Available online at: http://www.ijmtst.com/vol3issue12.html

International Journal for Modern Trends in Science and Technology

ISSN: 2455-3778 :: Volume: 03, Issue No: 12, December 2017

Privacy Preserving Approach for Accessing Electronic Health Records with Deteriorating Risk

V.K.Saxena[1] | Shashank Pushkar[2]

[1]Vikram University, Ujjain, M.P, India.

[2]Birla Institute of Technology, Mesra, Jharkhand, India.

To Cite this Article

V.K.Saxena and Shashank Pushkar, "Privacy Preserving Approach for Accessing Electronic Health Records with Deteriorating Risk", *International Journal for Modern Trends in Science and Technology*, Vol. 03, Issue 12, December 2017, pp.-30-38.

ABSTRACT

In the healthcare field, preserving privacy of the patient's electronic health records has been an elementary issue. Numerous techniques have been emerged to maintain privacy of the susceptible information. Whereas acting as a first line of defense against illegal access, traditional access control schemes fall short of defending against misbehavior of the already genuine and authoritative users; a risk that can harbour overwhelming consequences upon probable data release or leak. This paper introduces a novel risk reduction strategy for the healthcare domain, so that, the risk related with an access request is evaluated against the privacy preferences of the patient who is undergoing for the medical procedure. The proposed strategy decides the set of data objects that can be safely uncovered to the healthcare service provider such that unreasonably repeated tests and measures can be avoided and the privacy preferences of the patient are preserved.

Keywords: *Risk, Privacy preservation, Electronic Health Records, Risk reduction, HIPAA.*

I. INTRODUCTION

The electronic health records (EHR) [1, 2] of the patients include detailed information concerning their health issues and medical history in the healthcare field. The records comprise susceptible data, such as previously diagnosed health diseases and drug maltreatment, of which the patient would prefer to keep confidential. Distribution of such data, whether persistently or unintentionally, could invite grave harmful implications for the corresponding patient. Adverse consequences could range from social disgrace, complications in getting employment or health insurance policies and so forth [3]. In attempts to bring patients more restraint over their EHRs, legislations such as the Health Insurance Probability and Accountability Act (HIPAA) has been developed. Therefore, the privacy of such records must be protected and, hence, has been under intensive research analysis [5-8].

When the privacy of the medical records is being preserved, numerous techniques can be utilized. Normally, as shown in Figure 1, privacy can be managed by using cryptography, anonymization, or policy methods [9]. Anonymization techniques contain, utilizing statistical measures to conceal the identity of the patient amongst other patients before the data is uncovered to the data requestors and is generally used for discharging huge quantities of medical data for analytical purposes

[10, 11]. Cryptography techniques exertion by utilizing security measures such as encryption mechanisms to protect the susceptible records [12, 13]. Finally, policy methods preserve the patient's privacy by employing rules and constraints for authenticating and authorizing access to the private data [14, 15]. As a result, preserving privacy of a scrupulous patient, who is currently undergoing a medical diagnosis or procedure, cannot be realized through means of anonymization methods because identity is lost among multiple datasets. Therefore, the feasible solution, in such circumstances, requires utilizing cryptography or policy methods or even a combination of the two [9].

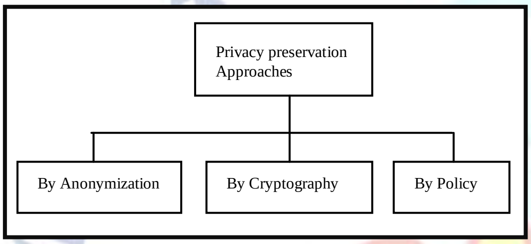

Figure 1. Different Privacy Preserving approaches

Access control technique is one of the major processes for preserving privacy of the medical records. This technique is elementary security mechanism that works by assessing an access request against a set of constraints and rules before finally granting or denying such access to system resources [12]. Several types of access control exist in the literature with different features: Mandatory Access Control (MAC) [12], Role Based Access Control (RBAC) [15-19], Attribute Based Access Control (ABAC) [20] and so on.

