Twofish 加密算法在医院远程信息系统中的应用

李建文,孔凤娟

(陕西科技大学 电气与信息工程学院,陕西 西安 710021)

摘 要:为了解决医院远程信息系统客户端的数据安全问题,提出利用 Twofish 加密算法对客户端数据进行加密的算法。该算法的引入有效克服了手机内存的有限性对加密技术的影响,对系统的安全性进行优化。在对 Twofish 算法加密过程研究的基础上,设计出基于 Java 客户端代码的安全实现,并通过测试。

关键词:医院远程信息系统;数据安全;Twofish;加密技术;Java

中图分类号:TP311.1 **文献标识码**:A **文章编号**:1674-7720(2011)03-0012-03

The applications of Twofish using in the remote information system

Li Jianwen, Kong Fengjuan

(College of Electric & Information Engineering, Shaanxi University of Science & Technology, Xi'an 710021, China)

Abstract: In order to solve the hospital information system data remote client security problems, using Twofish encryption algorithm for client data encryption algorithm is introduced. The mobile phone memory effectively overcome the limitation of encryption technology, so as to affect the security of the system is optimized. Based on Twofish algorithm encryption process on the basis of this, the client is designed based on Java code, and through the safety test.

Key words: remote information system using in hospital; data security; Twofish; encryption technology; Java

在移动信息化迅速发展的今天,移动终端特别是手机在我国医疗事业上的应用尚未得到很好的发展,制约其发展有多方面原因,其主要原因还是安全性问题[2]。医院工作质量的好坏取决于医院信息系统的完善与否,因此对医院信息系统的安全运行提出了更高要求。随着信息技术的发展,医院信息系统通常已具备较高的安全性,而数据安全却一直存在隐患。数据安全隐患主要体现在信息的截获、窃取、篡改和假冒上。

移动设备应用中最薄弱环节是客户机端设备,所以信息的安全性就显得尤为重要。

由于医院远程信息系统涉及到病人的私人信息及医院的机密治疗技术,如果系统再一步扩展还要涉及到金钱的交易等,因此对安全性要求会更高。无线环境中的安全受信道、手持设备等本身特有因素的影响,因此安全性难以保证。确保无线环境中的安全性(特别是对传输数据的保护)是系统首先应该解决的问题。

该项目通过一种加密算法对客户端数据进行加密,确保在数据信息传输过程中的安全。但是考虑到手机内存的有限性,本文利用一种更加适用于手机等这种小容量设备的加密认证技术,即基于 Twofish 算法的加密技术,使手机成为更加可靠的应用终端,使该远程信息系统真正得到完善和扩展。

1 Twofish 算法的提出

作为一种标准的数据加密算法,DES (Data Encryption Standard) 的密钥长度对于现在计算机的运行速度来说,在某些高机密的场合显得有点不足,已经不再安全,因此出现了一种更高标准的加密算法 AES (Advanced Encryption Standard)代替了原来的 DES。首先这种加密算法必须是块加密,因为块加密可以被用来对数据流进行加密,也可以被用来制造一些专用的数据加密设备。其次,这种加密算法必须使用更长的密钥,更大的加密块,更高的加密速度和灵活性。Twofish 则是 Counterpane 公司向 NIST 提交的一种满足 AES 要求的加密算法。Twofish 采用 128 bit 数据块,128/192/256 bit 可变长度密钥。Twofish 算法是进入 NIST 第二轮 5 种加密算法中的一种,具有加密速度快、结构简单容易实现、无

弱密钥、适应性强[1]等特点。

基于 Twofish 算法特点及应用性能，远程信息系统采用此算法对系统的安全性进行优化，使系统能适用手机等移动设备的无线环境，同时能让用户使用起来更加放心。

2 Twofish 算法的加密过程

Twofish 算法的加密过程如图 1[3]所示：开始处 P(plain text)表示需要进行加密的 128 bit 数据，即 16 B。然后将这 16 B 分为 4 组，每组 32 bit，即 4 B。在循环之前首先对这四组数据分别用 $k0$、$k1$、$k2$、$k3$ 进行异或操作，称之为 input whitening；然后对异或后的数据分组进行计算，计算后将 1~3、2~4 组的数据对换，如此循环 15 次，再 1~3、2~4 对换一次。对这 4 组数据分别用 $k4$、$k5$、$k6$、$k7$ 异或操作，称之为 output whitening；最后将这 4 组数据组合成 16 B 的数据，也就是最后的密文 C(cipher text)，长度与加密前的同样是 128 bit。具体来说，加密前的 plain text 是 128 bit，也就是 16 B。假设这 16 B 分别是 p0，…，p15，将 p0，…，p15 分为 4 组，即 P0，…，P3，四个字先进行下面的数学运算：

