International Journal For Technological Research In Engineering
Volume 4, Issue 10, June-2017 *ISSN (Online): 2347 - 4718*

ANALYSIS OF PSEUDONYMIZATION APPROACHES FOR PROVIDING SECURITY IN ELECTRONIC HEALTH RECORD SYSTEMS

P. Nagaraju[1], B. Jaya Sridevi[2], Y. Gopi[3]
Guntur, AP, India

ABSTRACT: Privacy is one of the essential issues in healthcare records machine. Several data protection and access controls mechanisms had been brought like pseudonymization, encryption, anonymization, role based access control model and many others to protect sensitive records. There may be a single pseudonym for a collection of replaced fields or a pseudonym in step with replaced area. The motive is to render the information document much less identifying and therefore lower customer or patient objections to its use. In this paper, we analyze the pseudonymized technique for Electronic Health Record (EHR) system.

I. INTRODUCTION

Many healthcare carters and insurance agencies nowadays have adopted a few shapes of electronic clinical report structures, even though maximum of them store scientific information in centralized databases inside the shape of electronic statistics. Typically, patient may have many healthcare providers, along with number one care physicians, professionals, the rapists, and different scientific practitioners. In addition, patient might also use more than one healthcare insurance organization for special forms of insurances, together with clinical, dental, vision, and so forth. Currently, each provider generally has its very own database for Electronic Medical Records(EMRs). Sharing statistics among healthcare practitioners throughout administrative barriers is translated to sharing facts between EMR structures. The electronic facts sharing between exclusive EMR structures are known as electronic Health Records (EHRs). The interoperation and sharing amongst special EMRs has been extremely gradual. Cost and poor usability were stated as the largest limitations to adoption of fitness IT, especially Electronic Health Records (EHR) systems. Cloud computing presents an attractive IT platform to cut down the cost of EHR systems in terms of each possession and IT renovation burdens for plenty clinical practices. It is broadly identified that cloud computing and open standards are crucial cornerstones to streamline healthcare whether or not it is for preserving health records, monitoring of sufferers, handling sicknesses and cares greater correctly and efficiently, or collaboration with peers and analysis of data. Many predict that handling healthcare. EHR structures are used in place of paper systems to boom physician efficiency, lessen costs (e.g., storage) and scientific mistakes, improve information availability and sharing, etc. An exemplary successful implementation of EHR machine inside the United States is the Veterans Administration healthcare system, with over 155hospitals and 800 clinics. It is one in every of the most important included healthcare information systems international and has been the usage of a single EHR device for years. Despite all of the promising elements, EHR structures aren't adopted by way of most people of healthcare structures. Statistical effects of the real adoption rate of HER in US clinical systems and the references therein. Among all of the limitations to the implementation of EHR systems, privacy and protection concerns on sufferers' medical facts are arguably most dominating. Records stored in a principal server and exchanged over the Internet are subject to theft and safety breaches. The Health Insurance Portability and Accountability Act (HIPAA) inside the US have been established to regulate EHR associated operations.

Pseudonyms are identifiers of subjects. The concern that may be recognized via the pseudonym is the holder of the pseudonym. A critical element for effectiveness of pseudonyms is the unlinkability among the pseudonym and its holder and if pseudonyms may be related among every different. In practical terms, anonymity happens when a person's identity can't be ascertained. An instance of a nameless transaction is one wherein neither participant acknowledges or knows something approximately the other. A widespread disadvantage of anonymity is that accountability turns into tricky and therefore anonymity services are exploitable with the aid of those engaged in crook activities. The highest diploma of anonymity can be reached with little expertise of the linking among the holder of a pseudonym and its pseudonym. Pseudonymity gives a compromise among anonymity and responsibility. A person employing a pseudonym engages in communications and transactions without revealing their identification. In most existing credentials systems a pseudonymous certificates binds a consumer's pseudonym to their public key, the personal key to which the user possesses. Such certificate is issued by way of a relied on company. Identities, pseudonyms and public keys need to be particular.

