电子银行系统的设计

杨小远[1] 陈旺虎[2]

(北京航空航天大学理学院数学系 北京100083)[1]

(西北师范数学与信息科学研究院计算机系 兰州730070)[2]

摘 要 本文通过作者在电子商务系统开发项目中的实践和学习,详细描述了一个电子银行系统的总体设计与实现,特别是对该系统中用到的电子商务安全策略进行了较为详尽的描述。

关键词 电子银行,支付网关,电子银行服务器,数字签名,证书,密钥协商

The Designing of A Electronic Bank System

YANG Xiao-Yuan[1] CHEN Wang-Hu[2]

(Beihang University, Deperment of Mathematile, Beijing100083, China)[1]

(Northwest Normal University, College of Mathmatice and information Science, Lanzhou 730070, China)[2]

Abstract The paper describes the designing of a electronic bank system on the basis of the experience on the development of electronic commerce application. Especially, the author detailed for the security mechanism of electronic commerce system.

Keywords Electronic bank system, Payment gateway, Electronic bank server, Digital signature, Digital cert, Keys negotiation

1 概述

互联网已引起了人类生活翻天覆地的变化,而电子商务应用的出现,必将使人们的生活模式发生许许多多的变化。电子银行系统正是电子商务在金融领域的成功应用。

本文根据作者在电子商务活动中长时间的实践和对国外成功电子银行系统的了解,就电子银行系统的设计、安全、性能等方面的问题进行了较为详细的阐述。电子银行系统是指利用网络手段实现银行的部分或全部功能的一种途径。电子银行系统允许个人用户或企业用户在网上完成相应的银行业务,具体包括帐号挂失、不同帐号间的转帐、帐号密码的更改、帐号余额的查询等等。

2 电子银行系统的总体结构

电子银行系统所涉及的实体包括:客户(个人或企业)、电子银行服务器、支付网关、银行以及电子商务安全机制所涉及的各个实体,如证书的认证机构等。

电子银行系统的一般体系结构可表示如图1。

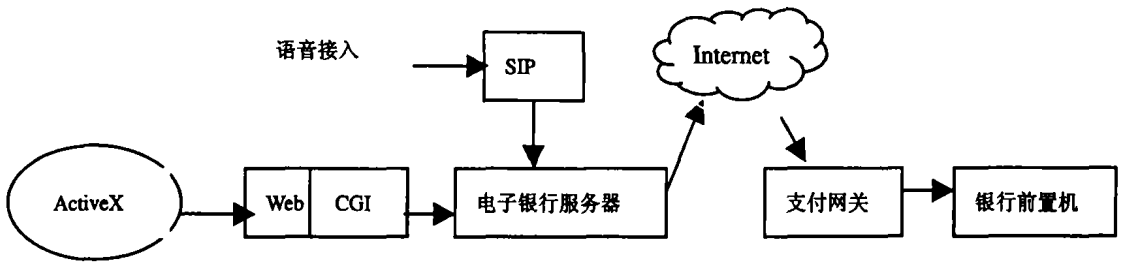

图1

在上述系统中:

客户通过浏览器或电话来传递信息,这些信息包括输入信息(帐号、密码及操作参数等)和输出信息(操作结果)。

电子银行服务器和支付网关之间是通过 Internet 连接的,一个电子银行服务器可以连接多个支付网关。电子银行服务器首先要根据传递信息中的银行代码,将从 CGI 接收到的信息传递到不同的支

杨小远 硕士,教授,主要从事信息数学和 Web 信息系统方面研究。陈旺虎 硕士,讲师,主要从事 Web 信息系统方面研究。

付网关。同时，电子银行服务器还要负责把响应信息发送给 CGI。

179用户通过电话输入交易信息，SIP 将用户的交易信息转发给电子银行服务器，然后由电子银行服务器把 SIP 的消息格式转换成支付网关所能理解的格式，电子银行服务器同时负责将支付网关的返回信息转换为 SIP 所能理解的格式，最后由 SIP 将交易结果信息通过电话通知用户。

