ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

Efficient Framework for Semantic Query Search Engine in Large-Scale Data Collection for Health Information Exchange

N. Raja Mohan Reddy[1], B. Nagalakshmi[2], A. Chandra Sekhar[3]

M.Tech Student, Dept. of CSE, GATES Engineering College, Affiliated to JNTUA, Andhra Pradesh, India[1]

Associate Professor, Dept. of CSE, , GATES Engineering College, Affiliated to JNTUA, Andhra Pradesh, India[2]

Assistant Professor, Dept. of CSE, , GATES Engineering College, Affiliated to JNTUA, Andhra Pradesh, India[3]

ABSTRACT: Electronic Health Record helps to improve the safety and quality care of every individual patient details, is necessary that of to be maintained by the clinic, through the interoperability of Health Information Exchange (HIE) differing from hospital to hospital. The CDA document generated and integrated Open API service based on cloud computing allows us conveniently to generate CDA documents without purchase of proprietary software. Using CDA document integration system integrates multiple CDA documents per patient into a single CDA document. Both physicians and patient can utilize the clinical data in chronological order. In this paper, the CDA documents integrate into single document and can be browsed as a readable format. It is easy to read and understand for physicians efficiently. Users no need to purchase or deploy any tools to convert the CDA XML document to other format. Converting of CDA XML format to readable format increases the usage of this system and reduces the time for physicians from delay of making decisions. The conversion can be done by methods that which supports for conversion of XML based format to readable format using APIs on cloud and that document can access by physicians and patients at need of view

I.INTRODUCTION

Electronic Health Records is a great tool for physicians and is about quality, safety and efficiency for health care delivery. In order to ensure successful an operation of EHR, a Health Information Exchange (HIE) system need to be implemented [1]. Health Level Seven (HL7) has established CDA as a major standard for clinical documents [2]. CDA is a document markup standard that defines the structure and semantics of clinical document for the purpose of exchange. The first version of CDA was developed in 2001 and Release 2 came out in 2005 [3].The Generation of CDA document, in each hospital invariably requires a separate Clinical Document Architecture system. So the hospitals are reluctant to adopt the new system. Solution of this problem is adoption of EHR (Electronic Health Record). The amount of exchanged CDA Document increases the time because of more documents that data are distributed in different documents. So all the CDA documents are integrated into a single document, the physician is empowered to review the patient's clinical history with conveniently. Although the Clinical Document Architecture is in XML based format, the physicians can be delay for making decisions. So adopting the system of new CDA architecture can give a elegant and contented file to users.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

II. LITERATURE SURVEY

1) Interoperability of personal health records

AUTHORS: J. L ahteenm€ aki, J. Lepp anen, and H. Kaijanranta,

The establishment of the Meaningful Use criteria has created a critical need for robust interoperability of health records. A universal definition of a personal health record (PHR) has not been agreed upon. Standardized code sets have been built for specific entities, but integration between them has not been supported. The purpose of this research study was to explore the hindrance and promotion of interoperability standards in relationship to PHRs to describe interoperability progress in this area. The study was conducted following the basic principles of a systematic review, with 61 articles used in the study. Lagging interoperability has stemmed from slow adoption by patients, creation of disparate systems due to rapid development to meet requirements for the Meaningful Use stages, and rapid early development of PHRs prior to the mandate for integration among multiple systems. Findings of this study suggest that deadlines for implementation to capture Meaningful Use incentive payments are supporting the creation of PHR data silos, thereby hindering the goal of high-level interoperability.

2) Applying cloud computing model in PHR architecture.

AUTHORS: S. Kikuchi, S. Sachdeva, and S. Bhalla,

In recent years, some practical and commercial Personal Health Records and some related services such as Google Health [1] and Microsoft HealthVault [2] have been launched. On the other hand, Cloud Computing has matured more and become the major streams to realize a more effective operational environment. However so far, there have been few studies in regards to applying Cloud architecture in the PHR explicitly despite generating volume data. In this paper, we review our trial on the general architecture design by applying the Cloud components for supporting healthcare record areas and clarify the required conditions to realize it.

3. Health Information Privacy, Security, and Your EHR.
AUTHORS: M. Bellare

If your patients lack trust in Electronic Health Records (EHRs) and Health Information Exchanges (HIEs), feeling that the confidentiality and accuracy of their electronic health information is at risk, they may not want to disclose health information to you. Withholding their health information could have life-threatening consequences. To reap the promise of digital health information to achieve better health outcomes, smarter spending, and healthier people, providers and individuals alike must trust that an individual's health information is private and secure. Your practice, not your EHR developer, is responsible or taking the steps needed to protect the confidentiality, integrity, and availability of health information in your EHR system.