While access control can act as a first line of defence against illegal access by denying such access request, it is unable to defend against misuse of system resources by users who have been granted access [21]. In the medical scenario, healthcare professionals can abuse their access rights with regards to patients' private health records; which could increase the risk of potential leakage of the sensitive information. In the United States, the Department of Health and Human Services has conducted an investigation with regards to patients' electronic health records in UCLA (University of California, Los Angeles) hospital and found that they have been excessively viewed by medical staff without a valid reason [22].

In order to overcome the potential misuse of already authorized users, access control schemes can be amplified with risk assessment measures. One important measure is calculating the reliability of an access appellant. Reliability can be determined by several means. One way of calculating trust is by analyzing the user's past behaviour towards a system resource in order to grant or deny future access demand [23]. In effect, the access control scheme becomes more adaptable and dynamic in responding to access requests due to the variability of the trust level of the access requestor, as opposed to traditional access control schemes [21, 24].

When Risk assessment measures are incorporated with access control techniques, a risky access demand can be allowed, rather than be denied, if it is within the tolerable thresholds. However, risk reduction strategies must be applied to lower the risk associated with such an access [25, 26]. Risk reduction techniques are obligatory actions [27, 28] that are performed to minimize the risk of access request such as increasing the security measures, performing anonymization to the datasets or employing system alerts and notifications [29].

This research tackles the issue of preserving privacy of the patient's EHR by incorporating a risk assessment element. More specifically, a risk reduction technique is proposed to lower the risk associated with an access request initiated by a healthcare professional to a particular patient's health record. That is, when a risky access request is made, the proposed technique will expose the patient's relevant and less sensitive data. Therefore, the risk reduction strategy is risk-aware and privacy preserving in addition to being HIPAA compliant.

This paper is intended as follows: section two shows the background information that act as the foundation of the research. Section three presents the related work. The proposed risk reduction strategy is analysed and described in section IV. The paper concludes with the discussions of related work in section V.

II. PRELIMINARIES

A. The Health Insurance Probability and Accountability Act (USA)

The HIPAA [4] is a United States legislation, which provides rules and regulations for securing the electronic medical records for the ultimate goal of preserving the patient's privacy. The legislation consists of multiple titles. However, title II of the act is concerned with regulations for safeguarding the health records' transactions and distribution. Under title II, the Privacy Rule of the HIPAA describes national standards in order to preserve privacy of the patients. In effect, the rule prohibits healthcare professionals from releasing the patient's medical data, to third parties, without an explicitly written permission from the corresponding patient. Furthermore, access to the patients' medical records without a legitimate reason should not be allowed since it violates the privacy of the patient. However, in situations where the access of the patient's stored medical data is deemed necessary in order to further advance the current medical treatment, the HIPAA allows the medical professionals access to such records. Finally, the legislation describes penalties and fines upon violating the privacy rules stated therein.

B. *Risk Assessment in information Security*

In their detailed risk assessment guide, the National Institute for Standards and Technology (NIST) [26] describe the method by which risk assessment is conducted. According to the definitions stated in the guide, should an entity be vulnerable to a certain threatening event, the risk is defined as a function of the likelihood of the threat and its potential impact. That is:

$$\text{Risk} = \text{Likelihood} * \text{Impact} \qquad (1)$$

III. RELATED WORK

A. *Risk-aware Access Control Models*

Risk Aware Access Control schemes (RAAC) [30] are considered as a dynamic and adaptable new type of access control models due to their inherent features of incorporating methods of risk assessment. In such models, the access is permitted or denied based on the outcome of a risk assessment function. When an access request is considered as risky but within acceptable intervals, risk reduction methods can be exploited such that the risk incurred of such access is minimized.