支付网关的主要功能是进行协议的转换，首先，支付网关要把电子银行服务器发送来的加密信息进行解密以得到明文信息，然后要对明文信息进行 ISO8583编码，再把 ISO8583包发送给银行。其次，支付网关起到隔离银行内部网络和公众网的作用，保证银行内部网的安全性和不变性。

当支付网关接收到银行前置机发送来的返回数据后，支付网关要对数据进行 ISO8583包的解码。然后用用户的证书进行加密发送给电子银行服务器。

从以上的描述可以看出，银行内部网只需向电子银行平台提供发送和接收数据的接口，其余的工作流程并不发生任何改变，这从根本上保证了电子银行系统的可行性和银行内部网的安全性。

3 电子银行系统的安全机制

勿庸置疑，电子银行系统的安全性是至关重要的。电子银行系统的安全机制是由证书认证机制进行保证的。证书认证机制要求参与整个商务活动的任何实体(包括软件平台)都需要拥有一个合法的证书。所谓合法的证书是指该证书是由一个权威的机构所发放并认证签名的。每个实体的证书包含了证书持有者的公钥、身份信息、上级证书的签名信息等。两个实体在互相通讯时主要采用非对称加密(公开密钥加密)的方式，即当一个实体向另一实体发送数据时用对方的数字公钥来加密传送数据；当对方接受到加密后的密文时用自己的私钥来解密接收到数据。因为，私钥是在本地保存的，不需要在网上传送，而公钥是公开的，所以，极大地保证了数据传输的安全性。

很显然，参与电子银行活动的各个实体要对自己的行为负相应的责任和连带责任，因此，要求参与该活动的实体要对自己的每个操作进行数字签名，当出现交易纠纷时以做凭证。同时，当一个证书的上级发放单位出现工作上的失误时同样要负连带责任，因此，当发放证书时上级证书要在每个发放证书上签名，从而保证了上级证书发放单位工作的公正性。