$$P(i)=\sum_{i=1}^{n}(4i+j)2^{8},\text{其中 } i,j=0,\cdots,3$$

在输入阶段，这些字与 4 个密钥扩展进行异或运算：

$$R(0,i)=P(i)\oplus K(i),\text{其中 } i=0,\cdots,3$$

在 16 次循环的每一次中，4 组数据的前两组与当前循环次数通过 F 进行计算，计算出 2 组数据。第 3 组数据与计算出的第 1 组数据“异或”，然后向右循环移动一位。第 4 组数据向左循环移动一位，然后异或计算出的第 2 组数据。然后将 1~3、2~4 组数据对换，作为下一轮计算的数据。程序表示如下：

$$(F(r,0),F(r,1))=F(R(r,0),R(r,1),r)$$
$$R(r+1,0)=ROR(R(r,2)\oplus F(r,0),1)$$
$$R(r+1,1)=ROL(R(r,3),1)\oplus F(r,1)$$
$$R(r+1,2)=R(r,0)$$
$$R(r+1,3)=R(r,1)$$

这里 $r=0,\cdots,15$，ROR 和 ROL 是一种循环移位函数，根据的第二个参数来决定是左移还是右移第一个参数。

输出阶段不再在最后一轮进行交换。而只是将结果与 4 个钥字进行异或。

$$C(i)=R(16,(i+2)\bmod 4)\oplus K_{i+4},\text{其中 } i,j=0,\cdots,3$$

在加密过程中，Twofish 使用了两个函数即 F 函数和 G 函数。G 函数是 Twofish 的核心，输入一个字并让该字的每一个字节通过一个不同的依赖于密钥的 S 盒，然后输出 4 个字节，用矩阵表示为：

$$\begin{bmatrix}Y0\\Y1\\Y2\\Y3\end{bmatrix}=\begin{bmatrix}01 & EF & 5B & 5B\\5B & EF & EF & 01\\EF & 5B & 01 & EF\\EF & 01 & EF & 5B\end{bmatrix}\cdot\begin{bmatrix}X0\\X1\\X2\\X3\end{bmatrix}$$

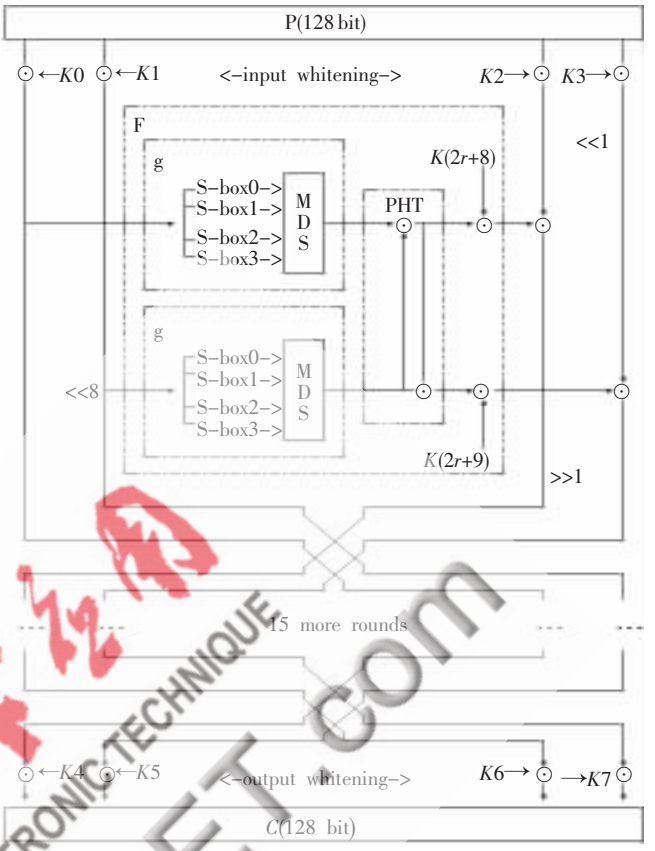

图 1 Twofish 加密过程

其中：$X0$、$X1$、$X2$、$X3$ 是输入字节，$Y0$、$Y1$、$Y2$、$Y3$ 是输出字节。

F 函数是一个基于 64 bit 的密钥独立的交换过程，它带 3 个参数、2 个输入字 R0 和 R1，以及轮数 r（用来选择合适的字密钥）。R0 通过 G 函数传递，它产生 T0；R1 被左移位 8 bit，然后通过 G 函数产生 T1。T0 和 T1 被结合并加入两个密钥扩展字。

$$T0=G(R0)$$
$$T1=G(ROL(R1,8))$$
$$F0=(T0+T1+K_{2r+8})\bmod 2^{32}$$
$$F1=(T0+2T1+K_{2r+9})\bmod 2^{32}$$

