REPORT OF THE SURVEY NO . 9
TITLE: Research issues for privacy and security of electronic health services
http://dx.doi.org/10.1016/j.future.2016.08.011

Context: this article is about “Research issues for privacy and security of electronic health services” is tired from “Future Generation Computer Systems “, Edited in 2016 and written by the following researchers: Buket Y¨uksel, Alptekin K¨upc¸¨ u, ¨Oznur ¨Ozkasap. The internet access link for this survey is : http://dx.doi.org/10.1016/j.future.2016.08.011 [98]

More and more we want to facilitate services online and even for health, because it has been discovered that many cases of illnesses can reached and healed by the electronic services, but how to secure and assure the privacy for the data used in these services (for patient and professionals) It’s why this article is written. With the prevalence of information and communication technologies, Electronic Health Services (EHS) are commonly used by patients, doctors, and other healthcare professionals to decrease health care costs and provide efficient healthcare processes. However, using EHS increases the concerns regarding security, privacy, and integrity of healthcare data. In this survey, we categorize and evaluate state of-the-art electronic health system research based on their architecture, as well as services including access control, emergency access, sharing, searching, and anonymity methods by considering their cryptographic approaches.

Background: the problems of health are growing every day and costs for healthcare are higher, but because the electronic services increases also, some ways have been found for to facilitate access to healthcare and reduce costs. That’s why we need to define some terms for a better approach of this survey.

Electronic Health Services (EHS) are the different tasks which can be done to facilitate the healthcare by the information and communication technologies (internet, telephone, card …).

More and more the use of Electronic Health services is increasing, for almost all the layers of society (patients, providers, employers, doctors, policy makers, and other healthcare workers)

Let’s take the definition of privacy from Wikipedia [99] which says that Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals, but share common themes. When something is private to a person, it usually means that something is inherently special or sensitive to them. The domain of privacy partially overlaps security (confidentiality), which can include the concepts of appropriate use, as well as protection of information. Privacy may also take the form of bodily integrity.

From the link http://encyclopedia.thefreedictionary.com/security “ we see that Security is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, or organization.

As noted by the Institute for Security and Open Methodologies (ISECOM) in the OSSTMM 3, security provides "a form of protection where a separation is created between the assets and the threat." These separations are generically called "controls," and sometimes include changes to the asset or the threat.

Then with these definitions we can go ahead with the subject, for a better use of the Electronic healthcare services we need to protect and keep the privacy of data patients, secure the data of professionals of health, the data of any actor of these activities.

So, the problem in this survey is that using EHS increases the concerns regarding security, privacy, and integrity of healthcare data. Then, in this survey it’s about to find the solutions for more secure and keep in privacy these data.

Electronic health services are increasingly used by patients, doctors, and other healthcare professionals. Although using EHS has several advantages, it brings several privacy, security, and integrity problems together.

As research questions:

About architecture:

In a distributed health data architecture, how does the EHS efficiently inform the patients about who is using their data and why?

In a cloud environment, how can patients be sure that their privacy is protected by cloud providers?

Which data is allowed to be disclosed for statistical analysis by cloud providers?

For Access control:

1. Which access control methods are the most efficient for the EHS?
2. Which access control method is more efficient for the emergency situations?

About sharing and emergency features:

1. In an emergency case, when selective sharing is used in the system, how can the system decide which data should be disclosed to the responsible healthcare professionals?
2. In an emergency situation, how can patients allow the healthcare personnel to reach their health information?
3. Without assuming a healthcare trusted authority exists, how can it be possible to use smart cards in emergency situations?815
4. How can biometrics be used by patients in an emergency situation?
5. How can we create an EHS that satisfies both source verifiability and selective sharing properties?