图2为中国点心 CTCA 证书认证体系的大致表示：

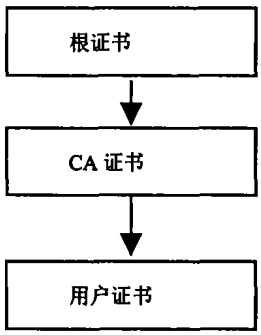

图2

现以电子银行系统的一次数据传送为例，对其安全策略表示如下：

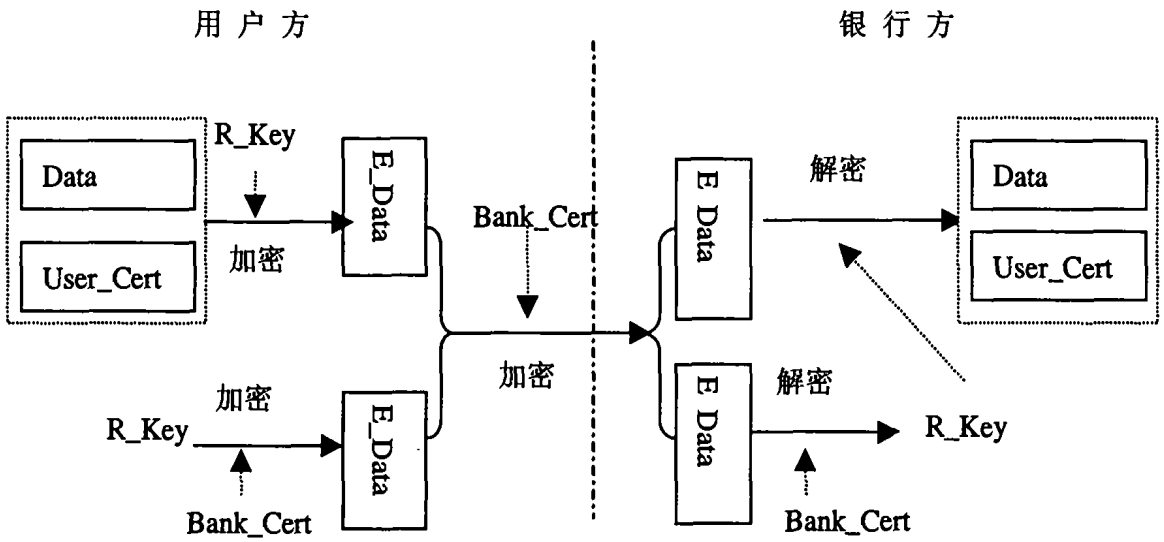

图3

符号说明：

Bank_PrivateKey——银行私钥

Bank_PublicKey——银行公钥

User_PrivateKey——用户私钥

User_PublicKey——用户公钥
User_Cert——用户证书
Bank_Cert——银行证书
Data——明文数据
E_Data——密文数据
R_Key——随机生成的对称密钥
(1)用户请求信息中的敏感信息的加密
(2)银行响应信息中的敏感信息的加密

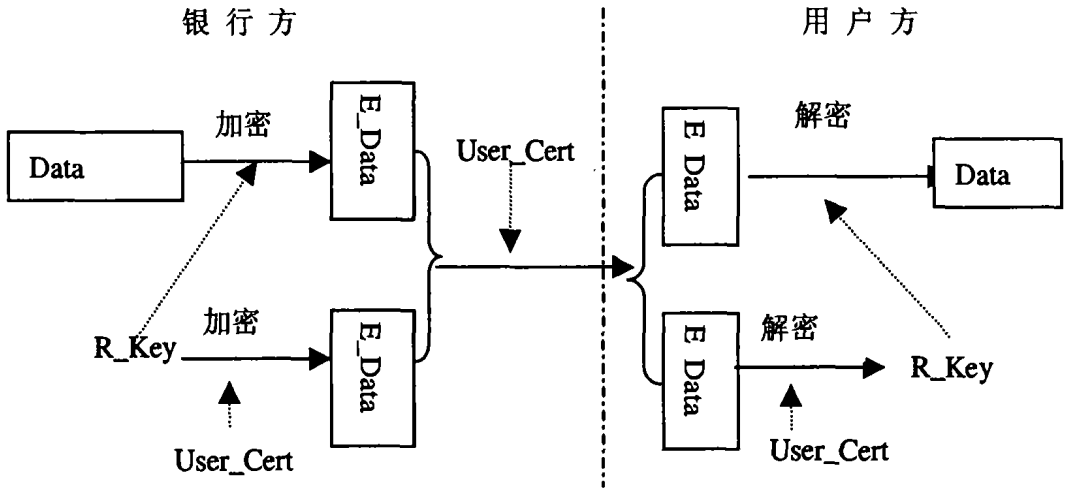

图4

注:在以上的加密过程中,考虑到加密的效率问题,结合了对称加密和非对称加密各自的优点,发展成为电子信封技术。也就是说,发送方随机的产生一个对称密钥,然后用该密钥对传送数据加密,同时将对称密钥用接受方的公钥加密,连同加密后的密文形成一个电子信封一起发送给接受方。接受方对对称密钥的密文采用其私钥解密,然后在用其解密加密后的数据。

(3)证书有效性验证

为保证参与商务活动的各个实体的身份的合法性,要对每个实体的证书进行在线的合法性验证。证书的验证是通过其上级证书或根证书来验证的。即动态地验证该证书是否由最权威机构的证书签名签发。

(4)身份认证和不可抵赖性

该方面是由数字签名技术来保证的。数字签名的算法可描述如下:s=Sign(k,h,t),操作流程是:输入明文 t,经过函数 Sign,用密钥 k 和哈希算法 h 操作,产生数字签名 s。签名算法是哈希算法和非对称加密算法的组合,其过程是:先用哈希算法对明文进行摘要运算,产生摘要值 hv,然后用发送方的私钥对摘要进行加密,结果是签名值。

