· 急救大数据 ·

具有隐私保护机制的灾难医学救援监测系统设计与实现探索

赵小柯[1] 李静[2] 赵宇卓[3] 黎檀实[3]

[1]南京大学信息管理学院,江苏南京 210023;[2]北京交通大学经济管理学院信息管理系 100044;[3]解放军总医院急诊科,北京 100853

通信作者:黎檀实,Email:lts301@163.com

【摘要】 在充分研究国内外紧急灾难医学救援监测机制的前提下,分析国内灾难医学救援监测系统功能的需求,解放军总医院急诊科、北京交通大学经济管理学院信息管理系和南京大学信息管理学院共同设计了具有隐私保护机制的灾难医学救援监测系统的逻辑架构和数据结构,实现了汇报员信息管理、灾难医学救援数据上传、灾难医学救援数据搜索三大功能,并开发了Android客户端和Web客户端,方便接入系统。同时,该系统的隐私保护功能,基于对称可搜索加密算法实现了不可信服务器的加密存储,保证了医疗卫生数据的安全性,有益于我国灾难医学救援数据采集工作的进一步发展与完善。

【关键词】 可搜索加密; 隐私保护; 灾难医学救援监测; Android

基金项目:国家自然科学基金(81701961);北京市科技新星计划项目(XX2018019);解放军总医院医疗大数据科研项目(2017MBD-30);医疗大数据应用技术国家工程实验室(2017-148)

DOI:10.3760/cma.j.issn.2095-4352.2019.02.020

Exploration of design and practice of disaster medical rescue monitoring system with privacy protection mechanism

Zhao Xiaoke[1], Li Jing[2], Zhao Yuzhuo[3], Li Tanshi[3]

[1]School of Information Management, Nanjing University, Nanjing 210023, Jiangsu, China; [2]Department of Information Management, School of Economics and Management, Beijing Jiaotong University, Beijing 100044, China; [3]Department of Emergency, Chinese PLA General Hospital, Beijing 100853, China

Corresponding author: Li Tanshi, Email: lts301@163.com

【Abstract】 On the premise of fully studying the disaster medical rescue monitoring mechanism in emergencies at home and abroad, the functional requirements of the domestic disaster medical rescue monitoring system was analyzed in this paper, the logical framework and data structure of disaster medical rescue monitoring system with privacy protection mechanism was designed by department of emergency in Chinese PLA General Hospital, department of information management in School of Economics and Management of Beijing Jiaotong University, the School of Information Management of Nanjing University. Three major functional modules were realized in the system: reporter information management, disaster medical rescue data upload, and disaster medical rescue data search. Android client and Web client were developed for easy access to the system. The system also had the function of privacy protection. Based on symmetric searchable encryption algorithm, the system realized the encryption storage of untrusted servers and ensured the security of medical and health data. It is beneficial for the further development and improvement of disaster medical rescue data collection in China.

【Key words】 Searchable encryption; Privacy protection; Disaster medical rescue monitoring; Android

Fund program: National Natural Science Foundation of China (81701961); Science and Technology New Star Program of Beijing Municipal (XX2018019); Big-date Research and Development Project of Chinese PLA General Hospital (2017MBD-30); National Engineering Laboratory for Industrial Big-data Application Technology (2017-148)

DOI: 10.3760/cma.j.issn.2095-4352.2019.02.020

伴随着信息技术的飞速发展,云存储等技术为跨机构、多主体之间进行信息共享提供了便利[1]。近年来我国的自然灾害、紧急突发事件一直呈高发态势,在积极救灾的过程中,暴露出我国在大规模突发性事件应急响应过程中各组织之间缺乏信息共享、人员管理混乱、数据保存与录入不当等问题[2]。与此同时,大量数据缺乏隐私保护,导致患者隐私泄露的问题也是灾难医学救援监测系统的隐患。灾难医学救援数据来自于灾区医院就诊病例与健康中心、农村医疗保健站和疏散中心的收治记录,包含患者的隐私数据,理应在数据收集场景下进行隐私保护处理。灾难医学救援数据也是我国调配医疗资源、控制灾难医学救援的重要参考,数据的安全存储也是进行数据收集过程中应该考虑的问题。受地方医疗卫生机构条件限制,一旦后台的服务器出现异常,灾难医学救援数据的安全性只能由数据自身保证。

与发达国家相比,我国还没有较为成熟的灾难医学救援监测系统,在理论层面的研究还有很多欠缺,在具体的系统实现方面研究较少,如何建立一个适应我国灾难医学救援数据收集场景的灾难医学救援监测系统,是一个亟待解决的问

