

数字时间戳技术在电子病历中的应用

孙萧寒

(渭南师范学院 计算机科学系, 渭南 714000)

摘要 数字时间戳可以为电子文件提供准确的时间, 并可以检验出文件在加上时间戳后是否被更改过。基于数字时间戳的线性链接机制、树型机制的优缺点, 提出了混合模式, 即整体结构使用树型机制, 内部结构使用链接机制, 该模式不需要安全信任 TSA, 并且验证时间也不会过长。针对电子病历存在的安全性问题, 利用混合模式分别由病人和医生对病历和诊断加盖时间戳, 使病历和诊断都具有一定的可靠性和匿名性。

关键词 数字时间戳 线性链接机制 树型机制 电子病历

中图法分类号 TP309.7; 文献标志码 A

1 数字时间戳技术

数字时间戳技术是数字签名技术的一种变种应用, 它可以为任何电子文件提供准确的时间证明, 并且可以检验出文件自加上时间戳后是否曾被人修改过^[1-3]。数字时间戳需要一个大家都公认的时间机关, 即时间戳权威(TSA)^[4-6]。

2 数字时间戳机制

2.1 线性连接机制^[7]

设第 n 个时间戳的协议过程如下:

(1) 用户 S 发送 y_n 和 ID_n 给 TSA, 其中 ID_n 是 S 的 ID, y_n 是第 n 个文档 X_n 的摘要;

(2) TSA 发回 $S_n = \text{SIG}_{\text{TSA}}(n, t_n, ID_n, y_n, L_n)$, 其中 t_n 是当前时间, L_n 是由下列递归方程定义的链接信息: $L_n = H(t_{n-1}, ID_{n-1}, y_{n-1}, H(L_{n-1}))$;

(3) 处理完下一请求后, TSA 发送 ID_{n+1} 给 S, (ID_{n+1}, S_n) 就是完整的时间戳。

当质疑时间戳时, S 出示 (ID_{n+1}, S_n) , 并请用户 ID_{n+1} 出示 (ID_{n+2}, S_{n+1}) , 其中 $S_{n+1} = \text{SIG}_{\text{TSA}}(n+1,$

$t_{n+1}, ID_{n+1}, y_{n+1}, L_{n+1})$, 而 $L_{n+1} = H(t_n, ID_n, y_n, H(L_n))$ 。若发现 S_n 与 L_{n+1} 不符合, 则验证失败。若两者符合, 但仍不放心, 可以去找 $ID_{n+2}, ID_{n+3} \dots$ 直至满意或发现有不符合的 L_{k+1} 和 S_k 为止。

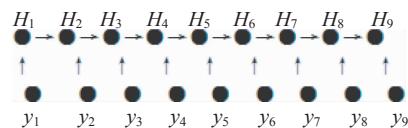


图 1 线性链接机制

2.2 树型机制^[8]

树型机制中时间戳被分成轮, 第 r 轮的时间戳 R_r 是第 $r-1$ 轮的时间戳 R_{r-1} 和第 r 轮内提交的所有文档累积的 Hash 值。第 r 轮中提交的文档被组织成一棵二叉树 T_r 。

用户如果想在这一轮中为至少一个文档盖上时间戳, 那么该用户就应当提交文档的 Hash 值。树的叶子 Y_r, i 是提交的文档。内部节点 k 是子节点的 Hash 值, $H_k = H(H_k, H_{K_L}, H_{K_R})$, 其中 K_L 和 K_R 分别是 k 的左右子节点, H 是 Hash 函数。

在图 2 中树根 $R_r = H(R_{r-1}, H_6)$, 是第 r 轮的时间戳, TSA 只储存每一轮的 R_r 。

2.3 混合模式

混合模式是指把线性链接机制和树型机制结合起来, 整体结构采用树型机制, 每一轮内采用线性机制。用户对自己的文档加上自己时间戳(如电

脑时间等)发给 TSA 加他们的时间戳。

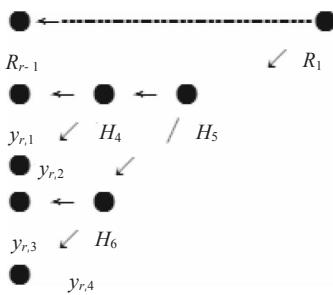


图 2 树型机制

3 混合模式的数字时间戳技术在电子病历中的应用

3.1 电子病历加盖时间戳流程

病历对医院、病人还有医生都具有重要的意义。电子病历有很多优点:如,提高工作效率;辅助医生做出判断;方便病人信息的异地共享等^[3]。但电子病历的安全问题是制约其发展的瓶颈。如何进行电子病历的认证等问题亟待解决。

电子病历涉及到三方实体:医生、病人和第三方(TSA 或病历管理员)。

病人首先获得第三方的公钥,填写自己的病历,加上自己的时间戳并保存,然后用自己的私钥加密病历,再用第三方公钥加密后发送给第三方。第三方收到病历后,加盖自己的时间戳并保存。只有病人有病历的修改权。病人每次修改病历后都要加盖时间戳保存,再用第三方公钥加密后发送给第三方。