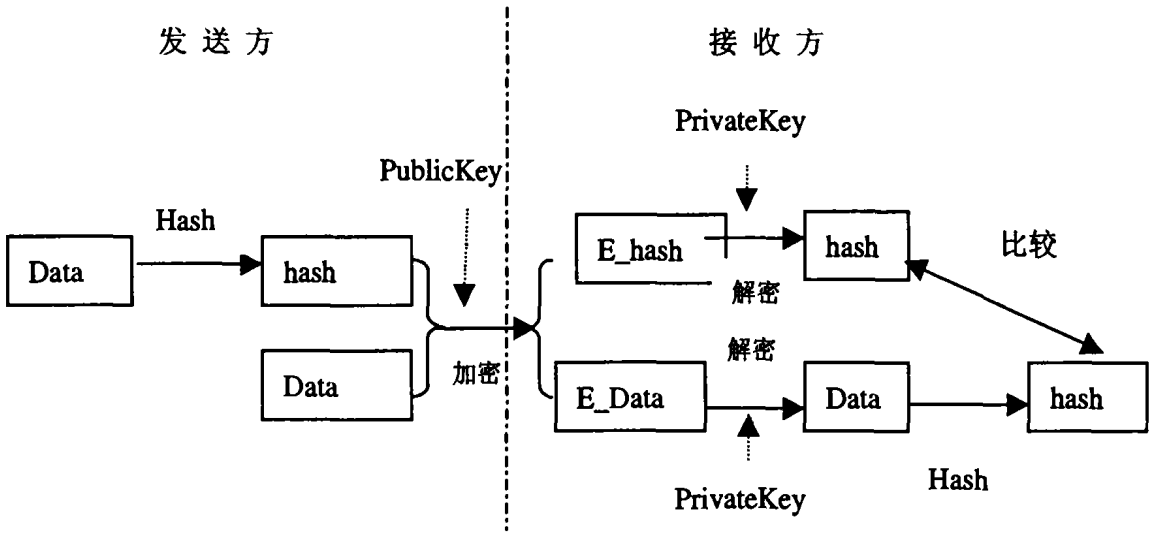

图5

注意:上述的哈希算法 h=Hash(t)是一个单向哈希算法,即从摘要值是不可能回到明文的;而且摘要值对明文的变化极为敏感,明文的极小变化可导致摘要的很大不同;同时,摘要的长度比明文小得

多。以上特点保证了数字签名的效率和可靠性。

数字签名的验证算法是：v＝Verify(k,h,t,s)，操作流程是：输入密文 t，经过 Verify 函数，用密钥 k 对签名值 s 进行解密，用哈希算法 Hash 对明文 t 进行哈希运算，然后对两个结果进行比较，相等即为验证通过，否则为验证失败。

一个完整的数字签名和验证过程可以用图表方式表示如图5。

(5)密钥协商机制

密钥协商机制也是数据传输安全性的一个很好的保证机制，其具体的实现方法是，由通信双方的任何一方定时的随机生成一个对称密钥，然后将该对称密钥用对方的公钥加密，然后发送给对方。当接收方收到后，解密对称密钥，如果成功通知对方，当双方确认后，该对称密钥在下次密钥协商之前将作为双方的加密的密钥使用。

因为，该方法中密钥是随即改变的，而且，该密钥在网上传输时仍然是有非对称加密方式进行加密的，故该方式具有很大的可行性。

在电子银行系统中，SIP 和电子银行服务器之间的数据通信，就采用了密钥协商机制。

4 系统模块设计

(1)ActiveX 控件

ActiveX 控件从页面中接收用户传来的请求信息，对用户的数据用证书进行加密，把加密之后的结果通过浏览器发送接 WEB。

CGI 把返回来的页面送给浏览器，浏览器通过 JavaScript 脚本调用 ActiveX 控件对加密的数据进行解密，通过 JavaScript 脚本把结果显示出来。

