A hybrid solution for privacy protection and data security issues in E-Health

QI Fangzhong[2], SHEN Chao[2], ZHOU Gengui[2]

Abstract. With the rapid development of e-health, the privacy protection and data security of patients' related data have been paid more and more attention. Previous studies have proposed some solutions to prevent such data from unauthorized users, but there are still some shortcomings especially in terms of meeting data storage, transmission and access requirements. In this paper, issues about security and privacy of patients' related data are discussed, and current solutions to the problems of data security in e-health are compared and analyzed.Requirements for data security including storage, transmission and access security are analyzed. Solutions based on Message Authentication Code, Digital Watermarking and Role-based Access Control Model are introduced respectively for data security and privacy protection in E-health. Patients' related data are divided into four levels and the roles of E-health platform are defined as four categories. And therefore, a hybrid solution to the security problem in E-health is proposed, and its effectiveness has been demonstrated in a wearable device scenarios. This solution can improve the security mechanism of an E-health system.

Key words. E-health, Data Security, Privacy Protection, Wearable Device.

1. INTRODUCTION

The rapid development of Internet and wireless communications technologies makes people's lives become more and more convenient. One of the most important changes takes place in E-health, which was involved from telemedicine. The World Health Organization defines e-health as 'the use of information and communication technologies (ICT) for health' [1]. It can break the geographical and time barrier to share bio-signal information to provide clinical support.

There are several problems in traditional health care. Because the record of patients is paper based, it is hard for medical personnels to provide special treatment based on the medical history. Patients cannot get effective treatment because of

[1] Acknowledgement - This work was funded by the National Natural Science Foundation of China(71371169).

[2] Workshop 1 - College of Economics and Management, Zhejiang University of Technology, Hangzhou, 310023, China

time and space constraints, while doctors are often faced with increasingly heavy workload. The emergence of e-health can address these problems to some degree. The face to face diagnosis is no longer that important. Doctors can get information about the vital signs of patients through wireless technology(i.e. ICT). It provides possibility for doctors to monitor patients' health status remotely and continuously in real time [2].

How the patient data can be passed to doctors through ICT? Figure 1 briefly illustrates the architecture of this process. Each patient is equipped with a wearable device, in which it has a wireless sensor node.

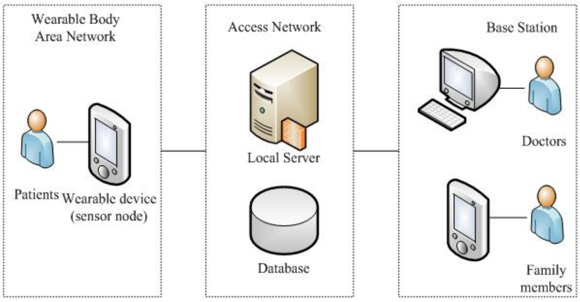

Fig. 1. A simple architecture of E-health.

The whole procedure can be divided into three parts, namely sensing, processing and transmitting. The node will detect vital signs of patient, location, even temperature and humidity [3]. A local server, which is Internet-enabled Personnel Data Assistant, will gather these patients' related data. The local server processes data, including aggregation and distributed storage. And then the server will establish communication channel and transmit data to base station.The base station will keep record of data. Doctors or family members, who have access to patient related data, can query information from database.

The studies on data security and privacy protection in e-health area are multiple in recent years. There have been a lot of approaches on e-health information protection. Miller et al and Barrows et al focus on the study of protecting patient's record information [4, 5]. They illustrated the characteristics of patient's record information and proposed an idea that social supervision mechanism was very important in protection of patient's information, unfortunately, there were no protection measures from technical aspects.

According to the studies of Boonyarattaphan et al, authentication and data transmission framework play an important role in E-health data securtiy, and they suggested that different encryption algorithms and advanced authentication mechanism should be involved to improve the protection situation of E-health data, however, no detailed mechanism about access control was proposed [6-9]. Sandhu et al illustrated an application of access control and introduced different access control models, including their strengths and weakness, while they did not focus much on the application of such model in the e-health environment [10-12].