4. A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud

AUTHORS: C. Ng and P. Lee. Revdedup

Benefited from cloud computing, users can achieve an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. Moreover, for existing schemes, the security of key distribution is based on the secure communication channel, however, to have such channel is a strong assumption and is difficult for practice. In this paper, we propose a secure data sharing scheme for dynamic members. Firstly, we propose a secure way for key distribution without any secure communication channels, and the users can securely obtain their private keys from group manager. Secondly, our scheme can achieve fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. Thirdly, we can protect the scheme from collusion attack, which means that revoked users cannot get the original data file even if they conspire with the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

untrusted cloud. In our approach, by leveraging polynomial function, we can achieve a secure user revocation scheme. Finally, our scheme can achieve fine efficiency, which means previous users need not to update their private keys for the situation either a new user joins in the group or a user is revoked from the group

5. **ADVANCE SECURITY TO CLOUD DATA STORAGE**

AUTHORS: P. Lee, and W. Lou

The proposed system is an effective and flexible distributed Scheme with explicit dynamic data support to ensure the correctness of user's data in the cloud. To fully ensure the data integrity and save the cloud users computation it is of critical importance to enable public auditing service for cloud data storage, so that users may depend on independent third party auditor to audit the outsourced data. The Third party auditor can periodically check the integrity of all the data stored in the cloud .which provides easier way for the users to ensure their storage correctness in the cloud.

III. EXISTING SYSTEM

Effective health information exchange needs to be standardized for interoperable health information exchange between hospitals. Especially, clinical document standardization lies at the core of guaranteeing interoperability.
It takes increasing amount of time for the medical personnel as the amount of exchanged CDA document increases because more documents means that data are distributed in different documents. This significantly delays the medical personnel in making decisions. Hence, when all of the CDA documents are integrated into a single document, the medical personnel is empowered to review the patient's clinical history conveniently in chronological order per clinical section and the follow-up care service can be delivered more effectively. Unfortunately for now, a solution that integrates multiple CDA documents into one does not exist yet to the best of our knowledge and there is a practical limitation for individual hospitals to develop and implement a CDA document integration technology.

IV.PROPOSED WORK

- In this paper we present (1) a CDA document generation system that generates CDA documents on different developing platforms and (2) a CDA document integration system that integrates multiple CDA documents scattered in different hospitals for each patient.
- CDA Generation API generates CDA documents on cloud.
- CDA Generation Interface uses the API provided by the cloud and relays the input data and receives
- CDA documents generated in the cloud.
- Template Manager is responsible for managing the CDA documents generated in the cloud server. Our system uses CCD document templates.
- CDA Generator collects patient data from hospitals and generates CDA documents in the template formats as suggested by the Template Manager.
- CDA Validator inspects whether the generated CDA document complies with the CDA schema standard.

ADVANTAGES OF PROPOSED SYSTEM:

- Hospital systems can simply extend their existing system rather than completely replacing it with a new system. Second, it becomes unnecessary for hospitals to train their personnel to generate, integrate, and view standard-compliant CDA documents.
- The cloud CDA generation service produces documents in the CDA format approved by the National Institute of Standards and Technology (NIST).
- If this service is provided for free at low price to hospitals, existing EHR are more likely to consider adoption of CDA in their practices.
- Interoperability between hospitals not only helps improve patient safety and quality of care but also reduce time and resources spent on data format conversion.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

ARCHITECTURE

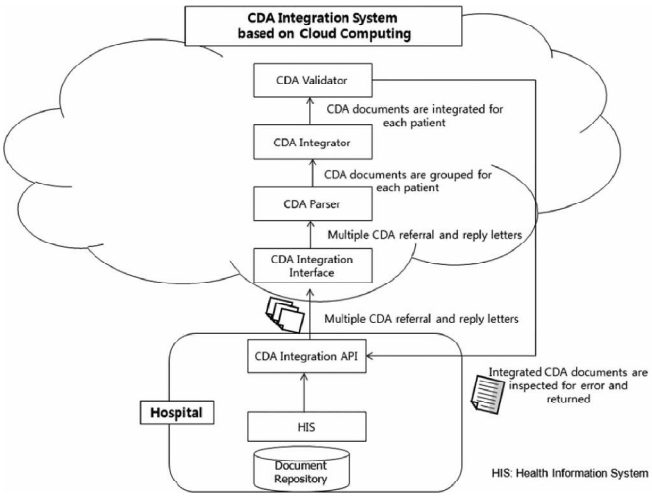

Fig 1 System Architecture

V. IMPLEMENTATION

Construction of System Environment

- In the first module we develop the Construction of the System Environment to prove our proposed system model. In this module we develop Hospital A, Hospital B, Doctor, Patient/User, Admin and Cloud Modules.
- In Hospital A, we create the User Authorization with Login Credentials. This module provides the option of Upload the Patient details as XML File in the Cloud with Encrypted and also provides the option to check the status of the uploaded file with the XML Format. The same is followed in the Hospital B too.
- In the Admin part, we provide the Admin Authorization with login Credentials and view pending request of users and doctors. The admin only give Approval to the request by sending secret key to user/doctor to access the file.
- In cloud Login, view the patient details in the XML format which is acquired from CDA.