For Search functionality some questions like:

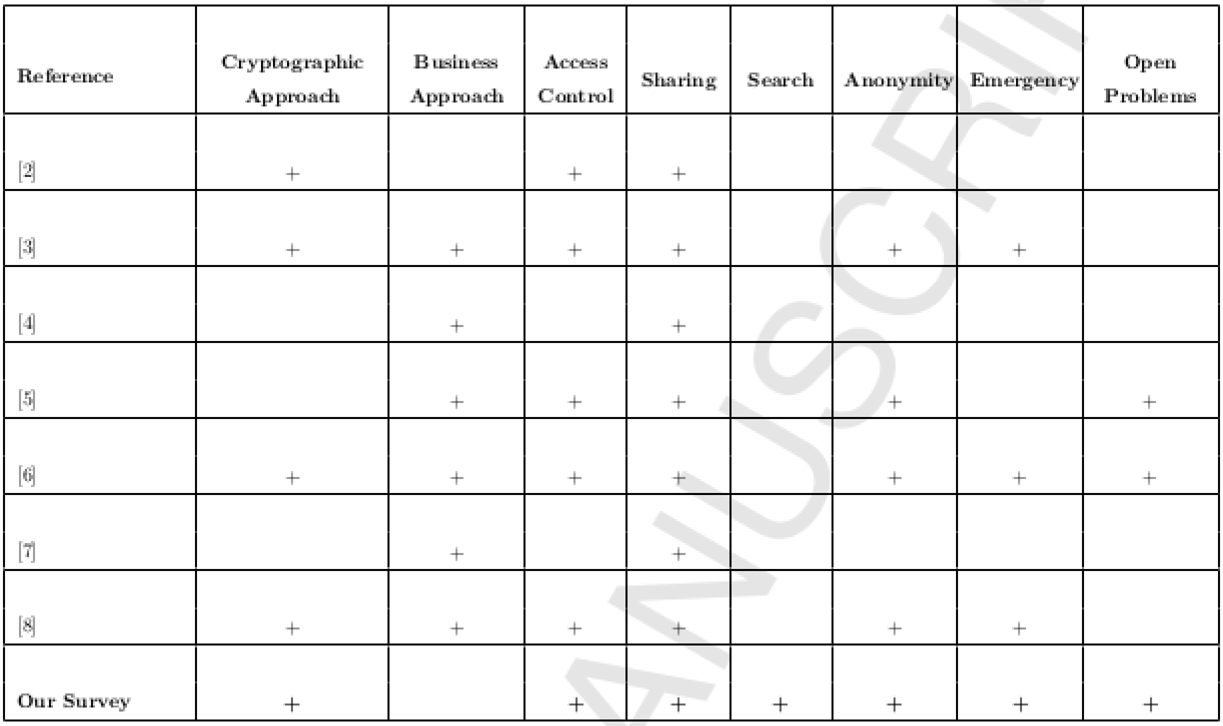
1. Can it be possible to create a privacy-concerned search method different than the proxy encryption and PEKS methods?
2. Is it possible to create collusion-safe proxy encryption scheme?
3. Is it possible to develop a proxy encryption scheme that uses semi-trusted or untrusted servers?

Concerning Anonymization:

1. How can we provide unlinkability for patients’ attributes in EHS?
2. Is it worth the cost to use onion routing algorithms to provide communication anonymity in EHS?
3. How can differential privacy techniques be applied to EHS, while845 obtaining meaningful results?