Previous studies have proposed some solutions to prevent patients' related data from unauthorized users, but there are still some shortcomings in terms of meeting the storage, transmission and access requirements of these data. In this paper, by analysing the data security and privacy protection issues and investigating the data security requirements in E-health area, we aim to propose a hybrid solution for privacy protection and data security problems in E-health.

The paper is organised as follows. Section 2 discusses the data security and privacy protection issues in E-health area. Section 3 analyses the specific requirements for data security in E-health, including storage, transmission and access security. Section 4 presents solutions to the current data security and privacy problems, and introduces the application of a hybrid solution. In section 5, we present our main conclusions.

2. DATA SECURITY AND PRIVACY PROTECTION ISSUES IN E-HEALTH

With the rapid development of E-health, various data security and privacy problems have caused widespread concern. Patients begin to pay more and more attention to the security and privacy of their health related data.

Data security means protecting data or confidential information from unwanted actions and destructive forces of unauthorized users in software systems and networks. It also means the data is safely stored and transferred. Data privacy means only specific data can be obtained by people who have authorization. Several threats may cause data security and privacy problems and make the data at risk [13]. Figure 2 shows the major threats to data security and privacy in E-health applications.

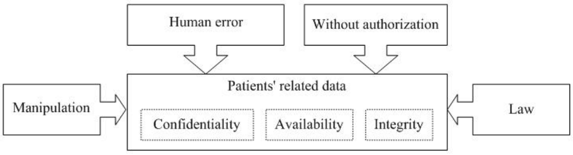

Fig. 2. Major threats to data security and privacy.

Patients' related data has three attributes, namely confidentiality, availability and integrity. Vulnerabilities of law and manipulation pose threats to these properties, but human error and unauthorized access are equally threats to these properties.

2.1. Data security issues

Doctors give treatment to patients based on data stored in the database. If the patients' related data is not securely stored or transferred, doctors will make inaccurate diagnosis. If the data security cannot be provided, the value of E-health will be lost greatly, especially for emergency care, which is an important area in E-health. It is ironic when doctors need to do first aid treatment but cannot find any information about the patient. Patients use wearable devices for saving life not for beauty [14].

2.2. Privacy protection issues

From a sociological point of view, data privacy is just like other personal privacy. Protecting health data privacy, like any other personal privacy, shows respect to the patients, especially for those patients who have devastating diseases, such as Aids, Hepatitis etc. Any leakage of this information may lead to discrimination from companies when patient applies a job. It will pose threat to social harmony and may cause social problems and even increase crime rate.

From a business point of view, as the most important resource, patients' related data means profits for commercial companies, especially for hospitals and pharmaceutical companies. Attackers will find various means to steal personal information and sell them to companies. Information leakage poses virious threats on patients: they are often rejected when apply assurance, are severely distracted by commercials, are deceived by cheaters to buy fake medicine, or even are destroyed by opponents who use diseases as weakness to make attack.

Once E-health is involved in security or privacy scandal, it will impact the development of E-health technology and application which will bring lasting benefit for society. From either personal or social angle, the data security and privacy in e-health should be dealt effectively [15].

3. REQUIREMENTS FOR DATA SECURITY IN E-HEALTH

3.1. Requirements for data storage security

The electronic health records, which are detected by wireless sensor nodes, are highly sensitive. It includes a lot of important patient-related data. In order to prevent the patient records from variously malicious intrusion, the requirement of data storage should be highly standard.

For the security reason of the E-health records, the USA and other European countries issued regulations successively. For example, in America, the Health Insurance Portability and Accountability Act (HIPAA) passed in 1996 to mandate the security and privacy of medical records [16]. The following five aspects are the primary requirements that the storage of e-health records should comply with.