The National Institute of Standards and Technology has developed a general risk-based access control model according to the models proposed by [31]. Several elements are incorporated to assess the risk; namely; operational need, situational factor and risk measures. A conceptual model for risk-aware attribute based access control [24] has been proposed based on these earlier works. Generally, risk-aware access control models proposed in the literature utilize the NIST definition [26] of risk assessment and calculation where a risk is evaluated as the function of a threat likelihood multiplied by the associated impact [32-38]. The subject requesting access to particular object are both associated with security clearances or weights of which are then incorporated with the calculation of risk. Access control models that use trust evaluations can be generally divided into two categories: static trust evaluations [34] and dynamic trust evaluations [36, 39]. Nonetheless, once a risky access request is allowed, risk should be lowered down to acceptable level using risk reduction techniques; an option that is employed by a subset of models.

B. *Risk Reduction Techniques*

Risk reduction in access control models are obligations that are usually required to be performed in order to lower the potential impact of a risky access request [27, 28]. Risk can be reduced by several means such as utilizing anonymization techniques [40, 41, 44] for protection against potential vulnerabilities, increasing security measures of the system by increasing the length of encryption keys or imposing a set of rules and required actions. Such obligations, of which all are supervised by the system, need to be satisfied by the user *before* or *after* access is granted [29]. Figure 2 illustrates risk reduction approaches that can be employed.

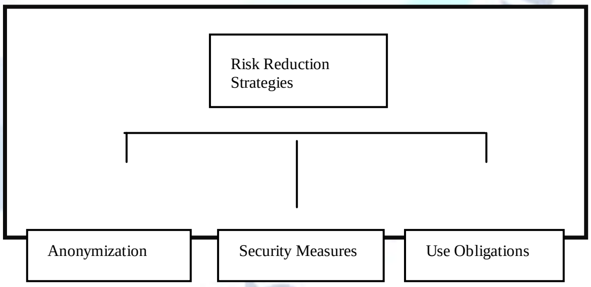

Figure 2. Risk reduction strategies for minimize the riskiness of an access request

IV. THE PROPOSED RISK REDUCTION STRATEGY

A. *The proposed risk reduction strategy*

1) *System Components*

1.1) *Trust calculation*

In order to assess the risk incurred of an access request, trust level of the requesting entity must be calculated and later it is evaluated in the other components. Trust is generally defined as forecasting an entity's future access, based on its historical behaviour [23]. Trust can be evaluated in several ways, such as mining past behaviour, using recommender systems to associate a subject with a recommended trust level or, more statically, assign security clearances for each entity by the system administrator [42].

Since, trust calculation is application specific and the system administrator can choose the appropriate trust model based on the requirement of the system, the proposed system in this work assumes that trust values have already been computed and ready for evaluation by the risk reduction system. Nevertheless, one of the widely known trust calculation and evaluation methods that analyze the user's past behaviour in order to assist in making decisions regarding future access requests is the Subjective Logic model [42]. In the model, the trust level of a user is computed using probabilistic methods that utilize Bayesian principles. An entity, *u*, requesting access to system resource, *i*, is given a trust or opinion representation that has been formed by entity *w*. that is, the opinion formed by *w* about access requestor *u* with regards to *i* is represented by the following tuple:

$$w^{w}_{u:i} = (b^{w}_{u:i}, d^{w}_{u:i}, u^{w}_{u:i}, a^{w}_{u:i})$$

Where

$$b^{w}_{u:i} + d^{w}_{u:i} + u^{w}_{u:i} = 1, \mathit{and}\ a^{w}_{u:i} \in [0,1]. \qquad (2)$$

In the above formula, $b^{w}_{u:i}, d^{w}_{u:i}, u^{w}_{u:i}$, represent the degree of *belief*, *disbelief* and *uncertainty* of entity *w* with regards to trusting system resource *i* to *u*. Furthermore, $a^{w}_{u:i}$ represents the a priori or base knowledge of entity *w* regarding *u* when no previous history is currently available; a typical situation when new users come into the system.

