云环境下组合电子健康记录访问控制框架①

夏亚洲, 姚志强, 熊金波

(福建师范大学 软件学院, 福州 350108)

摘 要: 针对云环境下电子健康记录信息安全共享的需求提出云环境下组合电子健康记录访问控制框架. 在该框架中基于多个 CDA 文档的逻辑关系, 提出并构建组合电子健康记录结构, 应用基于属性的多级安全访问控制策略实现组合电子健康记录的安全管理, 应用基于 XLINK 技术的 XML Web 服务实现组合电子健康记录的下载和查看. 通过对比分析可说明, 与已有方案相比, 本方案提出的框架更加适合云环境下的电子健康信息安全共享.

关键词: HL7 CDA; 多级安全访问控制; XLINK; XML; 云环境

Accss Control Framework for Composite Electronic Health Records in the Cloud Computing Environment

XIA Ya-Zhou, YAO Zhi-Qiang, XIONG Jin-Bo

(School of Software, Fujian Normal University, Fuzhou 350108, China)

Abstract: To meet requirements of EHRs security sharing in the cloud computing conditions, this paper presents an access control framework for composite EHRs under the cloud computing environment. We propose and construct composite EHRs based on multi-CDAs' logical relationship. On the basis of attribute-based multilevel access control policy, we realize the security management of composite EHRs. By using the XML Web service, which based on the XML XLINK technology, we achieve the goal of downloading and checking composite EHRs. Compared with existing schemes, our project is much more suitable for EHRs security sharing in the cloud computing conditions.

Key words: HL7 CDA; multilevel access control; XLINK; XML; cloud computing environment

医院应用许多 IT 设备和基础设施, 设备定期更新和维护的开销是巨大的, 通常医院会将部分开销转嫁给病人, 增加病人额外的负担. 随着医疗进入无纸化时代, 记录病人实时身体健康信息和终身电子健康信息成为可能, 但是, 需要记录的医疗健康数据十分庞大, 如何存储、有效分析利用和安全交换这些海量数据, 成为迫切需要解决的难题.

面对上述医疗系统存在的难题, 要求更高性能的软件、分布式的计算能力和标准化的数据共享方案. 云计算通过网络提供可伸缩的廉价分布式计算能力, 它具有超大规模(医院可以存储海量的医疗数据)和廉价(可有效减少医院和病人的开销)的特性. 因此, 研究云环境下电子健康记录信息的共享是未来的趋势.

目前, 鲜有完全实现云环境下电子健康记录信息共享的方案. Huang 等[1]提出 CDA 文档便携式安全交换技术, 通过加密 CDA 文档保存在可移动磁盘实现电子健康信息的安全交换和共享. Pardamean 等[2]提出云环境下一种集成的电子健康记录共享模型. 该应用是基于云平台的, 它将电子健康记录系统作为一种云软件服务, 提供给政府、医院、医生、病人、药剂师和医疗保险组织使用; 该系统的数据是集中式存储的, 允许使用者平等的共享数据. 文献[3-8]研究云环境下基于医疗系统的互操作性模型, 应用 HL7 相关的规范实现医疗系统机构间的信息交换和共享. Jin 等[9]提出

① 基金项目:国家自然科学基金(61370078)

收稿时间:2014-05-23;收到修改稿时间:2014-06-19

组合电子健康记录的访问控制模型. 该模型以现有 CDA 文档层级结构为基础, 根据 CDA 文档内信息的敏感程度, 提出认证域的概念, 从而实现 CDA 文档的访问控制. 文献[10-14]研究基于属性和行为的多级安全访问控制, 可以依据用户属性集或行为方式实现结构化文档多级安全访问控制. 上述几种方案, 存在如下几点局限: ①面向可移动存储, 不适合云环境下电子健康记录的安全共享; ②面向医疗系统内部的信息交换, 不适合云环境下电子健康记录的安全共享; ③研究单个 CDA 文档的访问控制, 未考虑多个 CDA 文档间的访问控制; ④应用单一安全级别访问控制策略, 未研究多级安全访问控制. 因此, 均无法满足云环境下电子健康信息的安全存储、访问和共享.