- Integrity: The storage of the electronic health records needs to assure its integrity. In other words, the data must be protected from unauthorized deleting, inserting, or any other kind of modification.

- Confidentiality: It protects data from being accessed by wrong people. There must be a trustworthy encryption to ensure the confidentiality of the data storage device.

- Disposal: There must be a procedure to control the disposal of e-health records storage equipment, such as used data storage device, media or hardware. In addition, if the storage equipment is retrieved or recycled, the rules would be stricter to ensure the data cannot be "recycled" [17].

- Accountability: The elaborate logs are indispensable for maintaining the e-health record in a traceable way. The records of the origin of the data, access to the data, data modification and data migration should be logged entirely [18].
- Disaster Recovery and Backup: Disaster Recovery and Backup system is essential to guarantee the data retrievable after the damage such as fire, flood, equipment crash, etc. Undoubtedly, the backup or disaster recovery system should be built in a different site from the original one.

3.2. Requirements for data transmission security

During the process of data transmission, it is highly likely that the patient-related data could be intercepted, destroyed or even rewritten. Therefore, the data transmission procedure should adopt the corresponding measures to protect the data from malicious attackers.

- Confidentiality: The data transmission must be encrypt with a secret key that only intended receivers can process key exchange.
- Promptness: Patients' related data generated by wireless sensor nodes should be in real time. Promptness ensures that transferring data is latest and unchanged rather than replayed and old [19].

3.3. Requirements for data access security

Usually, doctors, nurses, patients and other accredited users all have right to access the patients' related e-health data. However, inevitably there are some outsiders who want to access the data without permission. To avoid the irregular access, the requirements for data access are indispensable. The following five aspects are the primary requirements for data access security of E-health records.

- Authentication: Verify the identity of the user who is attempt to access the patient related data. The authentication must base on the authorization policy.
- Authorization: It is critical to form a level-based and role-based authorization policy to ensure all users have their own limitation of the data access.
- Access control: Access control is able to prevent the unauthorized users from touching the data. This control should also be used by the patients, doctors and other authorized users to access the data.
- Availability: The authorized users are able to access the e-health data whenever they need them.
- Non-Repudiation: Guarantee the data access privilege of the data source. In other words, the access request of the data generator should not be denied.

4. SOLUTION FOR DATA SECURITY AND PRIVACY

Since the security and privacy of patients' related data is extremely important in E-health, practical solutions should be come up to meet the above requirements discussed. Figure 3 shows the solutions to confront threats for data security and privacy protection.

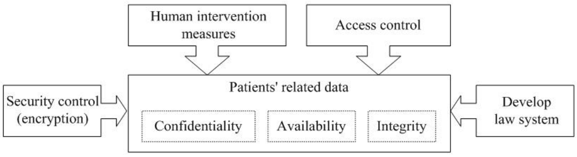

Fig. 3. Solutions to confront threads for data security and privacy.

In this paper, we mainly discuss solutions about security control for data security and solutions about role-based access control for data privacy.

4.1. Solution for data security

Data security in E-health is related to storage and transfer before data is collected into database. The wireless sensor nodes play an important role in this phase. Figure4 presents the architecture in the nodes.

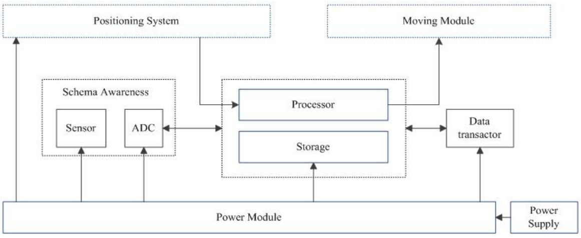

Fig. 4. The architecture of wireless sensor nodes.

The processing module is responsible to process and store data. To provide data security, some methods for information hiding should be applied in this module.

4.1.1. Message Authentication Code The most popular method in recent years for data security is based on Message Authentication Code (MAC) [20]. MAC is a piece of information, which is generated from secret keys and message, and is prepared to be authenticated. One MAC only maps onto one information.