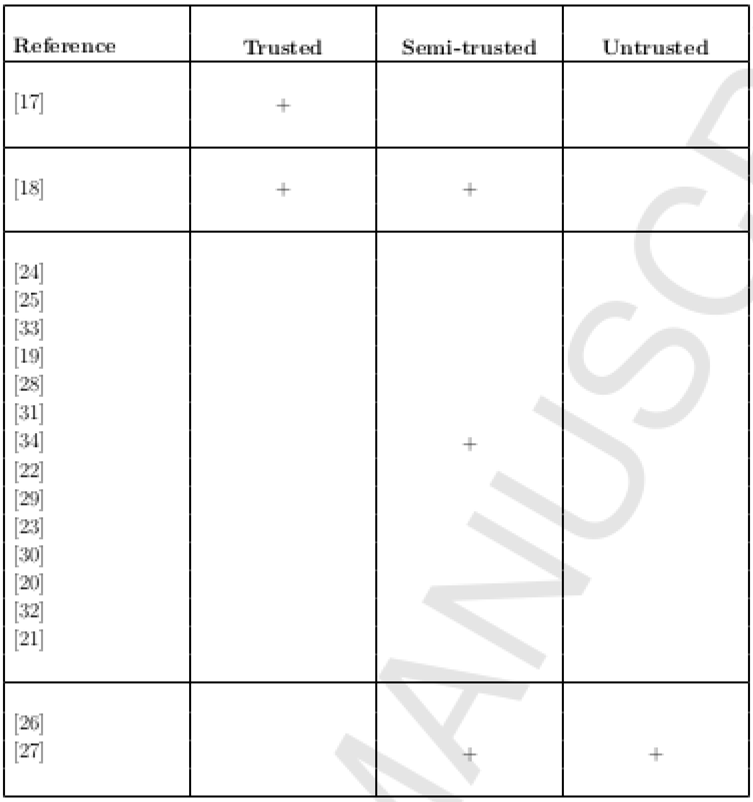
Related works

Comparisons with the other EHS related surveys



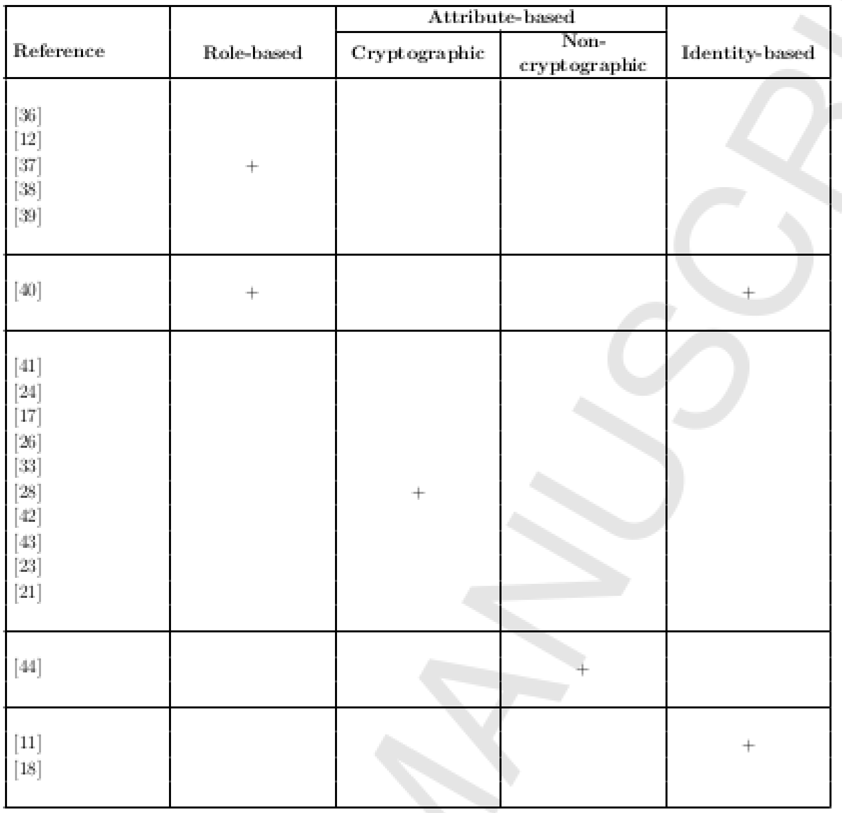
Reference	Cryptographic Approach	Business Approach	Access Control	Sharing	Search	Anonymity	Emergency	Open Problems
[2]	+		+	+				
[3]	+	+	+	+		+	+	
[4]		+		+				
[5]		+	+	+		+		+
[6]	+	+	+	+		+	+	+
[7]		+		+				
[8]	+	+	+	+		+	+	
Our Survey	+		+	+	+	+	+	+