In order to allow for dynamicity, the trust levels need to be updated according to the perceived behavioural evidence. To update the trust values, two parameters are introduced: $r^{w}_{u:i}$ and $s^{w}_{u:i}$. The former parameter calculates the number of positive actions, while the later calculates the negative ones. Based on these parameters, the ultimate trust level of an entity requesting access can be updated using the following equations:

$$b^{w}_{u:i} = \frac{r^{w}_{u:i}}{r^{w}_{u:i} + s^{w}_{u:i} + 2}$$

$$d^{w}_{u:i} = \frac{s^{w}_{u:i}}{r^{w}_{u:i} + s^{w}_{u:i} + 2}$$

$$u^{w}_{u:i} = \frac{2}{r^{w}_{u:i} + s^{w}_{u:i} + 2} \qquad (3)$$

Based on the above equations, the initial situation where there exists no behavioural history for the user, the values are:

$$b^{w}_{u:i} = 0, d^{w}_{u:i} = 0, u^{w}_{u:i} = 1 \quad \mathit{and} \quad a^{w}_{u:i} = 0.5$$

1.2) Disease Relevance Matrix

The purpose of the disease relevance matrix (DRM) is to provide relevance information for the different diseases. That is, for the set of *n* diseases, D$_1$, D$_2$, D$_3$,…, D$_n$, two diseases are relevant to one another if they have a positive relevance value. As illustrated in Figure 3, diseases D$_1$ and D$_3$ are correlated and relevant to each other because they have a positive relevance value. Relevance between the different diseases can (2) obtained using several approaches. One effective approach, as proposed in [43], is to mine for correlation information inside the database of the hospital. In their approach, the system maintains a log for all access requests that have been made on the patients' medical records for serving medical purposes, such as disease diagnosis purposes and so forth. Therefore, the access request information between the different patient records and the medical purposes to which they have been requested for access are available and used as observation instances. The relevance function, $f_n(r, p, t)$, calculates the total number of access requests that have been made by a healthcare professional *r* to the patients' health records of type *t* in order to serve a medical purpose *p*. Similarly, the function $f_n(r, p, t)$ yields the total number of access requests made by all healthcare professionals classified under the same group, G_r, and who have made access requests to medical records of type *t* in order to serve purpose *p*. maintaining such information is crucial in order to assist in calculating and inferring correlation information between the different diseases. That is, if a medical record, of which is classified under type *t*, is being frequently accessed to serve some purpose *p*, and then it can be inferred that there exists a degree of correlation and relevance between the two and vice versa. Such relevance information is realized by means of utilizing Bayesian principal of independence as follows:

$$P(i/X) = P(i/r,p,t) = \frac{P(i)P(r/i)P(p/r,i)P(t/p,r,i)}{P(r,p,t)} \qquad (4)$$

Where $P(1|X)$ denotes that the access request is relevant

While $P(0|X)$ denotes that the access request is not relevant.

The parameter *P*(i) yields the percentage of access requests that have been made in the past. The estimation of *P*(r|i) can be found by calculating the total number of access requests made by entity *r*. However, to solve the issue when the entity requesting access is new in the system, smoothing methods can be applied by incorporating the total number of access requests made by the entire entities belonging to the same group. Therefore,

$$P(r/i) = \frac{\alpha f_n(r,i) + (1-\alpha) f_n(G_r,i)}{f_n(i)} \qquad (5)$$

Where $\alpha \in [0,1]$

Similarly, the estimation of P(p/r,i) and P(t/p,r,i) is

$$P(p/r,i) = \frac{\beta f_n(p,r,i) + (1-\beta) f_n(p,G_r,i)}{\beta f_n(r,i) + (1-\beta) f_n(G_r,i)} \qquad (6)$$

And

$$P(t/p,r,i) = \frac{\gamma f_n(t,p,r,i) + (1-\gamma) f_n(t,p,G_r,i)}{\gamma f_n(p,r,i) + (1-\gamma) f_n(p,G_r,i)} \qquad (7)$$

Where $f_n(p, r, i)$ computes the total number of access requests that have been made by entity *r* to serve medical purpose *p*, and $f_n(t, p, r, i)$computes the total number of access requests for patients' records of type *t* of which have been made by entity *r* in order to serve purpose *p*.

