantically defined relations were implemented to determine the disclosure property among system users.

Ji-Jiang et al. 2015 [11] described an hybrid solution for privacy preserving medical data sharing in the cloud environment. Jiang's work highly focused, enforcement of privacy in the shared environment, which increases the high demand for access control mechanism. A real world case study has been detailed along with the integration of innovatively combined multiple paradigms to safeguard shared personal health records.

In 2015, Chandramohan et al. [12] illustrated a multi-agent approach to preserve user information privacy for a pervasive and ubiquitous environment. This work proposed an hybrid authentication technique based on cryptographic algorithms to ensure end-user privacy policies. They have also explained the need for ensuring confidentiality in the cloud applications.

Problem Formulation

The proposed privacy model has three types of privacy of policy namely default privacy, user privacy and case record (health record) policy. The default privacy policy is one that is made default in the health care system and it can be changed if the user wants to change his default privacy settings. User privacy is related to the privacy of an user registered with the system. Case record privacy is setting privacy for the health records related to the patient who is the primary user. All the above privacy is given three

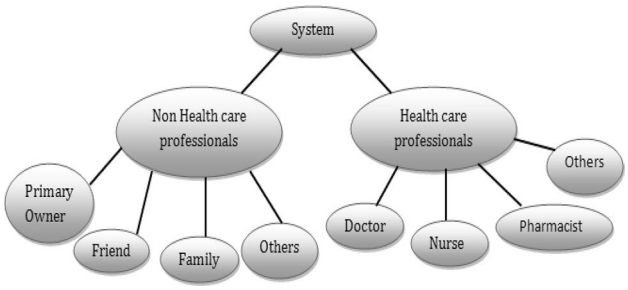

Fig. 1 User hierarchy

values high, medium and low. The default privacy is always medium when the user registers with the system. In the proposed data privacy policy and access control relationship plays a major role. The policy has been crated based on the relationship.

When a user (any one element from Fig. 1) registers himself with the health care system he creates a relationship with another user of the system, e.g., patient, doctor, nurse, ER units, pharmacist etc. Based on this relationship created one can add, view, edit and delete data regarding the primary user (patient). For data integrity the data is classified into validated data, non -validated data and Not applicable data. Based on the relationship created Validated data is one which is uploaded by the doctor who has high or medium confidentiality access policy in the system, non-validated data can be the one uploaded by any user who is not granted high/medium confidentiality access. Not applicable data is one that need not be validated, since it may not be related or it may be a minor cause. Base on the relationship the data is made available to the primary user (patient), immediate family, my doctor, other doctors, pharmacist, friends etc.

The proposed technique enforces the privacy over shared personal health data based on privacy rating assigned to the data as well as system entities. Initial level privacy ranking were assigned by the primary owner, where as the privacy rating which is crucial for determining access control were generated and assigned by the system. System centric access granting mechanism forms the key feature of our proposal, because it reduces patients' access definition process. In addition, the proposed privacy preserving technique derives the inherent properties from initial privacy ranking (which are defined by user without much over head) to have high ratio of data control.

The proposed privacy rating-based access control technique presumes a privacy scale composed of three major segments called low segment point (S_{lp}), medium segment point (S_{mp}) and high segment point (Sh_p). These parameters remain constant for defining access ranking for the data and entities of the storage system. The following section of this paper illustrates the algorithm involved in self generated privacy rating. To reduce the system complexity, the proposed privacy rating mechanism consists of discrete modellings like set representation and summation operations. The privacy rating generation is explained in accordance with cryptographic properties like availability, confidentiality and integrity.

Proposed Privacy Enforced Access Control Model

The proposed privacy policy is created and tested based on the privacy parameters that is confidentiality, data availability and data integrity.

Confidentiality

Data confidentiality means that the data are disclosed to only those who are authorized. All the actors involve should be a part of the system. To ensure confidentiality the privacy is set in the following manner.

Case 1: high confidentiality (user privacy policy).

In this case during the scenario when a pharmacist wants information about a patient and if he is trusted (high confidentiality) in this case he first needs to be a part of the system and he should hold a pharmacist account and if he is authenticated by the system at that particular time then he can enter the patient id and view his entire prescription along with the remarks entered by the doctor.