由上面的过程描述可以看出，Twofish 是一个用 32 bit 的伪哈德马转换 PHT 混合函数的输出。伪哈德马转换 PHT(Pseudo Hadamard Transforms)是一种简单快速的混合操作，例如给出 2 个输入值 a 和 b，则 32 bit 的 PHT 操作可以被定义为[3]：

$$a'=a+b \bmod 2^{32}$$
$$b'=a+2b \bmod 2^{32}$$

3 利用 Twofish 算法优化客户端

本项目对数据安全的设计是在不改变用户硬件、不改变底层通信协议(如 Http 等)的基础上通过应用层的解决方案来保证数据不在路途被篡改、截取或假冒。

根据上述原则，得出如图 2 所示的系统安全性研究的总模型和工作流程图。

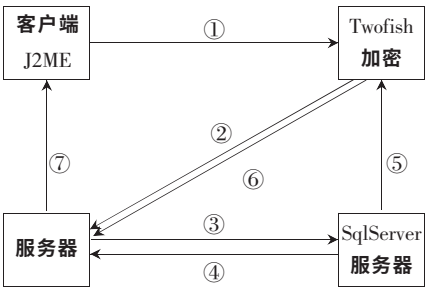

图 2 系统的工作流程

说明：

①表示客户将输入的数据信息（用户登录、用户查询、注册、预约等）发送给服务器端，同时将输入的信息利用 Twofish 算法进行加密。

②对输入的登录信息进行加密后再传给服务器。

③表示服务器通过 JDBC 访问后台数据库，利用 SQL 语句对数据库进行查询、修改等操作。

④如果没有查到数据或输入信息有误则返回给服务器，同时将没查到结果或错误信息返回给客户端。

⑤表示如果在数据库中查询到与 SQL 语句条件相匹配的数据信息，将此信息连同用户登录信息一起进行 Twofish 加密。

⑥表示将加密后的所有信息返回至服务器。

⑦表示服务器处理完之后再逐级返回，直到用户得到相应的查询信息成功或登录失败信息。

4 优化后的系统客户端的代码设计

系统设计均采用 Java 语言实现各种安全功能，其中使用的算法提供者采用了 Bouncy Castle JCE，因为在众多的提供者中，它是最安全的，并可免费获得。首先，在原来系统的基础上增加一个类 hosTwofish，接着就要考虑如何将客户端的数据进行加密传输和将查询到的数据查询后再解密显示于客户端。其实 Twofish 加解算法已经比较完善了，现在主要任务是如何把此算法运用于该系统数据加/解密中。一个最简单的方法就是在原来的数据操作的过程前后分别调用该类的加密方法 blockEncrypt(byte[] input, int inOffset, object sessionKey)，其中 input 表示明文，inOffset 表示数据开始的位置，sessionKey 表示用于加密的会话密钥；解密方法 blockDecrypt(byte[] input, int inOffset, object sessionKey)，其中 input 表示密文，inOffset 表示数据开始的位置，sessionKey 表示用于解密的会话密钥。然后创建一个类 HosTwofish 对象 hosTwofish，再通过调用解密方法 blockEncrypt()对输入的信息 sessfonKey 进行加密。同理，解密同样先创建对象 hosTwofish，再通过调用解密方法 blockDecrypt()对查询到的数据信息 sessionKey 进行解密，然后通过 XML 字符解析返回至客户端。

5 测试应用效果

为了说明 Twofish 算法应用到医院远程信息系统中保证数据传输安全的有效性和优越性，本文对系统的数据安全性进行了测试，从两个方面说明了 Twofish 算法应用到医院远程信息系统优点。

(1)对访问的速度影响小

加密算法选择的不合适就会影响系统的访问时间。采用 Twofish 算法进行加密处理对系统的响应时间影响不大，而用普通的加密技术，则会使系统的响应时间明显增加。

(2)数据的安全性得到很好的保证

通过大量的系统测试发现，系统有很好的安全性，没有出现过数据丢失和数据被修改的现象。

将 Twofish 算法应用到医院远程信息系统用以保证数据的安全性是系统的一个显著创新。项目从保证数据远程传输的安全性出发，综合考虑手持设备内存局限性及访问的数据量，优化客户端设计，使构建的系统具有较强的应用性和实用性。

参考文献

[1] 李占江.Twofish 算法的优化及其在移动支付系统中的实现[J].微计算机信息，2007，23(12)：6-8.

[2] 沈崇德.无线移动技术在现代医院管理中的应用[J].中国数字医学，2009，4(4)：14-16.

[3] 刘知贵，杨立春，蒲洁.基于 Twofish 算法的标书加解密研究[J].计算机应用，2004，24(6).

[4] 张和君，张跃.远程心电监护软件系统的设计与实现[J].计算机工程与应用，2006，42(15)：219-224.

[5] PU ZHANG, YUICHI KOGURC, HIROKI MATSUOKA, et al. A remote patient monitoring system using a Java-enabled 3G Mob. Proceedings of the 29th Annual International Conference of the IEEE EMBS clte internationale, Lyon, France, 2007, 8.

(收稿日期：2010-09-01)

作者简介：

李建文，男，1959 年生，教授，主要研究方向：嵌入式系统及应用。

孔凤娟，女，1980 年生，硕士研究生，主要研究方向：嵌入式系统及应用等。