In effect, the proposed analytical approach can decide whether an access request, made on a certain patient record, is relevant to the healthcare provider's own profession, as in Equation (6). Moreover, the approach can decide whether an access request made on the patient's record is relevant to the medical purpose associated, such as the purpose of diagnosing some disease as in Equation (7), which, effectively, can establish the relevance between the different types of diseases. Such correlation information can be stored in the Disease Relevance Matrix and updated frequently.

	D_1	D_2	D_3	…	D_n
D_1	1	0	1	…	…
D_2	0	0	1	…	…
D_3	1	1	1	…	…
…	…	…	…	…	…
D_n	…	…	…	…	…

Figure 3. Disease Relevance Matrix: two data objects are correlated if they have a positive intersecting value

1.3) Patient Privacy Preferences

The privacy preferences for disease disclosure are obtained by the corresponding patient when they fill out their medical forms and, afterwards, entered into the system by healthcare staff. Therefore, each previously diagnosed, and stored, disease is associated with a privacy preference consulting how sensitive this data is with regards to the patient. In effect, for two disease objects *oi* and *oj*, having the corresponding sensitivity weights *wi* and *wj*, scaled between [0, 1], if *wi* > *wj* then disease object *oi* is considered as more sensitive than disease *oj*, and vice versa.

1.4) The Risk Measure Formula

The risk measure formula is a mathematical equation, which will be developed in the future, of which assesses the riskiness of an access request to the patient's relevant data according to the trust level, t, of the doctor, and the privacy preferences,$\{w_1, w_2, \ldots, w_n\} \in W$, of the patient.

B. The Risk Reduction Strategy

In the proposed risk reduction strategy, every access request by healthcare professionals, to the patients' private data, need to be evaluated for potential risks. As illustrated in Figure 4, a doctor is treating a particular patient for a health issue. To avoid potential repeated tests and medical procedures as well as help assist in making better diagnostic decisions, the doctor issues an access request to the patient's stored health records. Upon receiving the access request, and to be consistent with HIPAA privacy rule, the risk reduction strategy operates by retrieving the patient's set of diseases that have a positive relevance to the current diagnostic effort alongside the corresponding sensitivity weights. Once such data is obtained, the Data Combination Risk Calculator, which applies the Risk Measure Formula, searches for the appropriate patient data combinations, those are, later, evaluated against the trust level of the doctor for potential data disclosure. Evidently, for two patients, who are being treated by the same doctor, and who also have the same set of already diagnosed and stored diseases, but with different privacy preferences, the output of the proposed risk reduction strategy will be different and tailored to each situation such that quality healthcare service is delivered without undermining the privacy preferences of each patient.

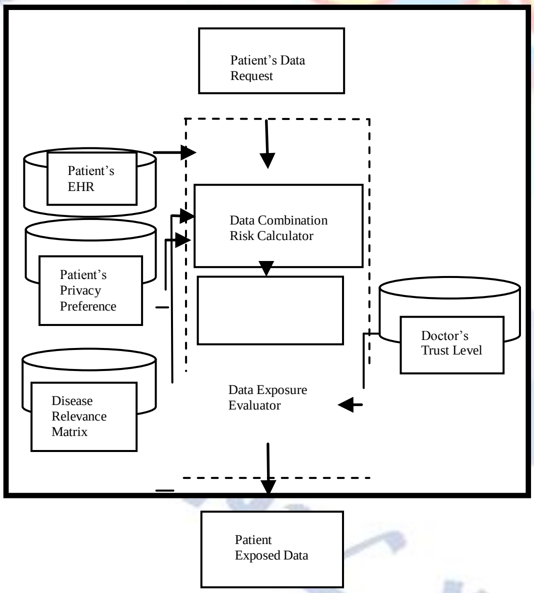

Figure 4. System Components of high-level architecture for proposed risk mitigation strategy

Figure 5 illustrates, in more detail, the activities and actions performed by the proposed Risk Reduction Strategy. When the system finds a set of relevant diseases from the patient's data to which a doctor requests access, the system computes the possible data combinations in a reverse manner. That is, the system begins by generating and computing the Risk Measure values for the combination that includes the total number of diseases, *n*. If the resulting Risk Measure value exceeds the trust level of the doctor, the system reiterates and generates data combinations of fewer numbers of diseases, by excluding one disease at a time and computing the Risk Measure value incurred, and so forth. The goal is to find the maximum possible number of diseases with maximum Risk Measure value. If such data combination is found and the risk incurred is below the trust level of the doctor, the data is then exposed and disclosed to the doctor. However, if the system fails to find a suitable relevant data combination for the doctor's trust level, then the data is regarded as highly private and an explicit consent must be obtained from the patient.