Server types in cloud architecture



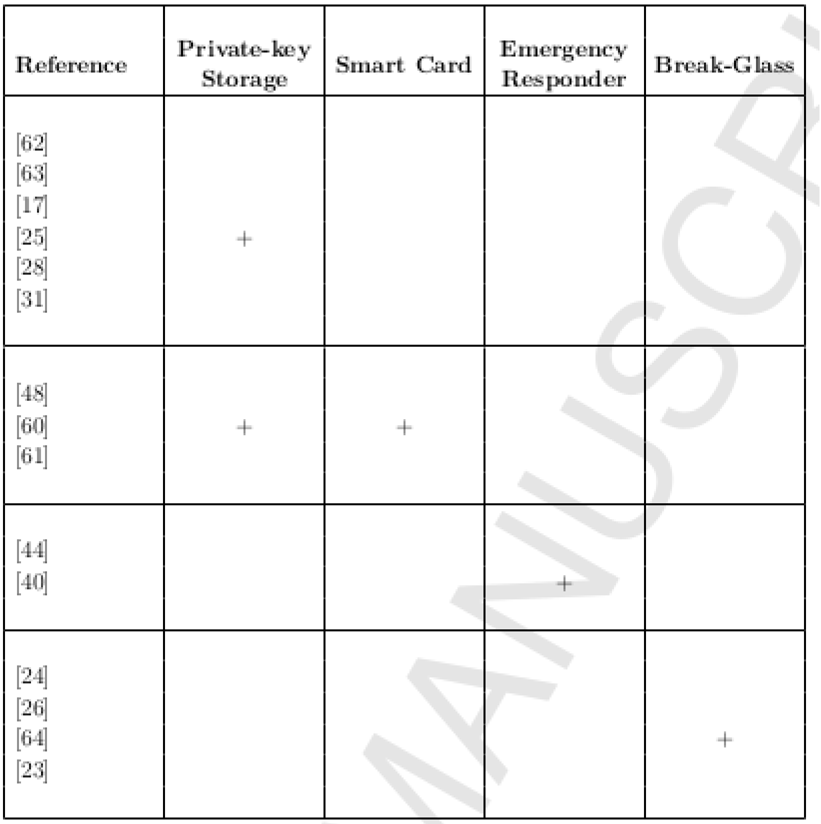
Reference	Trusted	Semi-trusted	Untrusted
[17]	+		
[18]	+	+	
[24] [25] [33] [19] [28] [31] [34] [22] [29] [23] [30] [20] [32] [21]		+	
[26] [27]		+	+

Access Control Techniques in proposed EHS



Reference	Role-based	Attribute-based		Identity-based
		Cryptographic	Non-cryptographic	
[36] [12] [37] [38] [39]	+			
[40]	+			+
[41] [24] [17] [26] [33] [28] [42] [43] [23] [21]		+		
[44]			+	
[11] [18]				+

Emergency Case Methods in proposed EHS



Reference	Private-key Storage	Smart Card	Emergency Responder	Break-Glass
[62] [63] [17] [25] [28] [31]	+			
[48] [60] [61]	+	+		
[44] [40]			+	
[24] [26] [64] [23]				+

METHODOLOGY EMPLOYED

firstly we have Accepted Manuscript.this part content

-the title of survey
-authors of this paper and all date about the appear in paper .then they cite the article.in the last part they describe each steps ,modifications that are leads to the publication to Manuscript.

-Then we have the title and authors of the paper.

-We have abstract
in this part ,they give a brief resume about to this paper and give also keywords

-then we have introduction
in this part we give definition of EHS, their roles and advantages on the security,privacy and integrity of the healthcare.
They explained each methodes and techniques used for ensure security,privacy and integrity in healthcare system.
Then we explained each methode in depth then we have releted works in a table in this table there is referances and their differents methodes applieds.

-Then they give their differents contibutions in this paper.
After this they give an plan that is structured like that :
The remainder of the article is structured as follows. Section 2 presents the review of the architectural aspects of EHS. Section 3 describes the access control techniques proposed for healthcare systems. Section 4 presents the proposed methods for EHS to preserve privacy of the users when an emergency situation happens. Section 5 presents sharing functionality and provides comparisons for the proposed sharing methods. Section 6 presents search techniques that t can be suitable for the application of EHS. Section 7 describes the anonymization approaches of EHS. Finally, Section 8 presents the openresearch problems about e-health services related to privacy, security, andintegrity of the health data, followed by concluding remarks in Section 9.

