Multi-Speciality Clinic using Cloud

Sanjana H[1], Sandhya N [2], Ranjita A[3], Bhoomika H[4], Prof.Priyanka P[5]

[1]Student , Dept. of CS Engineering, Angadi Institute of Technology and Management, Belagavi, Karnataka, India

---

Abstract - *In the last years, the adoption of Electronic Health Records (EHRs) have been widely promoted, with the final aim of improving care quality and patient safety. Yet, sharing patient data in a large distributed and heterogeneous context, such as the healthcare domain, has inherently introduced security and privacy risks, due to the great sensitivity and confidentiality of the patient data and the need of accessing such data by a large number of health care workers with various roles for the patient care. Health research, including health outcomes and comparative effectiveness research, is on the cusp of a golden era of access to digitized real-world data, catalyzed by the adoption of electronic health records and the integration of clinical and biological information with other data. This era promises more robust insights into what works in health care. Several barriers, however, will need to be addressed if the full potential of these new data are fully realized; these will involve both policy solutions and stakeholder cooperation. Although a number of these issues have been widely discussed, we focus on the one we believe is the most important—the facilitation of greater openness among public and private stakeholders to collaboration, connecting information and data sharing, with the goal of making robust and complete data accessible to all researchers.*

Key Words: **Real world data, Ontology, Information structuring, Cloud, Advanced Encryption Standarad (AES).**

1. INTRODUCTION

Health research, including health outcomes and comparative effectiveness research, is on the cusp of a golden era of access to digitized real-world data that promises to transform the way in which we understand and practice medicine. Part of this transformation will be driven by the quantity of real-world data that will be generated—as well as the broader interest in "Big Data." Real-world data are collected outside of a clinical trial and used for health care decision making. Real-world data can include electronic medical records originating from health care providers, data used to coordinate and pay for care, and pharmacy data used to fill prescriptions. Data may also be collected in patient registries or pragmatic clinical trials. Internet searches and social media are also a growing source. Real-world data become "big data" when multiple data sets are combined. They could allow health plans to develop benefits that are tailored to the patient and value based, varying cost sharing and access on the basis of clinical need. These new data will certainly have an impact on how we monitor both the safety and the effectiveness of treatment, and these efficiencies will likely accelerate efforts to replace the current, volume-based fee-for-service health care system into one that allows for more efficient spend of health care dollars.

The Advanced Encryption Standard (AES) is the first and only publicly accessible cipher approved by the US National Security Agency (NSA) for protecting top secret information. Encryption is one of the most common ways to protect sensitive data. Encryption works by taking plain text and converting it into cipher text, which is made up of seemingly random characters. Only those who have the special key can decrypt it. AES uses symmetric key encryption, which involves the use of only one secret key to cipher and decipher information.

Healthcare Information Services (HIS) have great potential to enhance the services offered by the healthcare industry, towards increasing productivity, lowering costs, reducing medication errors, increasing transparency and fraud detection and easing the manpower shortage in healthcare. The increased security and mobility requirements of modern HIS, make smart cards a possible solution, since smart cards can provide security assurance and obviously solve the mobility problem. Smart cards can grant convenient and flexible access to patient data, to both healthcare professionals and patients.

2. RELATED WORKS

In [1] The amount and quality of information available to health care professionals in EHRs has a pivotal role to support continuing, efficient and quality integrated healthcare [4], yet sharing patient data in a large distributed and heterogeneous context, such as the healthcare domain, inherently introduces security and privacy risks [36]. In particular, due to the great sensitivity and confidentiality of the patient data and the fact that such data may need to be accessed by a large number of health care workers with various roles for the patient care, a high level of secure protection for data and data access is required. One of the most challenging aspects with respect to security and privacy for healthcare organizations, however, is the amount of power given by 'Patient consent and confidentiality' to the patients in terms of access control restrictions over their individual EHRs [18]. Even though various techniques have been developed to effectively implement finegrained access control, which allows flexibility in specifying differential access rights for individual users, some unsolved problems can be pointed out with respect to the specification of complex policies over EHRs, where access should be granted or denied according to the right and the need of the healthcare workers to perform a particular job function on specific EHR sections.