The CDA Document

- In this module we develop the CDA document. The HL7 Clinical Document Architecture Release 2 (CDA R2) was approved by American Nation Standards Institute. It is an XML-based document markup standard that specifies the structure and semantics of clinical documents, and its primary purpose is facilitating clinical document exchanges between heterogeneous software systems.
- A CDA document is divided into its header and body. The header has a clearly defined structure and it includes information about the patient, hospital, physician, etc. The body is more flexible than the header and contains various clinical data.
- Each piece of clinical data is allocated a section and given a code as defined in the Logical Observation Identifiers Names and Codes (LOINC). Different subcategories are inserted in a CDA document depending on the purpose of the document, and we chose the Continuity of Care Document (CCD) because it contains the health summary data for the patient and it is also widely used for interoperability.

Construction of a Cloud Computing Environment

- In this module we develop the Cloud computing environment. In this module, we develop the construction of a Cloud Computing Environment and how multiple CDA documents are integrated into one in our CDA Document Integration System. The standard for this is Korean Standard for CDA Referral and Reply Letters (Preliminary Version). Templates which generate a CDA use CCD part of Consolidated CDA which is released by ONC and made by HL7. However, an actually generated CDA has a form of CDA Referral and Reply Letters.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 10, October 2017

- The rationale for CDA document integration is as followed. When CDA-based HIE (Health Information Exchange) is actively used among hospitals, the number of CDA documents pertaining to each patient increases in time. Physicians need to spend a significant portion of their time on reading these documents for making clinical decisions.
- At a hospital, the CDA documents to be integrated are processed through our CDA Integration API. The CDA Integration Interface relays each CDA document sent to the cloud to the CDA Parser, which converts each input CDA document to an XML object and analyzes the CDA header and groups them by each patient ID. The CDA Document Integrator integrates the provided multiple CDA documents into a single CDA document. In this process, the data in the same section in the document body are merged.

Integration of CDA Documents via Our Cloud Server

- We integrated multiple CDA documents of patient referrals and replies by using the API at our server. The use case scenario and patient data used for integration are shown in this module.
- We adopted sample patient data provided by the US EHR Certification Program, Meaningful Use. The data does not pertain to an actual person. It is fictional, and available for public access. This module is to show how a client integrating multiple CDA documents by using our API. The sample many clinical documents are shown to be successfully integrated.

V. CONCLUSION

The motive of this paper is to provide an integrity auditing scheme with public verifiability, green information dynamics and honest disputes arbitration. To eliminate the constraint of index usage in tag computation and effectively help statistics dynamics, it differentiate between block indices and tag indices, and devise an index switcher to hold block-tag index mapping to keep away from tag re-computation due to block replace operations, which incurs constrained additional overhead. Meanwhile, when you consider that both clients and the CSP probably can also misbehave at some stage in auditing and information replace, the present risk model is extended in contemporary studies to offer honest arbitration for fixing disputes between clients and the CSP, that is of crucial significance for the deployment and advertising of auditing schemes in the cloud environment. This is done by using designing arbitration protocols based on the concept of changing metadata signatures upon each replace operation.

REFERENCES

[1] Y. Deswarte, J.-J. Quisquater, and A. Sa¨ıdane, "Remote integrity checking," in Proc. 5th Working Conf. Integrity and Intl Control in Information Systems, 2004, pp. 1–11.
[2] D. L. Gazzoni Filho and P. S. L. M. Barreto, "Demonstrating data possession and uncheatable data transfer." IACR Cryptology ePrint Archive, Report 2006/150, 2006.
[3] A. Juels and B. S. Kaliski Jr, "Pors: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Computer and Comm. Security (CCS07), 2007, pp. 584–597.
[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Computer and Comm. Security (CCS07), 2007, pp. 598–609.
[5] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. 14th Intl Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT 08), 2008, pp. 90–107.
[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. 14th European Conf. Research in Computer Security (ESORICS 08), 2009, pp. 355–
370.
[7] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents." IACR Cryptology ePrint Archive, Report 2008/186, 2008.
[8] C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," Network, IEEE, vol. 24, no. 4, pp. 19–24, 2010.
[9] C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. 16th ACM Conf. Computer and Comm. Security (CCS 09), 2009, pp. 213–222.
[10] Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic audit services for integrity verification of outsourced storages in clouds," in Proc. ACM Symp. Applied Computing (SAC 11), 2011, pp. 1550–1557.