针对上述局限, 提出云环境下组合电子健康记录访问控制框架. 本方案基于多个CDA文档间的逻辑关系提出和构建组合电子健康记录结构, 优化电子健康信息的组织和管理, 提高系统的性能; 在安全访问控制方面, 应用多级安全访问控制策略, 有效保证系统安全性.

本文剩余内容的组织方式如下: 第 1 部分简要介绍关于CDA文档和组合电子健康记录的背景知识; 第 2 部分详细介绍云环境下组合电子健康记录访问控制框架, 包括基于属性的多级安全访问控制策略和基于 XML XLINK 技术的 XML Web 服务, 并用一个实例展示组合电子健康记录结构和多级安全访问控制策略的应用; 对比现有方案和本方案的优缺点, 表明本框架更适合云环境下组合电子健康记录信息的安全共享; 第 3 部分总结本方案.

1　背景知识

CDA 文档用符合 XML Schema 的规范来封装内容. CDA 文档整体是被一个<ClinicalDocument>元素封装起来的, 它包括两部分: CDA 头(Header)和 CDA 体(StructuredBody), 其中 CDA 头部分标识和分类文档的类型, 并且提供文档相关信息, 包括文档编辑者、病人、病人亲属和医疗提供商等信息. 文档体部分被一个<StructuredBody>元素封装起来, 它主要提供病人的诊断和医疗报告.

CDA 文档层级结构有利于对信息的分析和封装. 但是, 传统的 CDA 文档未考虑与其它 CDA 文档的关系. 在特定情形下需要得到与病人相关的所有CDA文档, 比如病案首页、出院摘要、检验报告、门诊就诊摘要和健康体检报告, 传统方法需要根据病人身份信息来多次定位不同的文档, 这种方式不利于电子健康记录的组织、搜索和管理. 因此, 提出组合电子健康记录, 利用 XML XLINK 技术, 将各个 CDA 文档依据其相互之间的逻辑关系组织成组合电子健康记录. 该模型应用树型结构组织医疗健康信息, 将病人所有相关的CDA文档以日期的粒度组织管理, 组合电子健康记录具体结构如图 1 所示. 组合电子健康记录有三个安全等级$\{sl_1, sl_2, sl_3\}$, 其中 $sl_1, sl_2, sl_3 \in SecLev$ 且安全级别 $sl_1 > sl_2 > sl_3$, 即沿着组合电子健康记录的根节点向下, 安全等级越弱. 安全等级的级别由属性集决定, 具体定义详见 2.1 部分定义 8.

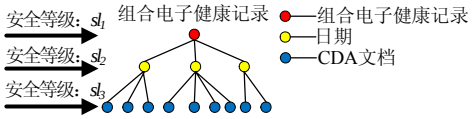

图 1　组合电子健康记录

2　云环境下组合电子健康记录访问控制框架

本文提出的组合电子健康记录访问控制框架如图 2 所示, 在访问控制模块中制定访问控制策略, 完成 HIS(Hospital Information System, 医疗信息系统)、医生、病人和数据共享者密钥的分发, 实现对文档的多级安全访问控制; 云端 XML Web 服务主要完成组合电子健康记录转换, 由于用户上传的组合电子健康记录是 XML 格式, 通过定制的 XSLT 模板将其转码为适合 HTML 显示的格式, 实现组合电子健康记录的云端在线查看.