-in the section 2 we the presentation the review of the architectural aspects of EHS.Here we have
two types of architectures used in EHS, which are distributed and cloud.
Concerning Distributed architecture it refers to a collection of independent computers that each has a role in information processing, but it appears as a single,integrated system to the users.
About cloud they defines cloud like that :Cloud architecture consists of a set of remote servers that allows data storage and online access to data.and they give all the severals types of cloud and explained each of them.in the last time they give in a table the related work about several servers types in cloud architectural.

-in section 3 we have acess control
firsly they gives a brief explication of the acess control as follows :is a way of preventing or limiting access to a resource according to properties and requirements of the system.

And they give the purpose of acess control like that :is that only authorized parties should contact the system and decrypt the data.
Then we have in this part a table that gives an related work about several techniques used or proposed by EHS.then they explained each of them.

-in section 4 we have Emergency Cases and Consent Exceptions.
Primary they focuses on need emergency cases and consent exceptions.they when and how used the emergency cases.and then they explained how to do when occur consent exceptions.
Secondly they gives related work about techniques used in a table.

-in section 5 they talks about sharing health data.
In this part they gives all of the personnes to that patients can share health data and explained the important of the share health data.then we have severals approach and their roles.finaly we have a related work about each approach.

-in section 6 talk about search.
This part the authors talks about search like that :Whenever data is shared, naturally, it is also searched. Searching data in the server is one of the important functions of EHS. Patients' data is encrypted and stored in a server. When patients, doctors, or researchers need to search the data, the server should return not more than the queried data and ideally should not learn anything about the quer.then we have a related work about Search Methods in proposed EHS.

-in section 7 we have Anonymity.
Here they gives meaning of anonymity and its need for many reasons.then we have a related work about Anonymization Methods in EHS.

-in section 8 we have Open Issues and Guidelines.

In this section, they present several research questions about privacy, security, and integrity considering our categories in EHS.

-After the differents section we have conclusion.
In this part the authors shows the importances and avantages of methodes brought by EHS,then they talks about their contrubutions .

-in the last time they gives all the references used in this survey.

Results found and perspectives

results found

unlike to the prior surveys, here we categorize and evaluate state-of-the-art electronic health services considering their cryptographic approaches. This survey is different from previous studies in being method-based and covering all privacy and security approaches proposed for EHS.
We established some categories as architecture, access control, emergency cases, sharing, search, and anonymity methods, and then for each category we explain existing methods and the research based on these methods. To the best of our knowledge, no prior survey has considered search methods in the context of privacy and security. This study systematically covers all aspects and methods of privacy and security in EHS. This work considers general healthcare services including mobile healthcare technologies. This survey particularly addresses for cryptographic approaches of EHS.
We present state-of-the-art approaches regarding security, privacy, and integrity aspects of EHS.
We systematically analyze and evaluate the systems with a method-based approach, and lay out a comprehensive survey of cryptographic approaches of EHS.
We consider components, characteristics, and challenges of e-health services.
We categorize state-of-the-art studies according to their architecture, access control, emergency cases, sharing, search, and anonymity techniques.
We discuss open problems and provide future directions for enhancing security
and privacy of EHS.
we categorized and evaluated research aspects of privacy and security in EHS
and discussed about the open issues based on their architecture and services including access control, emergency access, sharing, searching, and anonymity methods by considering their cryptographic approaches. Among these categories, some of them are more important and critical than the others. Access control is the most important functionality in any EHS. A system without secure and privacy concerned access control techniques cannot be used for sensitive health data. Privacy concerned emergency access methods and anonymity methods are also profoundly important for an EHS. However, sharing and search can be thought as optional functions and their absence does not cause privacy and security problems unlike access control function; they are complementary features increasing efficiency and usability of the EHS. Therefore, while sharing and search are the optional functionalities; access control, emergency access, and anonymity are crucial functions of EHS.