II. RELATED WORK

WiktoriaWilkowska and Martina Ziefle research turned into inspired through a trade-off among the genuine necessity of novel medical answers within the increasingly getting old populace and the existing expertise hole regarding public recognition of clinical technology in one of a kind contexts of use and numerous person agencies. Two much-discussed problems of scientific generation had been addressed—facts security and privacy. Apart from the prison and technical elements of safety and privacy, we centered at the notion of these aspects, asking beneath which situations customers could take delivery of scientific era and assessing if

customers' gender and fitness repute modulate attractiveness. Focus groups virtually uncovered an excessive attention of the significance of person-focused medical generation development and a high motivation to specific their personal evaluations and fears related with usage. This corroborates that contemporary technology improvement must consist of customers early in order to understand the perceived drawbacks and blessings, and to deal with their reviews in each development and public communique policy. The implementation of electronic health records does not only promises a higher level of service quality for the patients, but also reduces costs for social insurance systems and therefore for the society. As highly sensitive data is stored and handled in nation-wide medical systems, there is the requirement for assuring the patients' privacy to avoid misuse. Although several approaches for managing anamnesis system exist, their underlying security is too weak to assure confidentiality of life-long medical data storage. Moreover people need to be convinced of such centralized systems as they are strongly concerned about their privacy. Bernhard Riedl, VeronikaGrascher, Stefan Fenz, Thomas Neubauer discussed a variety of existing approaches and their security shortcomings, such as their dependence on a centralized patient-pseudonyms list, a life-long pseudonymor the concealment of an algorithm. We worked out several principles with the focus on assuring the confidentiality, integrity, availability and privacy of sensitive patient-related medical data. The existing works encompass the demonstration of the importance of privacy for EHR structures, the authentication based totally on existing wireless infrastructure, the role-based totally approach for access regulations, and many others. As the need for technical info, specifically, the cryptographic awareness of privacy and security in healthcare systems will become extra clear and stringent; a few current works observed this line of studies. Lee and Lee proposed a cryptographic key management solution for privacy and safety rules regarding sufferers' PHI. Patients have control over their PHI and are able to limit access to it. When the medical doctor needs to review the PHI for remedy, he has to achieve agreement or consent from sufferers who will use the proper keys saved on a clever card to decrypt the PHI ciphertexts. The authors then proposed a consent exception answer for emergencies, wherein a relied on server possesses all mystery keys of the patient and consequently can retrieve the PHI undeniable-texts upon emergency. Although technically accurate, the proposed scheme is unreasonable since the trusted server is capable of get right of entry to the sufferers' PHI at any time. As a result, PHI privacy isn't absolutely assured that is unacceptable for extremely touchy records like PHI. Furthermore, the authors did no longer deal with the issues associated with storing and retrieving PHI, which can be elaborate given the privacy requirements.

III. PSEUDONYMIZATION APPROACH

Pseudonymization allows an association with apatient only under specified as well as controlled environments. The various requirements on pseudonyms involve differenttypes of pseudonyms which can be partitioned into two groups:

- Randomly generated pseudonyms
- Pseudonyms chosen by users

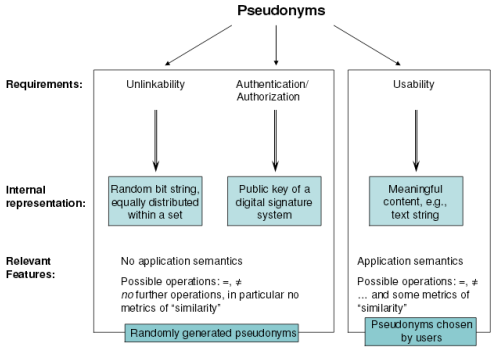

Fig1. Types of Pseudonyms

Randomly generated pseudonyms

Randomly generated pseudonyms, namely arbitrary random bit strings and public keys have similar properties. They are generated by a computer randomly and independently within a set and are completely application independent. If we regard randomly generated pseudonyms as abstract data types, the only operations that are possible for this type regarding link ability are "Equal" and "Not Equal". If two pseudonyms are not equal, they are stochastically independent. An observer cannot draw further conclusions. Particularly, he cannot link different pseudonyms. Even the observation f many of these pseudonyms does not help to identify the user on the long run.

Pseudonyms chosen by users

Pseudonyms selected via customers contain a few context semantics on the grounds that customers introduce a short-hand description for partial identities probably. Thus a person ought to selected pseudonyms which simplify spotting the context in which he has set up the corresponding partial identity or got in contact with it, e.g., the software, the function, the use case, or the communication partner.