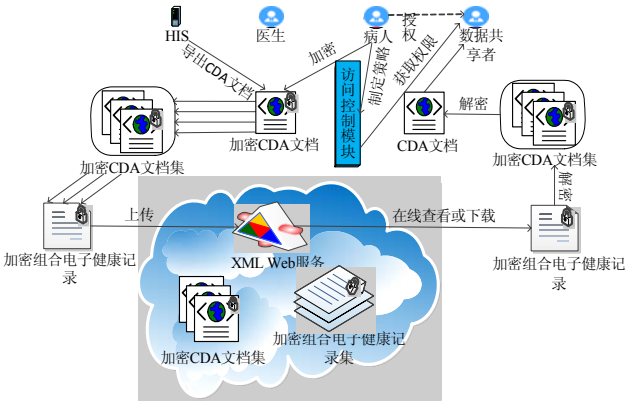

图 2　云环境下组合电子健康记录访问控制框架

2.1 访问控制模块

针对云环境中结构化文档易产生信息泄露和非授权访问等问题, 提出基于属性的多级安全访问控制模型, 构建访问控制策略并给出策略的形式化描述. 本框架假设拥有组合电子健康记录解密密钥的用户, 必定拥有相应的 CDA 文档解密密钥. 因此, 本文重点考虑组合电子健康记录的访问控制策略.

① 定义 1. 文档: 文档集 Documents Set: $DOCS=\{doc_1, \ldots, doc_n\}$, 其中 $doc_i(1 \le i \le n)$表示一个组合电子健康记录.

② 定义 2. 用户集合: 用户集合由需要访问电子健康记录的实体组成, 本框架包括医生、病人和数据共享者.

③ 定义 3. 属性类型: 属性类型表示实体访问文档时所拥有的特性, 属性类型可以是具体的特性, 比如 *subject_ID*(本框架应用实体的公钥)、*document_ID*、*Time*、*Location* 和 *Age*.

④ 定义 4. 属性集合: 属性集合由属性类型组成, $AS=\{AT_1, \ldots, AT_n\}$, 依据系统的安全需求, 安全管理员指定访问控制需求的属性类型. 比如 $AS=\{subject\_ID, document\_ID, Time, Location\}$. 属性集合在应用实施之前指定, 系统管理员可以动态增加新的属性集合.

⑤ 定义 5. 属性条件: 属性条件 CN 满足如下格式: "<*AT*> <*OP*> <*VALUE*>", 其中 $AT \in AS$,*OP* 属于逻辑运算符集合$\{\ge, \le, >, <, =, \ne\}$, *VALUE* 是 *AT* 的具体值, 比如 $Age \ge 65$.

⑥ 定义 6. 属性限制: 属性限制 *C* 由正则表达式构成, C 表示属性集合与属性条件的逻辑关联.

$C:=Clause_1 \cup Clause_2 \cup \ldots \cup Clause_k$;

$Clause:=Condition_1 \cap Condition_2 \cap \ldots \cap Condition_k$;

Condition := <*AT*> <*OP*> <*VALUE*>;

基于上述格式, 本框架的访问控制机制能够为不同的安全需求制定复杂的属性条件. 例如, "电子健康记录可以在上午 10 点到下午 3 点之间被数据共享者访问"可用如下格式表达:

$C=Time \ge 10{:}00 \cap Time \le 15{:}00 \cap Identity$="数据共享者"

⑦ 定义 7. 文档访问请求: 用户的访问行为由如下三元组表示:

$Acc=<U, doc, AS>$, 其中 $U \in User\ Set$, 表示发起访问请求的用户, $doc \in DOCS$, 表示请求访问的文档, *AS* 表示发起访问请求的用户属性集.

⑧ 定义 8. 安全等级有限序列: $SecLev=\{sl_1, sl_2, \ldots, sl_n\}$, 本框架提出的组合电子健康记录有三个安全等级$\{sl_1, sl_2, sl_3\}$, 其中 $sl_1, sl_2, sl_3 \in SecLev$ 且安全级别 $sl_1 > sl_2 > sl_3$, 即沿着组合电子健康记录的根节点向下, 安全等级越弱. 安全等级的级别由属性集合决定, sl_1 满足属性集合 AS_1, $AS_1=\{document\_ID, root\_Element\_key, User\_ID, User\_Public\_Key, User\_Private\_Key\}$, sl_2满足属性集合 *AS2*, $AS2=\{document\_ID, date\_Element\_key, User\_ID, User\_Public\_Key, User\_Private\_Key\}$, sl_3满足属性集合 AS_3, $AS_3=\{document\_ID, CDA\_Element\_key, User\_ID, User\_Public\_Key, User\_Private\_Key\}$.