MAC is attached to message, which is used to ensure integrity. It is an effective way to protect data security and to make sure the data is non-repudiation and accountability. However, there are still several problems to use MAC. Firstly, the volume of generated MAC message is a little bit large. It is a burden for wireless sensor node, whose resource is limited. Secondly, the separation between authentication node and message poses threat to manage and store data. Finally, MAC is mainly used in wireless sensor network. It cannot provide protect for off-line sensitive data, which is also important in E-health. Another technique should be applied in E-health to improve data security.

4.1.2. Digital Watermarking In digital watermarking, identification information (i.e. a piece of information, which is called digital watermarking) is embedded in plain text. In E-health, wireless sensor nodes collect a wide variety of data, which is not equally important for patients and doctors. Considering about the work load of wireless sensor nodes, not all those data deserve same encryption in aspect of complexity. Therefore, patients' related data are divided into four levels as shown in table 1. The classification and the degree of importance represent the complexity of algorithms to compute digital watermarking.

Table 1 Classification of patients' related data

Levels	**Data Description**	**Complexity of Encryption** **(a higher value indicates more complicated)**
Level 1	Account information	4
Level 2	Bio-signal information	3
Level 3	Location & Time	2
Level 4	Other data	1

For data in each classification, before it is transferred, a digital watermarking, which is computed by algorithms of this classification, is embedded by the processor in wireless sensor node. When server receives the process data delivered from wireless sensor nodes, server will analyze the classification of data. It extracts digital watermarking by extraction rules and computes the digital watermarking again using plain text. If the two pieces of digital watermarking identification information are same, the data will be stored and transferred securely.

Digital watermarking cannot only perform function to preserve data integrity, like MAC, it also takes other advantages. Digital watermarking is computed by Hash Function. Firstly, because of the properties of Hash Function, it can effectively provide data security. Secondly, digital watermarking technique merges plain text with identification information, which improves data elusiveness. Thirdly, data of different level use different complicated digital watermarking, which lighten the load of wireless sensor nodes. It is highly beneficial for limited resource of sensor nodes.

4.2. Solution for data privacy protection

To protect the e-health data privacy is not simple to prevent the data from being abused by third parties, but to authorize the right of controlling e-health their own data to users.

Current research on e-health data privacy protection focuses on two layers. The first layer is authentication and authorization, which is very common in data privacy protection mechanism [21]. The second layer is access control which is based on the first layer. Since the amount of data acquisition object is relatively huge, permission management plays a vital role in protecting the data privacy. In permission management, access control is the core content to achieve it. Because the patient related data is sensitive and private, two layers' protection should be applied.

4.2.1. Authentication and Authorization Authentication is based on various security measures including digital signature, password or biometric identification technology to verify the identity and authorization of users. Authorization, which is based on authentication, is used to authorize the request from verified users to ask for visiting server and resource appropriate permissions. Authentication and authorization mutually cooperate to identify the user identity in opened network environment.

Authentication normally can be divided into three categories: artificial articles (IC card and security card), digital password and biometric characteristics (fingerprints and iris). Each of them has their own advantages and disadvantages.

IC card is easy to use but it is also easy to lose and duplicated by illegal persons. And for digital password, the common authentication method is static password, however, because users normally could not be able to manage their passwords and meanwhile the passwords always have compulsory rules and phase change, it becomes hard to implement password mechanism and also the password becomes vulnerable due to malicious attack. Even for the biometric characteristics verification method, which is popular in various areas in recent years, there are still potential risks. For example, artificial finger could blind the fingerprint identification system. Therefore, a variety of combined authentication measures should be applied to improve the privacy of E-health data.

4.2.2. Access Control Access control refers to the defensive measures concerned with unauthorized use of resources. In other word, the user entering the database should be under control and is only permitted to access assigned resources. The access control under E-health environment aims to prevent the unauthorized visit and unauthorized use, letting the related users to use the E-health data in a specific scope. The basic principle of access control is illustrated in Fig. (5).