题。故我们设计了一种适应国内需求的具有隐私保护机制的灾难医学救援监测系统，实现了系统三大功能模块，为我国灾难医学救援监测工作的开展提供一定的参考。

1　国内外灾难医学救援监测系统研究现状

1979 年，美国就成立了美国联邦应急管理署（FEMA），通常通过电子可携带设备收集灾难医学救援数据。世界卫生组织（WHO）也曾主导设计了全球范围内第一个体系化的国际灾难医学救援信息监测系统（SPEED 系统）[3-4]，并在菲律宾、海地等国家实际灾难医学救援行动中得到推广和应用。SPEED 系统具有完善的灾难医学救援数据收集体系，日本后来也借鉴了这一系统。

中国疾病预防控制中心（CDC）曾于四川汶川大地震期间，在四川省 14 个重灾县组建起一款基于手机的紧急报告系统，共覆盖 38 种传染病情况[5-6]。该系统通过登记手机序列号、SIM 卡号的方式来确定汇报员的可信性，但弊端是成本的增加以及资源调配的不便性。

可搜索加密能很好地保证数据可用性，实现对密文的有效检索[7]。设计并实现一款具有隐私保护功能的灾难医学救援监测系统，对于我国灾难医学救援数据收集工作是一个很好的尝试，可以填补国内灾难医学救援数据收集工作研究的空白，基于可搜索加密算法的隐私保护机制的引入可以在数据收集过程中加强用户信息隐私保护，在满足灾难医学救援数据收集需求的同时，保障患者个人隐私权免受侵害。

2　灾难医学救援监测系统的设计

2.1　系统需求分析：系统的核心功能有灾难医学救援数据收集与预警、灾难医学救援数据管理、用户数据管理。根据处理的数据不同可将系统功能分为隐私数据管理和非隐私数据管理。隐私数据管理主要包括灾难医学救援数据收集、灾难医学救援数据加密存储、灾难医学救援数据预警；非隐私数据管理主要包括用户数据管理，其主要功能是对用户进行身份认证、发布系统公告、提供文件下载等。

2.2　系统逻辑架构设计：灾难医学救援系统逻辑架构见图 1。该系统分为表示层、业务层、数据层及基础设施层 4 层。

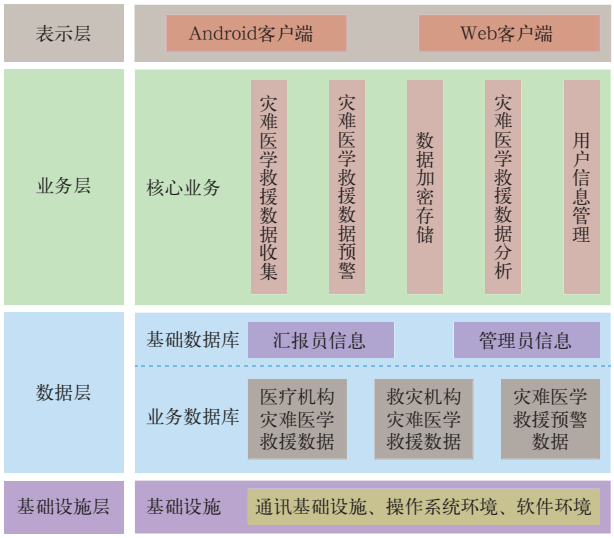

图 1　具有隐私保护机制的灾难医学救援监测系统逻辑架构

2.2.1　表示层：表示层实现了灾难医学救援数据汇报员、管理员与应用的交互，包括一个 Android 客户端与一个 Web 客户端。Android 客户端主要提供灾难医学救援数据上传、灾难医学救援数据查询等功能；Web 客户端进行用户管理，也可进行灾难医学救援数据上传等功能。

2.2.2　业务层：业务层是系统的核心部分，实现了系统的核心业务功能，负责处理表示层的操作，包括灾难医学救援数据收集与查询、灾难医学救援数据预警、数据加密存储、对灾难医学救援数据分析、用户信息管理等功能。

2.2.3　数据层：数据层主要负责操作数据库，分为基础数据库和业务数据库。基础数据库存储不需要加密的汇报员信息、管理员信息等数据；业务数据库存储需要进行隐私保护的业务数据，包括医疗机构和救灾机构的灾难医学救援数据以及灾难医学救援预警数据。

2.2.4　基础设施层：基础设施层指系统运行所需的通信基础设施、操作系统环境、软件环境等基础设施。

2.3　数据结构设计：系统设计的数据表包括医疗机构灾难医学救援数据表（tb_hos）、救灾机构灾难医学救援数据表（tb_ser）、灾难医学救援预警指标数据表（tb_zb）、灾难医学救援预警数据表（tb_yj）和用户信息数据表（tb_User）。其中医疗机构灾难医学救援数据表（tb_hos）结构见表 1，为了针对易感人群进行重点监测，收集灾难医学救援数据时 5 岁以下人群与 50 岁以上人群单独监控。