⑨ 定义 9. 访问策略: 访问策略由如下三元组表示: $Pol=\{S, doc, C\}$, 其中 *S* 表示策略的主体, 本框架表示病人、医生或者数据共享者, *doc* 表示请求访问的文档, *C* 表示属性限制集合.

授权决策机制保证用户能够获取其应有的权限. 授权策略集合 $Policy\ Set=\{Pol_1, Pol_2, \ldots, Pol_n\}$, 其中 Pol_i 表示一条访问策略.

① 断言 1. 策略符合: 设 $Acc=<U, doc, AS>$,表示当前用户发起访问文档的请求, $Pol=<S, doc, C>$是一条授权策略.

Policy Accord$(Acc, Pol)=(\exists Pol)((Acc.U \in Pol.S) \wedge (Acc.doc=Pol.doc \wedge True)$, 其中当 *Pol.C* 中所有的 *AS* 能够被 *Acc.AS* 替代, 则此时的布尔表达式为真(*True*), 否则为假(*False*), 即在授权策略集合中, 如果存在一条授权策略, 满足如上三个条件, 则称该访问请求符合该策略.

② 断言 2. 策略不符合: 设 $Acc=<U,doc,AS>$, 发起访问文档的请求, $Pol=<S,doc,C>$是一条授权策略. *Policy Not Accord*$(Acc, Pol=(\forall Pol)((Acc.U \notin Pol.S) \vee (Acc.doc \ne Pol.Doc) \vee False)$, 即在授权策略集合中, 如果每一条授权策略, 满足如上三个条件中的任意一个, 则称该访问请求与该策略是策略不符合的.

2.2 XML Web 服务

用户可上传加密文档和未加密文档存储在云端. 云端 XML Web 服务提供文档的下载和在线查看, 文档在线查看流程图如图 3 所示. 对于未加密的组合电子健康记录, 应用相应的XSLT模板, 将其转码为适合 HTML 显示的格式, 最终实现云端 Web 的在线查看.

对于加密的组合电子健康记录, 首先用户用相应的解密密钥解密, 然后再将其转码为适合 HTML 显示的格式, 最终实现云端 Web 的在线查看. 此流程同样适用于文档的下载, 用户下载的电子健康记录最终同样转化为适合 HTML 显示的格式, 方便用户查阅相关电子健康信息.

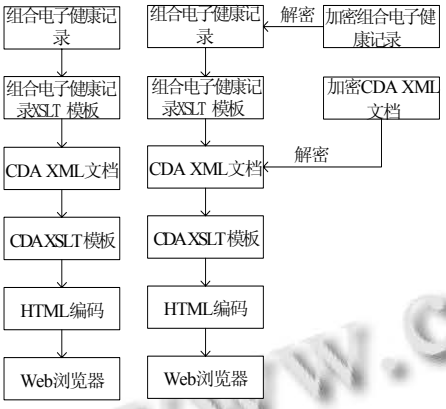

图 3　加密文档和未加密文档在线查看流程

本框架提出的组合电子健康记录基于不同 CDA 文档间的逻辑关系, CDA 文档应用符合 HL7 R2 规范的 CDA 样例作为本文的实例. 组合电子健康记录的主要内容为元数据和 CDA 文档, 元数据的内容主要包括病人的姓名、ID 和就诊时间区间, 与原始 CDA 文档相比, 就诊时间区间为新增元素, 它组织病人所有的或者特定时期的 CDA 文档; CDA 文档由以日期为基础的 CDA 文档的超链接构成, 通过 XML XLINK 技术, 可以查询到特定日期的相关 CDA 文档.