In the diagram, the roles of access control are divided into subject and object, with an access control implementation module connecting each other. The access control implementation module takes the responsibility of controlling the access right when the subject visits the object. Based on this module, the e-health system can determine whether subject is permitted for certain operation.

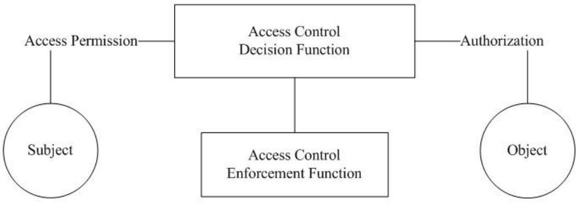
Access Permission
Access Control Decision Function
Authorization
Subject
Access Control Enforcement Function
Object

Fig. 5. The principle of access control.

Based on the authorization policy, access control model can be divided into three categories [22].

DAC permits the subject to impose specific restriction on access control, while MAC forbids the subject to interfere the process of access control. The problem of DAC is that it authorizes too much power to the subject, which may contribute to information leak and low defense capabilities facing Trojan horse attack. Meanwhile, MAC is normally applied in a narrow application field, which is very inflexible and lacks of holistic control in data privacy protection.

TBAC manages the privacy and security issue from application and enterprise level and introduces a very important concept—task. TBAC builds security model and mechanism based on the view of task oriented. The core idea of TBAC is combining the access right with task. In the process of task execution, when the authority is consumed, the subject could no longer visit the object. Thus, the authority given to user is not only related to subject and object, but also associated with the current task status, changing all the time according to the context of executing tasks. Because of the activity and dynamics of TBAC, it is broadly applied in workflow, distributed computing and multipoint access control information.

The core idea of RBAC is to directly authorize the access right to the role rather than the subject. The access right of subject is distributed through role mechanism. Because the role is relatively stable compared to the subject and could give more perceptual understanding, it is very suitable to be used in E-health data privacy protection. Fig. (6) shows a basic model of RBAC.

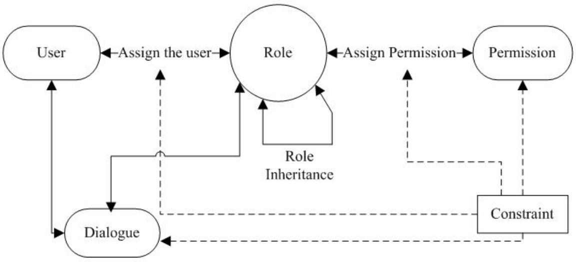

Fig. 6. A basic model of RBAC.

The basic RBAC model consists of three entities: user, role and permission. More specifically, access permission and role is mutually correlated, different roles have different permission. The resource that a user can access is depended on the user's role. Meanwhile, RBAC has the principle of least privilege, meaning that the user's power could not exceed the permission when doing the work. And last but not the least, in specific time period, some roles can only be granted to specific amount of users, which can be set at the beginning of creating the role.

In E-health environment, we should not simply focus on the protection of patients' related data privacy, restricting any visit from unauthorized users. Conversely, we should apply suitable privacy protection mechanism to maximize the value of these e-health data in a controllable level. Meanwhile, based on the characteristics of e-health data, traditional access control mechanism could no longer satisfy the needs and if the data volume kept expanding, the database storing this data would hard to manage and maintain. However, RABC is a suitable solution for addressing this problem. On one hand, the data owners desperately desire that their physical privacy would not be abused and sequentially bring inconvenient trouble to their normal life. On the other hand, since the development of data mining technology enormously improve people's normal life, the health related data could also be accumulated and then deeply analyzed to produce healthcare solution for those who needed it. By allocating and cancelling user's role to achieve the allocation and cancellation of user's permission, making the user and access permission separated logically. In the coming part, we present a hybrid solution which focuses on the role hierarchy management issues.