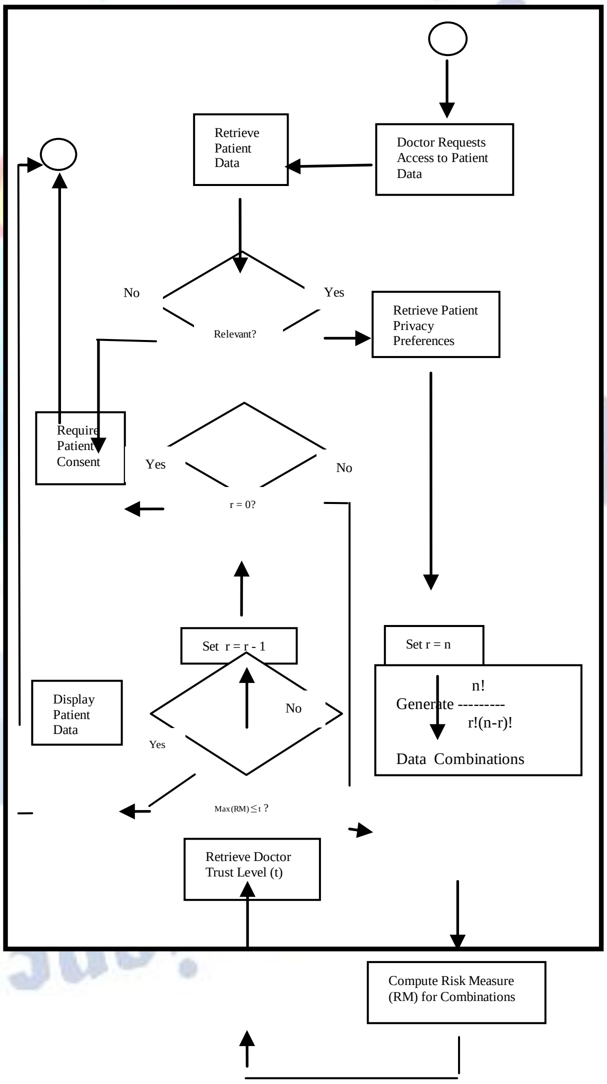

Figure 5. Main actions performed by the proposed risk reduction strategy, where n denotes the total number of the patient's relevant diseases obtained by the DRM.

V. CONCLUSION

In the field of healthcare, preserving privacy of the EHR of the patients has been a most important issue. Numerous approaches have been suggested and implemented to undertake the issue of preserving privacy by means of risk assessment and estimation. In addition, risky access request can be allowed by performing a suitable reduction technique.

In electronic health record, there is a significant need to design privacy-preserving systems, following usable and well-organized data search strategies. In the midst of others, reliability and privacy are the two important requirements that may impact the likability of medical records in different HSPs. The reason is, Health Service Program (HSP) may not satisfy the patient safety needs and collecting data from such HSP, while aggregating data from all HSPs to create patient medical history will impact its reliability. In e-health, trust can be established based on the quality and reliability of HSP, health professionals and data standard. Researchers have been pursuing the goal of achieving semantic interoperability of EHRs to allow sharing of medical data across healthcare organizations, but it has not been realized yet. There is a need for improvement of standardization frameworks that hold data integrity and incorporate integrated EHR schema and common semantics, to allow data sharing across health information exchanges. Digital devices from mobile phones to smart cards and RFID tags are becoming more and more everywhere.