XML 加密是 W3C(World Wide Web Consortium) 加密 XML 的标准, 加密过程包括加密 XML 文档的元素及其子元素, 通过加密, XML 的初始内容将被替换, 但其 XML 格式仍然被完好的保留. XML 加密支持三种加密方法, 仅仅使用对称加密的方法加密 XML、使用对称加密和非对称加密相结合的方法加密 XML 和使用 X.509 加密 XML. 本框架应用对称加密和非对称加密相结合的加密方式, 实现组合电子健康记录的访问控制: 通过加密根元素<组合电子健康记录>实现整个组合电子健康记录的加密, 对应的文档安全等级为 sl_1; 通过加密<日期>元素, 实现部分文档的加密, 对应的文档安全等级为 sl_2; 通过加密元素<CDA 文档>的内容, 实现单个文档的加密, 对应的文档安全等级为 sl_3. XML 加密过程可概括为五个步骤: (1)选择 XML 文档中的一个元素. (2)使用一个对称密钥加密元素. (3)使用非对称加密密钥来加密上述对称密钥(通常为公钥). (4)创建一个<EncryptedData>元素, 该元素下包含加密的数据和加密的密钥. (5)用加密后的元素替换掉初始元素. 下述实例代码对元素<CDA 样例>实现加密, 将加密后的数据和加密的密钥放入元素<EncryptedData>, 并用元素<EncryptedData>替代元素<CDA 实例>, XML 加密标准可参考[14,15].

未加密组合电子健康记录部分代码如下:

```
<组合电子健康记录
xmlns:xlink="http://www.w3.org/1999/xlink">
  <元数据>
    <name>
      <given> Henry </given>
      <family> Levin </family>
    </name>
<id extension="12345" root="2.16.840.1.113883.19.5"/>
    <time>
      <begin value="2000030714"></begin>
      <end value="20010401614"></end>
    </time>
  </元数据>
  <CDA 文档>
    <日期 时间="2000-03-07">
      <CDA 样例
      xlink:type="simple" xlink:href="CDA.xml"
                                  xlink:show="new"
xlink:actuate="onRequest">
        <名称> CDA 样例 </名称>
      </CDA 样例>
      <病案首页
   xlink:type="simple"   xlink:href="病案首页.xml"
   xlink:show="new"      xlink:actuate="onRequest">
        <名称> 病案首页 </名称>
      </病案首页>
      ...
    </日期>
      ...
  </CDA 文档>
```

</组合电子健康记录>

加密组合电子健康记录部分代码类似, 予以删略.

本实例假设数据共享者 A 拥有属性集 AS_1, 数据共享者 B 拥有属性集 AS_2, 数据共享者 C 拥有属性集 AS_3, 分别请求访问组合电子健康记录, 即发出如下请求 $Acci$ =<U, doc, AS_i>, 其中 i = {1, 2, 3}, 假设组合电子健康记录安全等级为 sl_1, 接收到访问请求后, 访问控制模块查询策略集, 如果存在策略$(((Acc.U \in Pol.S) \wedge (Acc.doc = Pol.doc) \wedge True)$, 那么允许数据共享者访问组合电子健康记录. 本实例中, 数据共享者 B 和数据共享者 C 不满足策略的第三个条件, 即属性集不满足, 因此无权限访问组合电子健康记录. 数据共享者 A 满足策略的三个条件, 因此可以访问组合电子健康记录.

目前支持 XLINK 的浏览器数量较少, 选取支持 XLINK 技术的 Internet Explorer 8.0 作为本文的应用场景. 本实例应用场景为数据共享者 A 请求访问组合电子健康记录, 其属性集 AS_1 满足访问整个组合电子健康记录的策略属性集合条件 C, 因此, 允许其访问整个组合电子健康记录. 图 4 为组合电子健康记录在 IE 8.0 浏览器显示的效果, 其组织的 CDA 文档由一系列的超链接地址构成, 通过点击 CDA 样例超链接, 可查阅样例具体的电子健康医疗信息.

图 4 组合电子健康记录 IE 在线查看

2.3 相关工作比较

云环境下组合电子健康记录访问控制框架与已有方案相比, 主要在云环境、组合电子健康记录和多级安全访问控制方面存在差异, 其具体比较如表 1 所示. 通过方案对比可表明, 组合电子健康记录访问控制框架在云环境、组合电子健康记录和多级安全访问控制方面拥有优势, 更加适合云环境下组合电子健康记录的安全共享.