4.3. A hybrid sulution and application

In a real application scenario, each user has his or her own user account and could have multiple roles in an E-health platform. For example, a user could simultaneously be a health data acquisition object, manager of the hospital, doctor or even other roles. The whole platform is centered on the data acquisition object; other roles are designed to serve the data acquisition object.

In the E-health platform, we define the roles into four categories: Platform Administrator, Agency User, Data Acquisition Object, Family and Friends.

- Platform Administration: platform administration is in charge of the daily management work, including creating new users and giving permission for other hospitals and health care centers that use the platform.

- Agency User: agency user includes the main members of hospitals and other health care centers. They are in charge of daily medical management, mainly referring to doctors and nurses.

- Data Acquisition Object: data acquisition object includes medical service object and data collection object. Data Acquisition Object normally is added to the platform by Platform Administration. And also the doctors and nurses can be invited to the nursing group for data acquisition object.

- Family and Friends: these two roles are invited to the nursing group by the data acquisition object given the permission to visit the detailed information for data acquisition object.

Since RBAC does not directly authorize the permission to the user, but firstly authorize the permission to the roles and then give the user specific role. This will make the permission management process simply. Fig. (7) shows a basic flow of permission management.

The focus of RBAC application in E-health environment is to solve the access control problem that different users can only access different data. In the E-health platform, data acquisition object can create a nursing group including Platform Administration, Agency User, Family and Friends, and only the people in the nursing

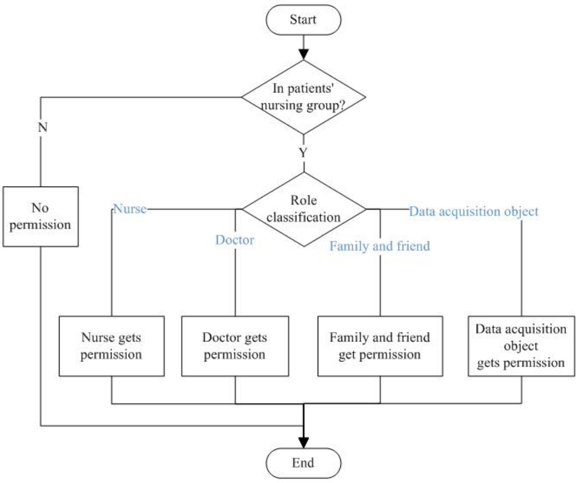

Fig. 7. A permission management process.

group can check the E-health information of data acquisition object, and different roles of users have different access permissions for the health related information. In details, firstly, if a user wants to access the health information of certain data acquisition object, he must be involved in the nursing group of the object. Secondly, different roles are granted different access permission to the E-health information, for example, the user who has the role of doctor would have different access permission from the user who has the role of nurse, and this setting is accomplished by the platform administration. While the Family and Friends role is set by the data acquisition object.

5. CONCLUSION

In E-health, the data security and privacy protection of patients' related data is one of the most important part for the development of E-health. From the aspect of treatment, sociology and business, failure to protect data security and privacy will cause several problems. To meet the requirements of data storage security, data transmission security and data access security, practical solutions to these problems should be provided. In this paper, we introduce Message Authentication Code and Digital Watermarking method for data security. Digital Watermarking can overcome some disadvantages of Message Authentication Code. It divides data into four levels and use different complicated algorithms to generate digital watermarking information. Some scientific experiments should be conducted to statistically show the advantage of Digital Watermarking. We introduce a Role-base Access Control for data privacy protection in E-health. We also propose a hybrid solution in which a gross clarification of roles is conducted in RBAC, and introduce a permission management process of its application. Meanwhile, the proposed model has been tested in real situation with changeable environment.

References

[1] *World Health Organization, WHO eHealth Resolution.* http://www.who.int/healthacademy/news/en/, (2005).