Case 2: medium/low confidentiality (user privacy policy).

In this case when the pharmacist enters the patient id, he will also be asked to enter the additional pin generated by the system based on the relationship set by the primary user (patient).This pin can be static or dynamic. It is automatically generated by the system and is made visible to the user. But in this case to ensure more privacy to the data the actor can only view the prescription data that is marked medium/low in the case record policy.

Case 3: no relationship privacy set.

In this case, he has to sent a request to the primary user (patient) and provided he can view the prescription if the patient gives him access.

Confidentiality is an act of preventing unauthorized access, traditional security system offers confidentiality through cryptographic algorithm. The proposed access control technique binds the electronic data with the system generated privacy ratings to prevent unauthorized access. The protocol maps the privacy rating of an user with the data and determines the access rights.

The confidentiality rating of the algorithm can be illustrated as follows,

Let x, y, z be the number of available data belongs to various privacy ranks, it can be calculated as

$$|C_{\mathrm{l}}| = x, \quad |C_{\mathrm{m}}| = y \text{ and } |C_{\mathrm{h}}| = z$$

$$\mathrm{CR}_{\mathrm{l}} = \prod_{i=1}^{x} Xi \tag{1}$$

$$\mathrm{CR}_{\mathrm{m}} = \prod_{i=1}^{y} Yi \tag{2}$$

$$\mathrm{CR}_{\mathrm{h}} = \prod_{i=1}^{z} Zi. \tag{3}$$

The (1–3) generates and assigns a privacy rating to each data composed under different privacy ranks (where pi operator indicates generation of privacy rating).

Cumulative CR for ranked data:

$$\alpha\{\mathrm{CR}_{\mathrm{l}}\} = \sum_{i=1}^{x} Xi \tag{4}$$

$$\alpha\{\mathrm{CR}_{\mathrm{m}}\} = \sum_{i=1}^{y} Yi \tag{5}$$

$$\alpha\{\mathrm{CR}_{\mathrm{h}}\} = \sum_{i=1}^{z} Zi. \tag{6}$$

To achieve the fine-grained access control by adopting privacy rating, the algorithm further computes mean of the CR by summing the above obtained values (4–6).

Mean confidentiality rating:

$$\mu\{C\} = \left[\left(\alpha\{\mathrm{CR}_{\mathrm{l}}\} + \alpha\{\mathrm{CR}_{\mathrm{m}}\} + \alpha\{\mathrm{CR}_{\mathrm{h}}\}\right)/\text{total number of ranks}\right].$$

Data Availability

Term availability denotes the probability of data, which readily available to the system users. To ensure hardware availability, the proposed technique is executed against the data stored in storage servers. In contrast our privacy rating access control technique determines availability of data (in terms of software availability) by generating a fine-grained privacy value over the stored data.

The data of the primary user is made available to the secondary user if he has high relationship. Relationship is how the primary user has created the policy for his immediate family, my doctor, other doctors, nurses etc. The basic policy high, medium, low, default is a part of the system. In relationship if a particular actor is marked low he can access data only the data that is marked low.

For example when a patient is in a remote area, where he is in need of health care and if the patient is not having proper access to internet or system to define his privacy policy in this case the primary user, i.e., the patient generates a code

Initial step separates the data based on its privacy ranking (low (A_{l}), medium (A_{m}), high (A_{h})), and determines the number of available data in each categories.

Let x, y, z be the number of available data that belongs to various privacy ranks, it can be calculated as

$$|A_{\mathrm{l}}| = x, \quad |A_{\mathrm{m}}| = y \text{ and } |A_{\mathrm{h}}| = z$$

$$\mathrm{AR}_{\mathrm{l}} = \prod_{i=1}^{x} Xi \tag{7}$$

$$\mathrm{AR}_{\mathrm{m}} = \prod_{i=1}^{y} Yi \tag{8}$$

$$\mathrm{AR}_{\mathrm{h}} = \prod_{i=1}^{z} Zi. \tag{9}$$

The (7–9) generates and assigns a privacy rating to each data composed under different privacy ranks (where pi operator indicates generation of privacy rating). Later routine of the proposed algorithm computes cumulating and mean availability raking over the stored data, which is used to define the access control.