In[2]Currently, there are multiple public and private efforts to digitize and aggregate health information from administrative claims, EHR, and laboratory tests. Some of these efforts are also collecting additional sources of data including genomic data, patient-reported data, and biometric data from sensors. Although combining data across sites of care and broadening access has potential value for health research, it poses a risk to privacy. Even with the protections provided through the Health Insurance Portability and Accountability Act [3], there is still the risk of reidentification, particularly if data sets are merged with other information such as voter registration. Removing personal identifiers, aggregating small samples as required through the Safe Harbor and Limited Dataset provisions of Health Insurance Portability and Accountability Act along with careful consideration of what is available through other public use data sets, may reduce that risk [4, 5]. We contend that there exist or there are emerging solutions that would permit the "mashing" together of data sets at a patient level with limited risk to privacy and that the more difficult issue is that of data ownership and access.

In[3]The core motivation for the design and implementation of EHR and related systems is the improvement of care quality. Access to updated sound (error free and up to date) patient information by the care provider would allow better diagnostic, treatment decisions, and follow up, including tracking medical errors. Patients would also be more able to move between care providers, looking for the best health service, or to carry health self management with increased support from monitoring devices and social support, so that society is steadily moving towards the Personally Controlled EHR (PCEHR) [2] [31] for the management of lifelong health information. In the limit this patient mobility must deal with cross-boundary issues in transnational use of data [22]. In close relation, is the improvement of administration processes, from admission to billing.

In[4] Smart cards are plastic, pocket-sized cards including integrated circuits. They were first realized in 1974, mainly for use as an electronic purse for telephone services. Since then, the applications of smart cards have expanded in many domains; they are used in financial transactions, for identification and personnel monitoring, tickets for public transit and healthcare services. A typical smart card example used in healthcare is shown in Fig. 1, the French Carte Vitale, used for health insurance purposes in France [3].

Fig-1: An example of a smart card: The Carte Vitale used for health insurance purposes in France.

Smart cards can be categorized, depending on their contact technology, in contact smart cards, contactless smart cards and hybrids. Contact smart cards have a contact area, comprising several gold-plated contact pads which provide electrical connectivity when the card is inserted into a card reader while power is supplied by the read.

3. BENEFITS AND OPPORTUNITIES

The introduction of smart cards in Healthcare Information Services (HIS) provides a lot of benefits to all parties involved: the users of healthcare services – patients, the healthcare professionals and providers, governments involved and the health managers and planners. A. Health data consistency, availability and management Inconsistency of patient data and incomplete medical records represent major problems in healthcare delivery. Patients cannot be trusted 100% to be accurate and truthful regarding their medical history. Through the use of smart cards, access to accurate information is provided on a timely basis. Smart cards can be used as a trusted primary data repository, held by the patient, granting access to a dynamic data repository, invaluable to healthcare professionals and providers.

Country-wide smart card implementations in HIS The current state of the most important implementations of smart cards use in the healthcare sector worldwide is summarized in Table I [1], [8], [12], [13], and two important Informational patient data, stored on the smart card's chip, depends on each implementation and can include: name, surname, date-of-birth, sex, address, card number, social security number, card issue/expiration date, a security token for identification etc.