[2] G. Eysenbach: *What is e-health?.*Journal of medical Internet research *3* (2001) No. 2, 68-68.

[3] M. Li, W. J. Lou, K. Ren: *Data security and privacy in wireless body area networks.*IEEE Transaction on Wireless Communications *17*(2010) No. 1,51-58.

[4] A. R. Miller, C. Tucker: *Privacy protection and technology diffusion: The case of electronic medical records.* Management Science *55* (2009) No. 7,1077-1093.

[5] R. C. Barrows, P. D. Clayto: *Privacy, confidentiality, and electronic medical records.* Journal of the American Medical Informatics Association *3* (1996), No. 2, 139-148.

[6] A. Boonyarattaphan, Y. Bai, S. Chung: *A security framework for e-health service authentication and e-health data transmission.* 9th International Symposium on Communications and Information Technology(2009) ,1213-1218.

[7] Y. Jian, S. Chen, Z. Zhang, L. Zhang: *Protecting receiver-location privacy in wireless sensor networks.*26th IEEE International Conference on Computer Communications (2007), 1955-1963.

[8] S. Haller, S. Karnouskos, C. Schroth: *The internet of things in an enterprise context.*Future Internet – FIS 2008, Springer Berlin Heidelberg (2009),14-28.

[9] S. Lim, T. H. Oh, Y. B. Choi, T. Lakshman: *Security issues on wireless body area network for remote healthcare monitoring.* IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (2010),327-332.

[10] R. S. Sandhu, E. J. Coyne, H. L. Feinstein: *Role-based access control models.* Computer *29*,(1996) No. 2, 38-47.

[11] V. Rajendran, K. Obraczka, J. J. Garcia-Luna-Aceves: *Energy-efficient, collision-free medium access control for wireless sensor networks.* Wireless Networks *12* (2006) No. 1, 63-78.

[12] J. B. Joshi, E. Bertino, U. Latif, A. Ghafoor: *A generalized temporal role-based access control model.* IEEE Transactions on Knowledge and Data Engineering *17* (2005) No. 1, 4-23.

[13] A. Appari, M. E. Johnson: *Information security and privacy in healthcare: current state of research.* International journal of Internet and enterprise management *6* (2010) No. 4, 279-314.

[14] M. Meingast, T. Roosta, S. Sastry: *Security and privacy issues with health care information technology.* 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (2006) ,5453-5458.

[15] N. Desai, H. Shahnasser: *A Light Review of Data Security and Privacy Approaches Applicable to E-Health Systems.* The International Conference on Computing Technology and Information Management (2014), 362-367.

[16] *U.S. Department of Health and Human Services, What should be considered before adoption of a health IT system for oral health?.*http://www.hrsa.gov/healthit/toolbox/oralhealthittoolbox/meaningfuluse/considered.html (2000).

[17] R. Hasan, M. Winslett, R. Sion: *Requirements of secure storage systems for healthcare records.* Proceedings of the 4th VLDB conference on secure data management, Springer-Verlag (2007) 174-180.

[18] R. Gajanayake, R. Iannella, T. Sahama: *Privacy by information accountability for e-health systems.* 2011 6th IEEE International Conference on Industrial and Information Systems (2011), 49-53.

[19] I. Solis, K. Obraczka: *The impact of timing in data aggregation for sensor networks.* Proceedings of the IEEE International Conference on Communications (2004),3640-3645.

[20] R. Martí, J. Delgado, X. Perramon: *Security specification and implementation for mobile e-health services.* Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service, IEEE Computer Society (2004),241-248.

[21] S. Han, G. Skinner, V. Potdar, E. Chang: *A framework of authentication and authorization for e-health services.* Proceedings of the 3rd ACM workshop on Secure web services(2006) ,105-106.

[22] J. B. Deng, F. Hong: *Ask-based access control model.* Journal of Software *14* (2003), No. 1, 76-82.

Received November 16, 2017