IV. PETERSON APPROACH

Peterson claims to provide a system for making available personal medical information records to an individual without jeopardizing privacy. The main ideas behind the approach are (i) the encryption of patient's data, (ii) the universal accessto medical records by any (also unauthorized) person while (iii) the patient is responsible for granting privacy.

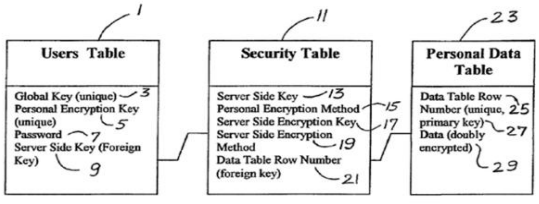

Fig2. Peterson Approach

This approach has of 3 database tables: such as "Security Table" that links the data in the "Data Table" to the appropriate entries in the "User Table" (using attribute data table row number). Data is stored double encrypted in the database.

V. THIELSCHER APPROACH

Thielscher proposed an electronic fitness report device, which uses decentralized keys saved on clever cards. The scientific facts is cut up into identity information and the anamnesis facts and saved in two different databases. The key saved at the patient's smart card is used to link the patient identity to her datasets. Therefore, this key generates a completely unique records identification code (DIC), which is likewise stored inside the database. Such a DIC does now not comprise any facts to perceive character. Data identification codes are shared between the patient and health care providers to authorize them to access the medical dataset. For more security the authorization is limited to a certain time period. After this period any access attempt is invalid.The keys to calculate the data identification code (DIC) are stored on smart cards. In case these smart cards are lost, a fall-back mechanism is provided by Thielscher.

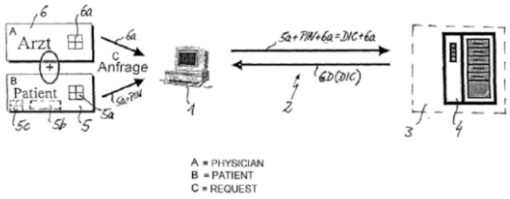

Fig3. Thielscher Approach

Every pseudonym grasped by a patient is stored in a list, which is stored at an off-line computer. In case the smart card is lost or destroyed, this list could be used to re-link the data to the patient.

VI. CONCLUSION

As highly sensitive data is stored as well as controlled in nation-wide medical systems, there is the requirement for assuring the patients' privacy to avoid misuse. However, several approaches for managing anamnesis systems exist; their underlying security is too weak to assure confidentiality of life-long medical data storage. In this paper, we analyzed about the pseudonymization approaches to improve the security of the Electronic Health Record (EHR) system.

REFERENCES

[1] Rui Zhang, Ling Liu,"security models and requirements for healthcare application clouds", IEEE3rd international conference on cloud computing, 2010.

[2] Rima Addas, Ning Zhang," Support access to distributed EPRs with three levels of identity privacy preservation", sixth international conference on availability, reliability, and security, IEEE computer society 2011.

[3] Scharter, Schaffer," Unique user-generated digital Pseudonyms", springer LNCS 3685 September 2007.

[4] Peterson, R.L.: Encryption system for allowing immediate universal access to medical records while maintaining complete patient control over privacy.US Patent Application Publication, No.: US2003/0074564 A1 (2003).

[5] Thielscher, C., Gottfried,M., Umbreit, S., Boegner,F., Haack, J., Schroeders, N.: Patent:Data processing system for patient data. Int. Patent, WO 03/034294A2 (2005)

[6] Pommerening, K., Reng, M.: Secondary use of the Electronic Health Record via pseudonymization. In: Medical and Care Compunetics 1, pp. 441–446. IOS Press, Amsterdam (2004).

[7] Denielslamanig,, Christian stingl , "privacy aspect of e-health" the 3rd international conference on availability, reliability and security, IEEE computer society 2008.

[8] Bernhard riedl, Veronica," Assuring Integrity and confidentiality for pseudonymized health data", IEEE3rd international conference on Availability, Reliability, and security, 2008.

[9] Benhard Riedl, Grascher, Fenz, Neubauer," Pseudonymization for Improving the privacy in e-health applications ", IEEE 41st Hawaii International conference on system sciences, 2008.