Rapid advancements in mobile technologies and applications resulted in new opportunities for the incorporation of mobile health into existing e-health services. This emphasizes on the need of designing insubstantial privacy-preserving e-health protocols which is suitable for resource-constrained devices. There are a number of open research issues in the field of privacy enabled e-health systems supporting varied environment including: (i) supporting heterogeneous environment, (ii) supporting different stakeholders by allowing different types of access and usage control, (iii) support for crisis conditions, (iv) trust and reputation modeling, (v) interoperability, (vi) data integrity, (vii) traceability of illegitimate distribution, and malicious users.

In this regard, the paper introduced a risk reduction strategy, which controls the access to the patient's susceptible data. These data is based on the dependability of the requesting healthcare contributor, which is according to the privacy preferences and represented as sensitivity weights, of the patient.

REFERENCES

[1] E. P. Ambinder. Electronic health records. Journal of Oncology Practice, 2005, vol. 1, p. 57.

[2] What is an electronic health record (EHR)? 2016. Available: https://www.healthit.gov/providers-professionals/faqs/ what-electronic-health-record-her

[3] T. C. Rindfleisch. Privacy, information technology, and health care. Communications of the ACM, 1997, vol. 40, pp. 92-100.

[4] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

[5] Y. Yang, C. T. Liu, and T. W. Tseng. Design and Implementation of a Privacy Aware Framework for Sharing Electronic Health Records. International Conference on Healthcare Informatics (ICHI) 2015, pp. 504-508.

[6] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang. A Medical Healthcare System for Privacy Protection Based on IoT. Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), 2015, pp. 217-222.

[7] R. M. Salih and L. T. Lilien. Protecting users' privacy in healthcare cloud computing with APB-TTP. Pervasive Computing and Communication Workshops, IEEE International Conference, 2015, pp. 236-238.

[8] J. Zhou, X. Lin, X. Dong, and Z. Cao. PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System. IEEE Transactions on Parallel and Distributed Systems, 2015, vol. 26, pp. 1693-1703.

[9] J.-J. Yang, J.-Q. Li, and Y. Niu. A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Generation Computer Systems, 2015, vol. 43, pp. 74-86.

[10] L. Sweeney. k-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, vol. 10, pp. 557-570.

[11] R. Agrawal and C. Johnson. Securing electronic health records without impeding the flow of information. International Journal of Medical Informatics, 2007, vol. 76, pp. 471-479.

[12] W. Stallings and L. Brown. Computer Security: Principles and Practice, 2014, Pearson Education.

[13] W. Gasarch. A survey on private information retrieval. 2004, in Bulletin of the EATCS.

[14] F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli. Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security (TISSEC), 2001, vol. 4, pp. 224-274.

[15] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-based access control models. Computer, 1996, pp. 38-47.

[16] J. Reid, I. Cheong, M. Henricksen, and J. Smit. A novel use of RBAC to protect privacy in distributed health care information systems. in Information Security and Privacy, 2003, pp. 403-415.

[17] W. Lampson. Protection. ACM SIGOPS Operating Systems Review, 1974, vol. 8, pp. 18-24.

[18] G. S. Graham and P. J. Denning. Protection: principles and practice. in Proceedings of the May 16-18, 1972, spring joint computer conference, 1972, pp. 417-429

[19] R. Sandhu, D. Ferraiolo, and R. Kuhn. The NIST model for role-based access control: towards a unified standard. in ACM workshop on Role-based access control, 2000.

[20] C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone. Guide to attribute based access control (ABAC) definition and considerations (draft). NIST Special Publication, 2013, vol. 800, p. 162.

[21] Q. Wang and H. Jin. Quantified risk-adaptive access control for patient privacy protection in health information systems. in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, 2011, pp. 406-410.

[22] M. Hennessy-Fiske. UCLA hospitals to pay $865,500 for breaches of celebrities' privacy. Los Angeles Times. April, 2016. Available: http://articles.latimes.com/2011/jul/08/local/la-me-celebrity-snooping-20110708

[23] Josang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision. Decision support systems, 2007, vol. 43, pp. 618-644.