表 1　医疗机构灾难医学救援数据表结构

字段名	数据类型	字段说明
ID	INT	灾难医学救援数据记录序列号，自增主键
RCNO	VARCHAR（50）	病历编号
Hos_ID	VARCHAR（50）	医疗机构编号
Dis_ID	VARCHAR（50）	疾病编号
N_d5	VARCHAR（50）	5 岁以下病例数
D_d5	VARCHAR（50）	5 岁以下死亡数
N_u5	VARCHAR（50）	50 岁以上病例数
D_u5	VARCHAR（50）	50 岁以上死亡数
N_n5	VARCHAR（50）	5 岁以上 50 岁以下病例数
D_n5	VARCHAR（50）	5 岁以上 50 岁以下死亡数
R_Data	VARCHAR（50）	汇报日期
R_ID	VARCHAR（50）	汇报员编号

3　灾难医学救援监测系统实现

3.1　系统架构：本系统架构分为服务器端、用户端和数据库三部分，核心业务通过服务器端的服务连接器 Servlet 来实现。

3.1.1　服务器端：系统的服务器端采用数据访问对象（DAO）设计模式开发。

3.1.2　用户端：系统提供 Android 客户端和 Web 客户端两种接入方式。Android 客户端采用 Android 9.0 版本开发，通过网络访问接口连接 Servlet 实现灾难医学救援数据上报、灾难医学救援预警等功能。Web 客户端则通过“汤姆猫”（Apache Tomcat）提供的 Web 服务器连接 Servlet 来实现业务操作。

3.1.3　数据库：使用 java 数据库连接（JDBC）接口来访问 MySQL 数据库，本系统共有 2 个 MySQL 数据库，一个存储

灾难医学救援监测数据，一个存储用户信息。

3.2 Android 客户端实现：Android 客户端用户通过点击 APP 图标登录系统，输入 Web 客户端注册时填写的用户名与密码，通过验证进入灾难医学救援监测系统菜单界面（主窗体），用户可以通过主窗体调动相关各个功能子模块，如灾难医学救援数据上报、灾难医学救援数据查询、系统设置、地图定位等。单击主窗体中的功能按钮即可打开相应功能的应用程序组件 Activity。

3.3 Web 客户端实现：Web 客户端通过 Apache Tomcat 内置的 Web 服务器访问 Servlet，系统的内部业务 Servlet 是客户端通用的。设置 Web 客户端和 Android 客户端是为了方便汇报员随时随地汇报数据，地方救灾管理部门也可以在通信不便的地区设置专人负责数据录入。

3.4 隐私保护功能实现：该系统的隐私保护功能采用对称可搜索加密算法，通过将分组加密后得到的密文与一个具有特殊结构的伪随机比特流按位异或，得到的比特流可以实现可搜索加密，在对数据进行搜索的同时不会泄露有关明文的其他信息。

在数据加密的场景中，采用高级加密标准算法对隐私数据进行加密。加密之后得到密文序列，其中密文 $X_i=E(W_i)$，为了避免出现无法解密的问题，将预加密后的词 X_i 分割成 L_i 和 R_i 两部分，其中 L_i 对应 X_i 的前 $n-m$ 个比特，R_i 对应其余 m 个比特，将预加密之后的词 X_i 与陷门 $T_i=\langle S_i, F_{k''}(S_i)\rangle$ 逐位异或，其中 S_i 为伪随机位，$F_{k''}(S_i)$ 为 S_i 的伪随机函数，$k''=f_k(S_i)$。S_i 与，$F_{k''}(S_i)$ 的长度分别对应 L_i 与 R_i。

在数据查询的场景中，客户端需要用户本地输入关键字 w 与密钥 K，在本地生成关键字陷门 $T_k(w)$，将陷门上传至服务器，服务器通过陷门与密文异或，将密文与 $F_{k''}(S_i)$ 对比，若相等则证明该组密文是包含关键字 w 的目标数据，服务器端将密文返还给客户端。客户端收到目标数据之后，使用密钥 K 进行解密得到明文。

3.5 服务器端实现：采用浏览器 / 服务器（Browser/Server）结构，核心业务模块包括汇报员信息管理模块、灾难医学救援数据上报模块、灾难医学救援数据查询模块。

3.5.1 汇报员信息管理模块：本模块主要实现用户注册功能，让汇报员通过 Web 客户端进行注册，定义注册提交类，获得用户操作类以启动数据库连接和关闭数据库连接，相应接口中定义汇报员注册需要用到的方法。