(2)WEB/CGI

Web 负责把 ActiveX 控件、银行证书、根证书和相关 Html 文件下载到客户端。

CGI 程序接收电子银行发送来的数据包。并根据浏览器发送来的请求类型读取不同的模板文件，同时把电子银行返回的数据插入到模板文件中。

(3)电子银行系统服务器

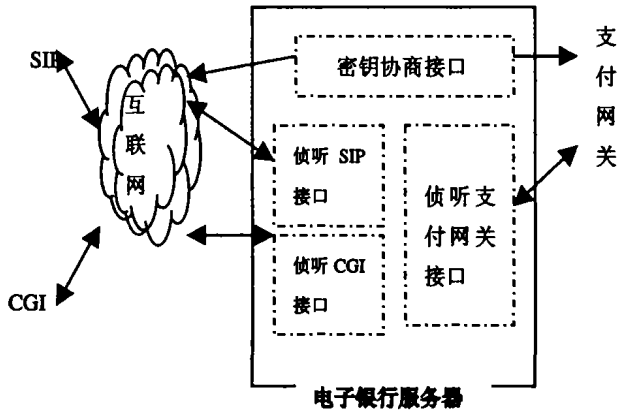

图6

电子银行平台服务器是电子银行系统的核心，它介于支付网关和用户之间，监听和处理用户的请求以及银行的返回信息。

① 接收用户发送的企业登录、余额查询、明细查询和修改密码等请求数据包，对其进行解数字信封和验证数字签名，拆数据包并按照银行系统内部的 ISO8583通信协议要求进行包格式转换，转发请求给银行系统；

② 接收银行系统内部传出来的响应信息，按照电子银行服务器通信协议要求将 ISO8583进行包格式转换后打包，作数字信封和数字签名，发送响应给用户。

(4)支付网关

支付网关的模块图可表示如图7所示。

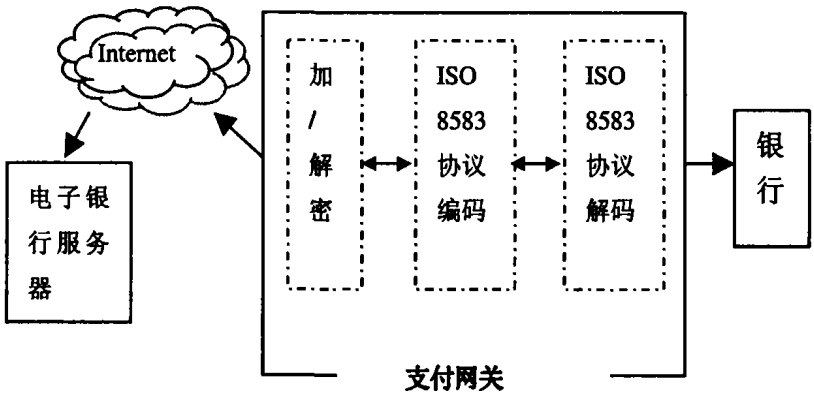

图7

(5)银行前置服务器

银行前置服务器的功能是获得以银行内部数据报格式表示的请求数据报文，以供银行内部业务的工作使用；或者当银行内部业务处理结束后，向平台服务器发送具有该格式的结果数据报文。

该服务器在物理位置上应位于银行内部，以保证银行业务数据的安全性，同时可以减少系统的开销。

(下转第277页)

工作量变为原来的52%(=40%+60%×20%)左右,这将非常有效地加快新基于 Web 的 DSS 系统的开发进度,节省开发成本。

小结与进一步研究 本文介绍了一种基于 Web 的防汛抗旱决策支持系统的构建方法。这个方法利用 COM 组件、XML 通用数据交换、WebGIS 等技术成功地将决策支持系统中的管理业务逻辑与客户端 ASP 代码调用分离,使得整个决策支持系统在使用方便、决策科学、准确性高、实时性强的同时又具有较高的可维护性和可移植性。目前,这一技术已成功应用在安徽省防汛抗旱指挥调度系统的建设中(见图6),并获得了用户的好评。