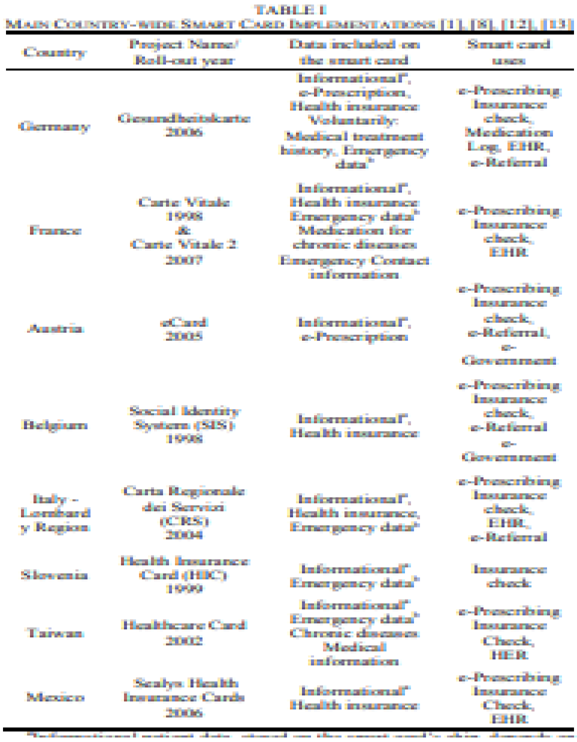

TABLE I
MAIN COUNTRY-WIDE SMART CARD IMPLEMENTATIONS [1], [8], [12], [13]

Country	Project Name/ Roll-out year	Data included on the smart card	Smart card uses
Germany	Gesundheitskarte 2006	Informational[a], e-Prescription, Health insurance Voluntarily: Medical treatment history, Emergency data[b]	e-Prescribing Insurance check, Medication Log, EHR, e-Referral
France	Carte Vitale 1998 & Carte Vitale 2 2007	Informational[a], Health insurance Emergency data[b] Medication for chronic diseases Emergency Contact information	e-Prescribing Insurance check, EHR
Austria	eCard 2005	Informational[a], e-Prescription	e-Prescribing Insurance check, e-Referral, e-Government
Belgium	Social Identity System (SIS) 1998	Informational[a], Health insurance	e-Prescribing Insurance check, e-Referral e-Government
Italy - Lombardy Region	Carta Regionale dei Servizi (CRS) 2004	Informational[a], Health insurance, Emergency data[b]	e-Prescribing Insurance check, EHR, e-Referral
Slovenia	Health Insurance Card (HIC) 1999	Informational[a] Emergency data[b]	Insurance check
Taiwan	Healthcare Card 2002	Informational[a] Emergency data[b] Chronic diseases Medical information	e-Prescribing Insurance Check, HER
Mexico	Sealys Health Insurance Cards 2006	Informational[a] Health insurance	e-Prescribing Insurance Check, EHR

4. CHALLENGES IN MHEALTH REALIZATION

It is no surprise that EHR implementation is an expensive affair. The selection, implementation, and optimization of EHR will take away the lion's share of the planned capital budget investment. Not everyone in the medical staff would be open to the idea of technological implementation in the establishment. In addition, there are health practitioners who are doubtful about the efficacy of electronic health records. Prior to deploying the EHR system, the staff needs to be given thorough training about the new workflow. The physicians and the medical team has to spend extra time and put in extra effort to understand the new system. It is a time-consuming process and a hassle for both the staff and the management. It is a logistical nightmare for the staff to export paper-based documents to date to the digital records. There will be large chunks of documents about the medical history of hundreds of patients and data entry might become a tedious and a time-consuming task for the staff. Interoperability refers to the ability of different EHR systems or software to exchange information so that different providers can make use of it. In EHR, interoperability is a necessity in order to get a complete picture of the patient's health. It remains a huge challenge for healthcare providers to build an interoperable system that enables the transfer of information among multiple providers. Effective communication between the healthcare provider and the IT vendor is essential to build an EHR system that gives the desired results. It is not a one-time activity but a continuous process to ensure that the expectations of both the parties are met.

Cloud storage separates the ownership and the control benefit of the EHR provider. Besides, it is widely believed that the cloud server cannot be fully trusted (i.e. semi-trusted).That is to say, it will follow the protocols, but tries to explore as much privacy of the data as it could. Intuitively, encrypt the EHR before outsourcing them to the cloud is an effective solution. However, traditional public key encryption (PKE) cannot satisfy the needs of one-to-many encryption. It has to distribute different private key for different users for decryption. Meanwhile, there should be the same amount of copies of ciphertext.