医生首先从第三方获得用第三方私钥解密后的病人病历,医生用病人的公钥再次解密后查阅病人病历,但医生只有查阅权限。医生做出诊断后,写病历诊断,加盖自己的时间戳,用自己的私钥加密,最后用第三方公钥加密后发送给第三方,第三方把获得的病历诊断加盖自己的时间戳并保存。医生在每次修改后都会加盖时间戳保存,再用第三方公钥加密后发送给第三方。

第三方把病人的病历和医生的病历诊断保存

起来,并给这个病历随机产生一个 ID 号,作为一个树根把病历和病历诊断链接起来,而每个病历和病理诊断又可以与它的前后一个病历和病历诊断形成一个线性链接。

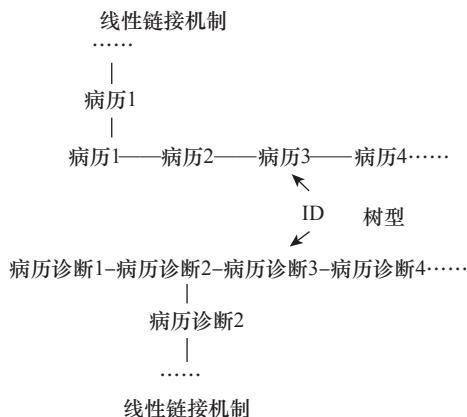


图 3 病历与病历诊断结构图

3.2 电子病历的安全性分析

线性机制的优点是难于伪造,但是它的验证时间太长^[7];树型机制验证过程虽然简单,但是它无法提供每一轮内的文档时间比较而且必须相信 TSA^[8]。

利用混合机制对电子病历加盖时间戳,它的优点是很难伪造病历,也容易验证^[9]。它的缺点是需要一个独立的绝对可靠的第三方。如果这第三方和医生或病人串通就可以伪造病历或病历诊断^[10,11]。

参 考 文 献

- 1 Stalling W,密码编码学与网络安全:原理与实践(第三版). 杨明,等译. 北京:电子工业出版社,2004
- 2 冯登国. 公开密钥基础设施. 北京:人民邮电出版社,2001
- 3 王 勇,朱方金,史清华. PKI 中数字时间戳技术. 大连理工大学学报,2003;43:27—29
- 4 钟 声,邱 钢,孙红兵. 基于时间戳的密码身份认证方案. 计算机应用,2006;26:71—72
- 5 潘 勇,徐向阳,潘龙英,等. 前向安全数字签名在证书管理中的应用. 科学技术与工程,2006;6(5):621—624
- 6 吕婉丽,钟 诚. 数字签名方案的分析. 广西科学院学报,2002;18(4):161—164
- 7 张科伟,唐晓波. 时间戳协议研究. 计算机应用研究,2004;10:100—103

(下转第 7054 页)

A Simplified Difference Matrix of the Attribute Reduction Method

HAO Wei-lai, ZHANG Xue-bin

(Heilongjiang Institute of Science and Technology Graduate Institute, Harbin 150027, P. R. China)

[Abstract] Difference matrix for the existing algorithm for attribute reduction defects, and by differences in matrix reduction properties of more complex process. Some improvements, conditions of property classified by group, representative records to generate the different extraction matrix are made of, simplified the difference matrix of order and the demand reduction properties of complexity. Thus the time complexity and space complexity of the optimization are done, saved time and space algorithm complexity. Examples show that the algorithm can effectively attributes reduction, access to the desired results, and the improved algorithm is simple and efficient.

[Key words] difference matrix reduction domain

(上接第 7046 页)

- | | |
|--|--|
| 8 张科伟, 唐晓波. 时间戳协议研究. 计算机应用研究, 2004; 43 (10): 27—29 | 10 胡亮, 初剑峰, 林海群, 等. IBE 体系的密钥管理机制. 计算机学报, 2009; 32(3): 543—551 |
| 9 张仁辉, 王晓明. 电子病历管理系统的设计与实现. 微计算机信息, 2009; 25(3): 267—269 | 11 张仕斌, 何大可, 代群. PKI 安全认证体系的研究. 计算机应用研究, 2005; 7: 127—130 |

The Research on the Application of Digital Time-stamp Techniques in Electronic Medical Records

SUN Xiao-han

(Weinan Teachers University, Weinan 714000, P. R. China)

[Abstract] Time-stamp can provide accurate time for electronic files and test if the file added time-stamp has been modified. Based on the advantages and disadvantages of the linear-linking scheme and tree-like scheme, a hybrid model is introduced, which creates the integral structure in tree-like scheme and the internal structure in linear-linking scheme needs no complete trust to TSA and the very long verifying time. Patients seal time-stamp on their medical records and doctors on their diagnosis based on the hybrid model to solve the secure problems of electronic medical records. Both patients' medical records and doctors' diagnosis have anonymity and reliability to a certain degree.

[Key words] digital time-stamp linear-linking scheme tree-like scheme electronic records