Cumulative AR for ranked data:

$$\gamma\{\mathrm{AR}_{\mathrm{l}}\} = \sum_{i=1}^{x} Xi \tag{10}$$

$$\gamma\{\mathrm{AR}_{\mathrm{m}}\} = \sum_{i=1}^{y} Yi \tag{11}$$

$$\gamma\{\mathrm{AR}_{\mathrm{h}}\} = \sum_{i=1}^{z} Zi. \tag{12}$$

To achieve the fine-grained access control by adopting privacy rating, the algorithm further computes mean of the AR by summing the above obtained values (10–12).

Mean availability rating:

$$\mu\{\mathrm{A}\} = \left[\left(\gamma\{\mathrm{AR}_{\mathrm{l}}\} + \gamma\{\mathrm{AR}_{\mathrm{m}}\} + \gamma\{\mathrm{AR}_{\mathrm{h}}\}\right)/\text{ total number of ranks}\right].$$

Data Integrity

Integrity restricts the malicious adversaries from altering the content of the data being distributed over a network.

The proposed privacy rating based access policy identifies integrity component of the electronic health record and safeguards from malicious activities by assigning a privacy rating.

Data integrity means that all data are accurate and not altered by any one during storage. In this for example if the E-R team (emergency response) wants to view the patient data during emergency, this team is by default provided high policy access, since they are the next trusted user of the system. They use the system when the primary user (patient) is not able to change the privacy settings or use the system. This team has the right to enter the name, id of the patient in emergency situation using the special marking module they are given the access to the special search. However, during this type of access, they have to add a remark for viewing the data which improves the data integrity of the patient. All the above privacy policy discussed is a part of the Java-based health care system developed by us.

Integrity rating (IR), can be calculated by identifying the category, in which the data belongs. To maintain the constant integrity rate independent of data size, the proposed privacy rating based access control technique branches the available data into three major groups called validated data set, non-validated data set and not applicable data set:

$$\text{Available data } D = \{D_{\text{v}} || D_{\text{nv}} || D_{\text{na}}\}$$

$$D(|I_{\text{l}}|) = x, \quad D(|I_{\text{m}}|) = y \text{ and } D(|I_{\text{h}}|) = z$$

$$\text{IR}_{\text{l}} = \prod_{i=1}^{x} Xi \tag{13}$$

$$\text{IR}_{\text{m}} = \prod_{i=1}^{y} Yi \tag{14}$$

$$\text{IR}_{\text{h}} = \prod_{i=1}^{z} Zi. \tag{15}$$

Cumulative IR for ranked data:

$$\beta\{\text{IR}_{\text{l}}\} = \sum_{i=1}^{x} Xi \tag{16}$$

$$\beta\{\text{IR}_{\text{m}}\} = \sum_{i=1}^{y} Yi \tag{17}$$

$$\beta\{\text{IR}_{\text{h}}\} = \sum_{i=1}^{z} Zi. \tag{18}$$

To achieve the fine-grained access control by adopting privacy rating, the algorithm further computes mean of the IR by summing the above obtained values (16–18).

Mean integrity rating:

$$\mu\{\text{I}\} = \left[\left(\beta\{\text{IR}_{\text{l}}\} + \beta\{\text{IR}_{\text{m}}\} + \beta\{\text{IR}_{\text{h}}\}\right) / \text{ total number of ranks}\right].$$

Performance Evaluation

This section discusses the set of results generated by the proposed privacy rating based access control model. The core part of this section explains, how the cryptographic parameters like confidentiality, integrity and availability is achieved in accordance with the system generated privacy ratings. Also to abide with user-centric model, the proposed technique allows user to define privacy ranks for the data involved without much overhead to the user.