5. MEDICAL RESEARCH

A number of medical research efforts have based on mHealth to monitor and study the deployment of sensor-based technologies is the been patient diagnosis and treatments, including: Aged population health monitoring [18], calorie in take monitoring [18], treating patients with diabetes [19], [20],blood-pressure monitoring, treating cardiac patients [20], [21],and blood oxygen level monitoring (i.e., pulse oximeter) [22]. Telemonitoring is not only suitable and vital for patients with heart-related diseases and conditions, it is also necessary for patietswith other health problems, such as diabetes. Kollmann*etal.*[23] consider Type 1 diabetes patients and their interactions with physicians via data-ready mobile phones. The objective of this study was to evaluate the patient acceptance feasibility to use mobile phones to collect, transfer, and receive health related data/instructions to assist Type 1 diabetes patients. Patients were provided with Java- based data-ready mobile phones, which were synchronized with a remote database at the MC where health-related data were stored and appropriate statistics were generated and used by the CT. The acceptance feasibility was measured through a set of questionnaires, which were given to the patients. Currently, there are multiple public and private efforts to digitize and aggregate health information from administrative claims, EHR, and laboratory tests. Some of these efforts are also collecting additional sources of data including genomic data, patient-reported data, and biometric data from sensors. Although combining data across sites of care and broadening access has potential value for health research, it poses a risk to privacy. Even with the protections provided through the Health Insurance Portability and Accountability Act [3], there is still the risk of reidentification, particularly if data sets are merged with other information such as voter registration. Removing personal identifiers, aggregating small samples as required through the Safe Harbor and Limited Dataset provisions of Health Insurance Portability and Accountability Act along with careful consideration of what is available through other public use data sets, may reduce that risk [4, 5]. We contend that there exist or there are emerging solutions that would permit the "mashing" together of data sets at a patient level with limited risk to privacy and that the more difficult issue is that of data ownership and access.

Information processing infrastructure since the early designs the need for data mobility,i.e. by smartcards before the Internet full deployment, and the security issues that it raises, has beena prime concern. Patient data needs to travel with him in order to provide useful and timely support to the treatment, however it requires also authenticity certification and privacy. Concerns of security and privacy [35] encompass risks from the user, external attacks, and unethical data mining from companies. Cloud computing, EHR storage and processing in the cloud promises anywhere, anytime access to critical data. However, privacy and security slip from the hands of the care providers and the patient. In the framework of globally distributed cloud services, provides a traffic shaping algorithm to overcome traffic analysis attacks, and a resource distribution ensuring minimum delay and queue stability. The risk of third party intrusion is very high in the cloud. A encryption approaches [36][16] allow proper data access control by the authorized users in a context of multiple access levels, providing 1378 confidentiality, authenticity, unforgeability, anonymity and collusion resistance. Secure communication is a priority requirement for EHR pipeline. Secure communication over public Internet of laboratory results as HL 7 messages using a combination of off-the-shelf secure tools through a DIRECT gateway has been demonstrated [63].

6. CONSTRUCTION OF OUR SCHEME

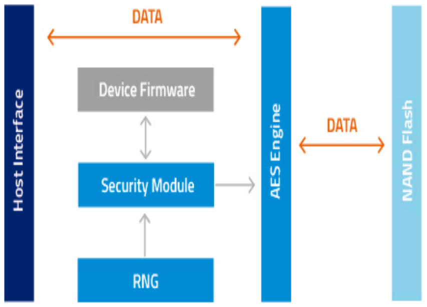

Fig-2: AES-256 encryption mechanism in ATP Secure Encrypt

AES-256, which has a key length of 256 bits, supports the largest bit size and is practically unbreakable by brute force based on current computing power, making it the strongest encryption standard. They make use of a hardware-based set of security modules and an AES engine. When the host writes data to the flash storage device, a Random Number Generator (RNG) generates the 256-bit symmetric cipher key, which is passed to the AES engine. The AES engine encrypts the plain text (source data) into cipher text (encrypted data) and sends it to the NAND flash for storage. Symmetric encryption is sometimes called private key encryption, because both parties must share a symmetric key that can be used to both encrypt and decrypt data.

Symmetric encryption is sometimes called private key encryption, because both parties must share a symmetric key that can be used to both encrypt and decrypt data.

Asymmetric encryption is used primarily as a mechanism for exchanging symmetric private keys. There's a reason for this, asymmetric encryption is historically a more expensive function owing to the size of its keys. So public key cryptography is used more as an external wall to help protect the parties as they facilitate a connection, while symmetric encryption is used within the actual connection itself.