3.5.2 灾难医学救援数据上报模块：本模块是为了实现灾难医学救援数据收集功能，以医疗机构灾难医学救援数据上报为例，定义医学救援数据提交类，获得医疗机构灾难医学救援数据上报操作类，进行启动数据库连接和关闭数据库连接的操作，相应接口中定义医疗机构灾难医学救援数据上报需要用到的方法。

3.5.3 灾难医学救援数据查询模块：查询灾难医学救援数据需要获取用户持有的口令 Key 值与搜索关键词，可以基于汇报日期、汇报员编码、医疗机构编码或地区编码来搜索灾难医学救援数据。以医疗机构编号为例，定义用于跳转的类，定义根据医疗机构编号查询灾难医学救援数据的方法类，通过 Service 查询出相应的记录，解密后通过 Action 跳转。

4 总结与展望

充分吸收借鉴 SPEED 系统在灾难医学救援监测场景下的优势，探索性地提出了一个符合我国国情的灾难医学救援信息监测系统框架。系统采用 Browser/Server 结构，使用 Web 服务器，建设成本较低；通过 Web 客户端和 Android 客户端均可进行灾难医学救援信息上报与查询，在通讯网络中断的场景下，可以设置专人负责通过 Web 客户端进行信息录入和查询，更为灵活。采用 APP 来代替现有的手机固件，便于就地组建灾难医学救援信息监测小组，扩展监测范围，降低成本。另外，该系统还具有隐私保护机制，避免了不可信的第三方服务器的威胁。系统设计与实施均从便于救灾主管单位在灾难发生地快速建设系统、组建信息监测团队、建立起标准化的信息监测机制的需求出发，具有易于推广、易于建设、安全性好的优点。

当然，本研究仍存在不足之处，下一阶段将深入研究：① 多关键词可搜索加密实现：本系统采用单关键词可搜索加密算法，但实际应用中难免会应用到多关键词搜索的场景，下一步将更新隐私保护算法，实现多关键词可搜索加密算法，提高系统灵活性。② 用户强身份认证登录的实现：本系统身份认证是通过校验汇报员编码实现的，安全性较低，且存在编码更新、管理困难的问题，进一步将实现动态口令身份认证，Web 客户端扫描二维码登录。

利益冲突 所有作者均声明不存在利益冲突

参考文献

[1] 赵宇卓，王俊梅，潘菲，等. 急救数据库建设初探 [J]. 中华危重病急救医学，2018, 30 (6): 609-612. DOI: 10.3760/cma.j.issn.2095-4352.2018.06.022.
Zhao YZ, Wang JM, Pan F, et al. Pilot research: construction of emergency rescue database [J]. Chin Crit Care Med, 2018, 30 (6): 609-612. DOI: 10.3760/cma.j.issn.2095-4352.2018.06.022.

[2] 封宗超，李运明，郝新忠，等. 突发事件医疗信息统计存在问题及对策 [J]. 解放军医院管理杂志，2011, 18 (10): 915-916. DOI: 10.3969/j.issn.1008-9985.2011.10.008.
Feng ZC, Li YM, Hao XZ, et al. Medical information statistics in the disaster and emergency events [J]. Hosp Administration J Chin PLA, 2011, 18 (10): 915-916. DOI: 10.3969/j.issn.1008-9985.2011.10.008.

[3] WPRO. Surveillance in post extreme emergencies and disasters (SPEED) [EB/OL]. (2012-04-11) [2018-08-17].

[4] 李静，李梅，赵宇卓，等. 国际灾难医学救援信息监测系统的启示 [J]. 中华危重病急救医学，2018, 30 (6): 526-530. DOI: 10.3760/cma.j.issn.2095-4352.2018.06.005.
Li J, Li M, Zhao YZ, et al. Enlightenment from the surveillance in post extreme emergencies and disasters [J]. Chin Crit Care Med, 2018, 30 (6): 526-530. DOI: 10.3760/cma.j.issn.2095-4352.2018.06.005.

[5] Yang C, Yang J, Luo X, et al. Use of mobile phones in an emergency reporting system for infectious disease surveillance after the Sichuan earthquake in China [J]. Bull World Health Organ, 2009, 87 (8): 619-623.

[6] Guo Y, Su XM. Mobile device-based reporting system for Sichuan earthquake-affected areas infectious disease reporting in China [J]. Biomed Environ Sci, 2012, 25 (6): 724-729. DOI: 10.3967/0895-3988.2012.06.016.

[7] Goldreich O, Ostrovsky R. Software protection and simulation on oblivious RAMs [J]. JACM, 1996, 43 (3): 431-473. DOI: 10.1145/233551.233553.

（收稿日期：2018-08-20）