All the actors involved in the health care system are rated from 0 to 10 of privacy rating (PR). Based on the basic privacy policy high (patient, ERunit), medium (my doctor, family) and low (others) is set. This 0–10 is divided into 3 levels of privacy rating and the actors get classified into various levels. 0–3.3 (low), 3.4–6.3(medium) and 6.4–10 (high).Using this privacy rating (PR) in the case when the doctor is under the low (0–3.3) user privacy policy and the record policy is also marked 0–3.3 then the data is accessible to the doctor. If the doctor is falls between PR 3.4–6.3 then he can view any data that has PR < 3.4 and up to PR = 6.3. If the doctor falls between PR 6.4–10 then he can view any data < PR 6.4 and up to PR 10. This is done to maintain high level of data privacy and accuracy for the users of the health care system. The policy implementation is explained with a scenario, If a doctor wants to view the data of a patient and if the doctor has a PR value of 5.3, then any data that falls between 0 and 5.3 can be viewed by that doctor:

$$\text{Privacy Rating (PR) of data, } \text{PR}_{\text{d}} = [\,\mu\{\text{A}\} + \mu\{\text{I}\} + \mu\{\text{C}\}\,]$$

$$\text{Privacy Rating (PR) of user, } \text{PR}_{\text{u}} = \left[\left\{A_{\text{u}} + I_{\text{u}} + C_{\text{u}}\right\} / \text{ total number of ranks}\right].$$

Access rights can be granted by comparing PR_{u} and PR_{d} with the early defined privacy rankings. Whereas A_{u} remains the availability rating of the user and C_{u} be the confidentiality rating determined based of the data owner–data consumer relationship, I_{u} be the integrity rating of the user, which is assigned based on type of data defined during case sheet generation.

If Data 1 = 3.3
Data 2 = 4.5
Data 3 = 6.7

Data 4 = 1.2

Like this if each data have a PR value assigned first for calculation: Step 1: any data that have PR above 5.3 is eliminated.

Step 2: sum up all the values below the PR value below 5.3 (3.3 + 4.5 + 1.2) = 9.0

Step 3: divide the sum value by 3(9.0/3) = 3

Step 4: if this value is ≤ 5.3 then it is made available to the doctor and any data > 5.3 is not available, since it is more secured.

All the privacy parameters are assigned a PR value and it is classified into 3 levels as below:

1. Availability: primary user (patient) = 6.4–10
   My doctor, family = 3.4–6.3
   Others = 0–3.3
2. Confidentiality: based on the users high = 6.4–10, medium = 3.4–6.3, low = 0–3.3
3. Integrity: the data are classified as validated data (6.4–10), non-validated data (3.4–6.3) and not applicable data (0–3.3)

Figure 2 describes that the level of confidentiality over various data samples increases with the increase in privacy rating. For instance, a physician who wants to generate the case sheet for the data (*D*) submitted by his patient, the system calculates the privacy rating for the *D* and compares it with the PR value of physician. If $PR_d = 5.3$ and $PR_u = 3.5$, the confidentiality rating to the data depends on the PR_d value. Hence the physician who has PR of 3.5 will not be able to access the submitted health data *D*, because confidentiality directly proportionate with the PR value of data (*D*).

Traditional privacy preserving techniques offers low integrity against the large sized data; this scenario may due to poor robustness in the algorithm. Figure 3 depicts the integrity variations of traditional privacy systems. Ubiquitous computing model forms the primary implementation of the health care application to offer high scalability and flexibility hence physicians deal with large group of patients which ultimately results in large sized case sheets. Traditional privacy models conclude integrity with the policy of graceful degradation (i.e., level of integrity applied over case sheets degrade with the increase in size of patient data). As novelty, our privacy rating based access control technique offers uniform integrity level independent of the data size.

This result is achieved by dividing the data into three major types called validated, non-validates and non-applicable data sets. Figure 4 shows that the proposed model offers constant integrity level for the any data amount of data, which is crucial for achieving fine-grained access control. In accordance with Fig. 4, if a physician generates a case sheet for a particular patient, system divides the case sheet into three forms namely validated, non-validated and not

Fig. 2 Confidentiality vs privacy rating

Fig. 3 Integrity vs availability of traditional systems

applicable based on the privacy ranking of the data. The proposed model assigns integrity rating to the each component of data sheets by adopting the principle of cumulative and mean distribution to achieve uniform integrity level independent of data size.

In addition, privacy rating-based access control limits the amount of data available to the user based on their privacy ranking. Figure 5 shows that for a user with very low privacy rating can be made available with less amount of data. This implementation prevents unwanted access to the user's data, thereby fine-grained access control mechanism is achieved. In the proposed system, for example Alice (a friend of Bob, who is primary data owner) makes a request to access Bob's health sheet with the system.