[24] S. Kandala, R. Sandhu, and V. Bhamidipati. An attribute based framework for risk-adaptive access control models. in Availability, Reliability and Security (ARES), 2011 Sixth International Conference on, 2011, pp. 236-241.

[25] G. Stoneburner, A. Y. Goguen, and A. Feringa. Sp 800-30. Risk management guide for information technology systems. 2002.

[26] Guide for Conducting Risk Assessments. National Institute of Standards and Technology, NIST Special Publication 800-30, September 2012. Revision 1.

[27] K. Irwin, T. Yu, and W. H. Winsborough. On the modeling and analysis of obligations. in Proceedings of the 13th ACM conference on Computer and communications security, 2006, pp. 134-143.

[28] M. Pontual, O. Chowdhury, W. H. Winsborough, T. Yu, and K. Irwin. On the management of user obligations. in Proceedings of the 16th ACM symposium on Access control models and technologies, 2011, pp. 175-184.

[29] Díaz-López, G. Dólera-Tormo, F. Gómez-Mármol, and G. Martínez-Pérez. Dynamic counter-measures for risk-based access control systems: An evolutive approach. Future Generation Computer Systems, 2016, vol. 55, pp. 321-335.

[30] J. P. Office. Horizontal integration: Broader access models for realizing information dominance. MITRE Corporation Technical Report JSR-04-132, 2004.

[31] R. McGraw. Risk-adaptable access control (radac). in Privilege (Access) Management Workshop. NIST–National Institute of Standards and Technology–Information Technology Laboratory, 2009.

[32] N. Dimmock, A. Belokosztolszki, D. Eyers, J. Bacon, and K. Moody. Using trust and risk in role-based access control policies. in Proceedings of the ninth ACM symposium on Access control models and technologies, 2004, pp. 156-162.

[33] L. Zhang, A. Brodsky, and S. Jajodia. Toward information sharing: Benefit and risk access control (BARAC). in Policies for Distributed Systems and Networks, 2006. Policy 2006. Seventh IEEE International Workshop on, 2006, pp. 9 pp.-53.

[34] P. C. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner, and A. S. Reninger. Fuzzy multi-level security. IEEE Symposium on: an experiment on quantified risk-adaptive access control in Security and Privacy, SP'07. 2007, pp. 222-230.

[35] Q. Ni, E. Bertino, and J. Lobo. Risk-based access control systems built on fuzzy inferences. in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, 2010, pp. 250-260.

[36] Burnett, L. Chen, P. Edwards, and T. J. Norman. TRAAC: trust and risk aware access control. in Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on, 2014, pp. 371-378.

[37] Kamwan and T. Senivongse. Risk of privacy loss assessment of cloud storage services. 18th International Conference on Advanced Communication Technology (ICACT), 2016, pp. 105-111.

[38] H. Khambhammettu, S. Boulares, K. Adi, and L. Logrippo. A framework for risk assessment in access control systems, computers & security, 2013, vol. 39, pp. 86-103.

[39] L. Zhou, V. Varadharajan, and M. Hitchens. Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage. IEEE Transactions on Information Forensics and Security, 2015, vol. 10, pp. 2381-2395.

[40] Armando, M. Bezzi, N. Metoui, and A. Sabetta. Risk-aware information disclosure. in Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance, Springer, 2015, pp. 266-276.

[41] H. Taneja and A. K. Singh. Preserving Privacy of Patients Based on Re-identification Risk. Procedia Computer Science, 2015, vol. 70, pp. 448-454.

[42] Josang, R. Hayward, and S. Pope. Trust network analysis with subjective logic. in Proceedings of the 29th Australasian Computer Science

Conference-Volume 48, 2006, pp. 85-94.

[43] Q. Wang and H. Jin. An analytical solution for consent management in patient privacy preservation. in Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium, 2012, pp. 573-582.

[44] Shaden Al-Aqeeli, Mznah Al –Rodhaan, and Yuan Tian. Privacy Preserving Risk Mitigation Strategy for Access Control in E-Healthcare Systems. International Conference on Informatics, Health & Technology (ICIHT), 2017, published in IEEE Xplore.