7. PROPOSED SYSTEM

Switching from traditional health information handling to Electronic health record is expected to increase performance and decrease costs associated with healthcare activities. The goal of Electronic health record can be summarized as: Achieving the greatest benefit in the shortest timeframe, with the least risk and associated cost. This goal can be achieved through the following increments: Efficiency, equity, service delivery (time reduction), patient-centeredness, safety, security, effectiveness, and improved quality decision techniques. These increments should be achieved with an overall cost reduction. This proposed approach demonstrates the effective implementation of a universal classic medical record in electronic form, a procedure by which, clinicians are led to utilize algorithms and intelligent systems for their differential diagnosis, final diagnosis and treatment strategies.

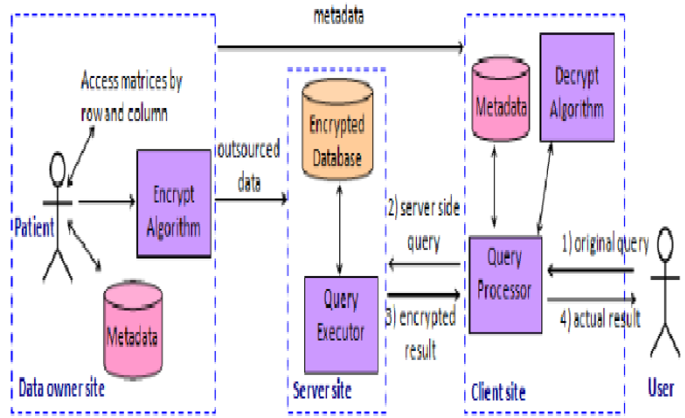

Fig-3: Block Diagram of an EHR system

The advantages are:

- *Better health* by encouraging healthier lifestyles in the entire population, including increased physical activity, better nutrition, avoidance of behavioral risks, and wider use of preventative care
- Providing accurate, up-to –date, and complete information about the patients at the point of care.
- Necessary treatment can be provided to patient in time.
- Reduces loss of life due to lack of timely treatment.
- Health related information will be more secured.

8. CONCLUSION

The world is changing for health research. Not everyone is ready for it. The era of digitized real-world data holds great promise in its ability to transform health care. Yet this promise can be fully realized only if access to data is broadened, if connectivity between data sets is improved, if the methods for analyzing large data sets are advanced, communication of evidence is encouraged and put in the right context ,and if there are clear standards for how privacy can be maintained that also recognize that no solution is entirely secure.

REFERENCES

1. Flora Amato, Giuseppe De Pietro, Massimo Esposito and Nicola Mazzocca, "An integrated framework for securing semi-structured health records", Knowledge-Based Systems, vol. 79, no. 0, pp. 99-117, 2015.

2. Marc L. Berger, Craig Lipset, Alex Gutteridge, Kirsten Axelsen, Prasun Subedi and David Madigan, "Optimizing the leveraging of real-world data to improve the development and use of medicines", Value in Health, vol. 18, no. 1, pp. 127-130, 2015

3. Manuel Grana, Konrad lackwoski ENGINE centre Wroclaw Technological University Email: konrad.Jackowski@pwr.edu.pl

4. Anastasis P. Keliris, Vassileios D. Kolias and Konstantina S. Nikitamedical

5. Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for finegrained access control of encrypted data. Presented at Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006.

6. Yu S, Wang C, Ren K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing. Presented at Infocom, 2010 proceedings IEEE. IEEE, 2010

7. Beimel A, et al. "Secure schemes for secret sharing and key distribution," Ph.D. dissertation, Faculty of computer science, Technion-Israel Institute of technology. Israel, 1996.

8. Cheung L, Newport C. Provably secure cipher text policy ABE. Presented at Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007.

9. Dong C, Chen L, Wen Z. When private set intersection meets big data: an efficient and scalable protocol. Presented at international conference on computer and communications security. ACM, 2013. ZU.

10. Li J, Ren K, Zhu B, et al. Privacy-aware attribute-based encryption with user accountability. Presented at international.