表 1 组合电子健康记录访问控制框架与已有方案对表

方案	云环境	组合电子健康记录	安全访问控制	多级安全访问控制
方案[1]	×	×	√	×
方案[2]	×	×	√	×
方案[9]	×	√	√	×
本文框架	√	√	√	√

3 结语

本文针对云环境下电子健康医疗信息的安全存储、访问和交换, 结合 XML 相关技术, 提出组合电子健康记录结构并用一个实例展示其结构; 结合基于属性的多级安全访问控制思想, 提出相应的组合电子健康记录访问控制策略, 进而构建云环境下组合电子健康记录访问控制框架. 与已有方案相比, 本方案在多级安全访问控制和组合电子健康记录方面具有优势, 本文提出的组合电子健康记录, 综合考虑不同电子健康记录间的逻辑关系, 并将相关电子健康记录以超链接的形式关联起来, 有利于电子健康记录的管理和分析; 基于属性的多级安全访问控制模型支持细粒度级别保护, 可控制多个文档、单一文档和文档部分内容的访问, 同时支持灵活制定和实施访问控制策略.

参考文献

1 Huang KH, Hsieh SH, Chang YJ, Lai FP, Hsieh SL, Lee HH. Application of portable CDA for secure clinical-document exchange. J Med Syst, 2010, 34(4): 531–539.

2 Pardamean B, Rumanda RR. Integrated model of cloud-based e-medical record for health care organizations. 10th WSEAS International Conference on E-Activities. 2011. 157–162.

3 Lupse OS, Vida MM, Tivadar L. Cloud computing and interoperability in healthcare information systems. The first International Conference on Intelligent Systems and Applications. 2012. 81–85.

4 Mansoor ME, Majeed R. Achieving interoperability among healthcare organizations[Master Thesis]. Blekinge Institute of Technology, 2010.

5 Lupse O, Vida M, Stoicu-Tivadar V. Using HL7 CDA and

CCD standards to improve communication between healthcare information systems. 2011 IEEE 9th International Symposium on Intelligent Systems and Information (SISY). IEEE. 2011. 453–457.

6 Vida M, Lupse O, Stoicu-Tivadar L. Improving the interoperability of healthcare information systems through HL7 CDA and CCD standards. 7th IEEE International Symposium on Applied Computational Intelligence and Informatics(SACI). IEEE. 2012. 157–161.

7 Yao Q, Wang Y, Li JS. Hospital information system integration based on cloud computing. 1st International Workshop on Cloud Computing and Information Security. Atlantis Press. 2013. 246–249.

8 Bahga A, Madisetti VK. A cloud-based approach to interoperable EHRs. IEEE J. Biomed. Health Inform, 2013, 17(5): 894–906.

9 Liu XM, Ma JF, Xiong JB, Liu GJ. Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data. International Journal of Network Security(IJNS), 2014, 16(4): 351–357.

10 Shen HB, Fan H. An attribute-based access control model for web services. 7th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06). IEEE. 2006. 74–79.

11 Wang GJ, Liu Q, Wu J. Hierachical attribute-based encryption for fine-grained access control in cloud storage services. Proc. of the 17th ACM Conference on Computer and Communication Security. ACM. 2010. 735–737.

12 Wan ZG, Liu JE, Deng RH. HABSE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. IEEE Trans. on Information Forensic and Security, 2012, 7(2): 743–754.

13 熊金波,姚志强,马建峰,李风华,李琦.基于行为的结构化文档多级访问控制.计算机研究与发展,2013,50(7):1399–1408.

14 Sicuranza M, Esposito A. An access control model for easy management of patient privacy in EHR systems. 2013 8th International Conference for Internet Technology and Secured Transactions(ICITST). IEEE. 2013. 463–470.

15 XML Encryption Syntax and Processing, W3C Recommendation 10 December 2002, http://www.w3.org/TR/2002/REC-xml enc-core-20021210/.

16 XML-Signature Syntax and Processing, W3C Recommendation 12 February 2002, http://www.w3.org/TR/2002/REC- xmldsig-core-20020212/.