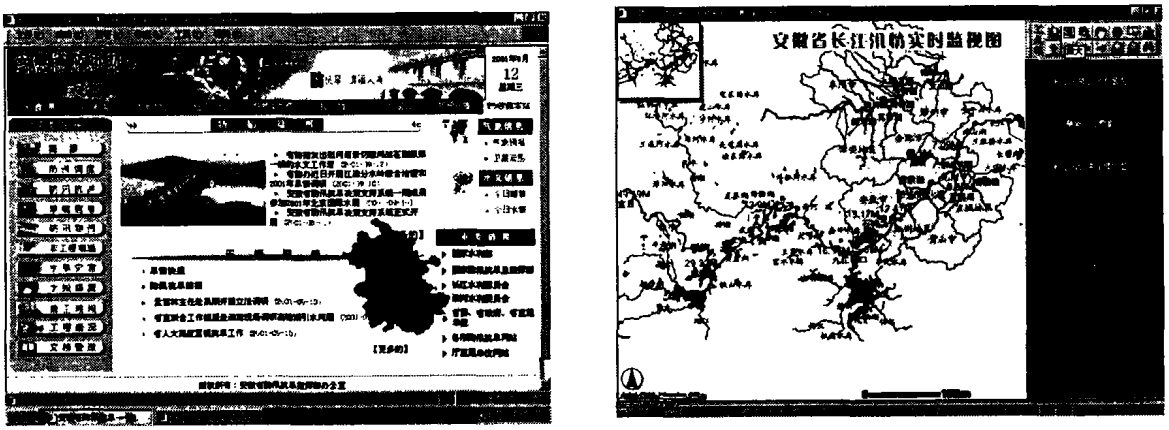

图6 基于 Web 的安徽省防汛抗旱决策系统客户端界面

下一步的研究工作是将现有的决策支持系统技术与人工智能技术结合起来,充分运用现已不断成熟的数据仓库、数据挖掘和专家系统技术,研究出一种基于 Web 的智能防汛抗旱决策支持系统,使系统在现有的先进性基础上,在智能化界面、广义推理、智能化数据库、自学习和自适应能力等方面有新的突破和创新,更好地为防汛抗旱指挥调度服务、为科学决策服务。

参 考 文 献

1 俞瑞钊,陈奇著. 智能决策支持系统实现技术. 浙江大学出版社,2000
2 史忠植,等. 智能决策系统. 中科院计算所,1991
3 史忠植,张海俊,何清. 智能战略决策支持平台——多主体环境 MAGE,2003
4 地理信息系统与管理决策. 北京大学出版社,2000-4-1
5 潘爱民著. COM 原理与应用. 清华大学出版社,1999
6 马智民,俞全宏,姜作勤,编著. 应用地理信息系统设计与实现. 1996,7
7 陈秀万著. 洪水灾害损失评估系统——遥感与 GIS 技术应用. 中国水利水电出版社,1999.2
8 修文群. 网络地理信息系统
9 Hopwood D. A Comparison between Java and ActiveX Security. http://www.users.zetnet.co.uk,Oct. 1997 Microsoft Inc., An Overview of Distributed Applications. http://msdn.microsoft.com,2002
10 Oberg R J. Uderstanding & Programming COM+, Prentics-Hall Inc,2000
11 Harold E R. XML Bible (2nd Edition). IDG Press,2001
12 Sturm J. Developing XML Solutions, Microsoft Press,2000
13 Ceri S, Pelagatti G. Distributed Databases Principles and Systems, McGraw-Hill Inc.,1984
14 Box D, Essential COM. Addison Wesley Longman Inc.,1997
15 张巍,吴强,蔡庆生. 可移植 Browser/Server 方式的管理信息系统. 小型微型计算机系统,2003

(上接第263页)

5 基本工作流程

除查询明细以外,所有的业务流程都相同。

1. AxtiveX 控件把帐号,密码及其他的相关敏感信息加密,通过 Internet 发送给电子银行服务器;

2. 电子银行服务器对从 ActiveX 控件来的消息不做任何处理,透明地发送给电子银行支付网关;

3. 电子银行支付网关接收电子银行服务器发送过来消息,解密之后,变成8583报文,明文传送给银行;

4. 电子银行支付网关处理之后,把消息变成8583报文,传给电子银行网关;

5. 电子银行网关接收8583报文之后,取出消息,对消息加密,发送给电子银行服务器;

6. 电子银行服务器不作任何处理把消息转发给 ActiveX 控件,控件对消息解密,显示出来。

参 考 文 献

1 张福德. 中国电子商务. 蓝天出版社
2 中国电信电子商务规范. 北京创原世纪信息技术有限公司