Perspectives :
-the design of a system of alert which inform by an alert to users registred on the system of who is using their data and why.
-create a key secure only accessible for users, not available even for the cloud providers. By this way of serure data, only the users are responsible of their own data and with these keys they can decide who have the right to disclose in an emergency case. For statistical analysis, a module can be created for the recuperation of data with anonymity.
-another perspective for access control would be to do a comparative analysis between the different 3 access control methods used for access control in the purpose to know the most efficient.
For the emergency case, make a scenario in a litterature survey for to obtain the most efficient(rapid access,rapid of best healing, rapid take in charge …)

-As question for perspective, we have the following question :In an emergency case, when selective sharing is used in the system,how can the system decide which data should be disclosed to the responsible healthcare professionals?
-Another perspective would be to make a state of different emergency cases, which would permit to establish the best methods according each case.
-Without assuming a healthcare trusted authority exists, how can it be possible to use smart cards in emergency situations?
How can biometrics be used by patients in an emergency situation?
How can we create an EHS that satisfies both source verifiability and selective sharing properties?

Most important publications for this works

[6] S. Avancha, A. Baxi, D. Kotz, Privacy in mobile technology for personal healthcare, ACM Computing Surveys (CSUR) 45 (1) (2012) 3. 8 times

[42] L. Guo, C. Zhang, J. Sun, Y. Fang, PAAS: A privacy-preserving attribute-based authentication system for ehealth networks., in: Distributed Computing Systems (ICDCS), IEEE 32nd International Conference, 2012, pp. 224–233.7 times

[11] J. Sun, Y. Fang, Cross-Domain data sharing in distributed electronic health record systems, IEEE Transactions on Parallel and Distributed Systems 21 (6) (2010) 754–764. 6 times

[62] J. Benaloh, M. Chase, E. Horvitz, K. Lauter, Patient controlled encryption: ensuring privacy of electronic medical records, in: CCSW, 2009, pp. 103–114. 6 times

[17] S. Narayan, M. Gagné, R. Safavi-Naini, Privacy preserving EHR system using attribute-based infrastructure, in: Proceedings of the 2010 ACM workshop on Cloud computing security workshop, ACM, 2010, pp. 47–52. 6 times

[8] J. L. F. Alemán, I. C. Señor, P. Á. O. Lozoya, A. Toval, Security and privacy in electronic health records: A systematic literature review, Journal of Biomedical Informatics 46 (3) (2013) 541–562. 5 times

[44] A. Mohan, D. Bauer, D. M. Blough, M. Ahamad, B. Bamba, R. Krishnan, L. Liu, D. Mashima, B. Palanisamy, A patient-centric, attribute-based, source-verifiable framework for health record sharing, 2009, Georgia Institute of Technology. 5 times

[40] J. Sun, X. Zhu, C. Zhang, Y. Fang, HCPP: Cryptography based secure EHR system for patient privacy and emergen. 5 times

[18] Y. Tong, J. Sun, S. S. Chow, P. Li, Towards auditable cloud-assisted access of encrypted health data, in: Communications and Network Security (CNS), 2013 IEEE Conference on, IEEE, 2013, pp. 514–519. 4 times

[26] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson, A. D. Rubin, Securing electronic medical records using attribute-based encryption on mobile devices, in: Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, ACM, 2011, pp. 75–86. 4 times

[21] F. Xhafa, J. Li, G. Zhao, J. Li, X. Chen, D. S. Wong, Designing cloud-based electronic health record system with attribute-based encryption, Multimedia Tools and Applications 74 (10) (2015) 3441–3458. 4 times

[23] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Transactions on Parallel and Distributed Systems 24 (1) (2013) 131–143. 4 times

[60] W.-B. Lee, C.-D. Lee, A cryptographic key management solution for HIPAA privacy/security regulations, IEEE Transactions on Information Technology in Biomedicine 12 (1) (2008) 34–41. 4 times

our references :

[99] wikipedia

[98] http://dx.doi.org/ 10.1016/J.future.2016.08.011