As a result system calculates privacy rating for the requested data and compares it with Alice's PR value before granting the access permission.

If the PR value of Alice equals 6.7 and PR_d equals 3.2, the system makes only less amount of Bob's health data to be available to Alice. Figure 6 describes overall relationship between privacy rating with confidentiality, integrity and availability.

Thus, from the result analysis done, it is concluded that the proposed privacy model provides high confidentiality,

Fig. 4 Integrity vs availability of proposed model

Fig. 6 Privacy vs availability

availability and data integrity. The dependence of which is depicted in Fig. 6.

Conclusion and Future Work

In this paper, a privacy enforced model for enhancing privacy in cloud-based healthcare systems is proposed for providing privacy preserved access control to the data owner. For this, we have used the relationship for setting the privacy for the data. Mainly, we have classified the policy users as low ranked, medium ranked and highly ranked system users similarly the system divides data is classified as validated, non-validated and not applicable data.

In addition, simple discrete mathematical modelling was involved to reduce the system overhead during the access granting mechanism. By considering the ubiquitous computing environment, the privacy rating based privacy policy defines well suited access control over data in correspondence with the parameters like confidentiality, availability and integrity is maintained by the proposed privacy protocol. Implementation results shows that privacy rating act as a governing body to maintain other access control parameters.

As a part of our future work, the proposed privacy rating based access control policy can be enhanced with two-way SMS service for achieving remote healthcare. In addition, to offer an enhanced access policy, configurable API application can be modelled to integrate as part of the system.

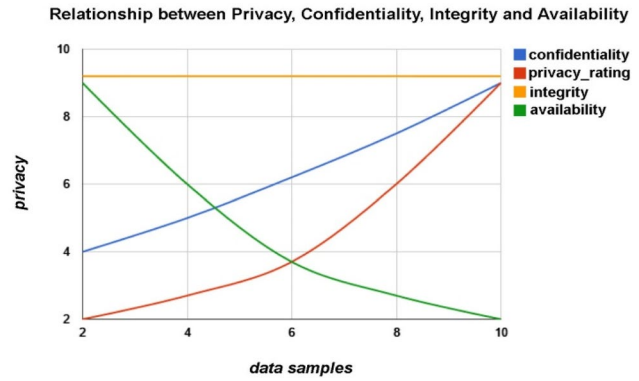

Fig. 5 Relationship between privacy, confidentiality, integrity and availability

Compliance with Ethical Standards

Conflict of Interest The authors declare that they have no conflict of interest.

References

1. Pervasive computing http://www.webopedia.com/TERM/P/pervasive_computing.html (2012). Accessed 3 Sep 2012.
2. Goldschmidt PG. HIT and MIS: implications of health information technology and medical information systems. Commun ACM. 2005;48:68–74.
3. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. Proc IEEE Symp Secur Privacy. 2007;2007:321–34.
4. Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with nonmonotonic access structures. Proc ACM Conf Comput Commun Secur. 2007;2007:195–203.
5. Cheung L, Newport C. Provably secure ciphertext policy ABE. Proc ACM Conf Comput Commun Secur. 2007;2007:456–65.
6. Goyal V, Jain A, Pandey O, Sahai A. Bounded ciphertext policy attribute based encryption. Proc ICALP. 2008;2008:579–91.
7. Liang X, Cao Z, Lin H, Xing D. Provably secure and efficient bounded ciphertext policy attribute based encryption. Proc ASIACCS. 2009;2009:343–52.
8. Zou X, Dai Y, Doebbeling B, Qi M. Dependability and security in medical information system. In: Proceedings HCII 2007, LNCS 4553; 2007. pp. 549–558.
9. Bobba R, Khurana H, AlTurki M, Ashraf F. PBES: a policy based encryption system with application to data sharing in the power grid. Proc ASIACCS. 2009;2009:262–75.

10. Sanchez D, Batet M, Viejo A. Utility-preserving privacy protection of textual healthcare documents. J Biomed Inform. 2014;2014:189–98.
11. Yang J-J, Li J-Q, Niu Y. A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Gener Comput Syst. 2015;2015:74–96.
12. Xiao Y, Shen X, Sun B, Cai L. Security and privacy in RFID and applications in telemedicine. IEEE Commun Mag. 2006;44(4):64–72.