基于IC卡的电子钱包系统设计与实现

蔡友林[1]， 潘仕彬[2]， 何为民[2]， 蔡丽林[3]

(1.东华理工大学数学与信息科学学院,江西 抚州 344000;2.海南政法职业学院,海南 海口 571100;3.嘉兴航运管理处,浙江 嘉兴 314000)

摘 要:介绍了IC卡技术,提出了利用IC电子钱包作为直接支付手段,然后给出了基于IC卡电子钱包消费系统的总体方案设计及功能模块设计,以及实现系统的一些安全技术。基于IC电子钱包消费系统,不依赖网络通讯,且系统组建灵活,成本低,维护简单。

关键词:电子钱包;IC卡;读写器

中图分类号:TP274 **文献标识码**:A **文章编号**:1674-3504(2008)02-197-04

当前,校园一卡通系统消费子系统大部分是基于网络的系统,通过一张IC卡,师生员工们可以在联网的任何一个消费地点消费。考虑到数据安全可靠,消费卡(IC卡)是无值卡,即卡上并没有存储金额,所有金额都统一存储在计算机里(若IC卡有值,也只是作为参考,以计算机上的存储值为准)。因此,整个交易过程依赖于计算机网络,它的优点是实时性强,功能强大完善,容量大。缺点是成本高、维护复杂、系统庞大不够灵活。对于相对人数较少的学校及校园网络不是很健全的学校,如何利用计算机技术和射频卡(非接触式IC卡)技术,是一个值得探讨的问题。

1 IC知识

在识别卡的发展中,先后出现光电卡、条码卡、磁卡和IC卡。光电卡和条码卡因其防伪性差,目前仅用于某些特定的应用。磁卡防伪能力较差且易磨损磁化,适合用卡次数不频繁的场合,现在已基本不用了。现在普遍使用的是IC卡,IC卡的存储容量小到几十位,大到几十k字节。根据卡片与读写设备通信方式的不同,IC卡可分为接触与不接触两种;根据其集成电路的不同,可以分为存储器卡、逻辑加密卡和CPU卡三大类(王爱英,2000)。本系统采用非接触式MIFARE-1卡,因其具有密码保护,很难复制,适合作小额电子钱包。

MIFARE-1型IC卡内部有1k字节的EEPROM存储器,分为16个扇区(0~15),每个扇区4块(块0~3),共64块,按块号编址为0~63。第0扇区的块0(即绝对地址0块)用于存放厂商代码,已经固化,不可更改。其他各扇区的块0、块1、块2为数据块,用于存贮数据;块3为控制块。其中,每个扇区的块3(即第四块)为密钥和存取控制块,包含了该扇区的访问密码A(6个字节)、存取控制(4字节)和访问密码B(6个字节),是一个特殊的块(图1)。其中,存取控制位规定了该扇区数据块访问所用的密码类型及读写方式。用户可根据扇区的不同设定不同的密码,也就说每个扇区的密码和存取控制都是独立的,可以根据实际需要设定各自的密码及存取控制(一卡多用)。扇区的访问密码分为KEY A和KEY B两组不同密码,根据访问条件,在校验KEY A和KEY B之后才可以对存储器进行访问。

	密码A (KEY-A,6字节)						存取控制C (4字节)				密码B (KEY-B,6字节)					
字节	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

图1 密钥块数据格式

Fig. 1 The data format of key block

2 系统设计

2.1 系统拓扑结构

整个系统由若干个独立脱网工作的窗口机、IC卡和卡务中心的发卡计算机和消费服务器组成(图2)。

发卡计算机。采用串口与发卡读写器相连,并且和消费服务器相联,主要用来对卡片初始化,充

收稿日期:2007-11-28

作者简介:蔡友林(1976—),男,硕士,讲师,主要研究方向:计算机应用及信息处理。

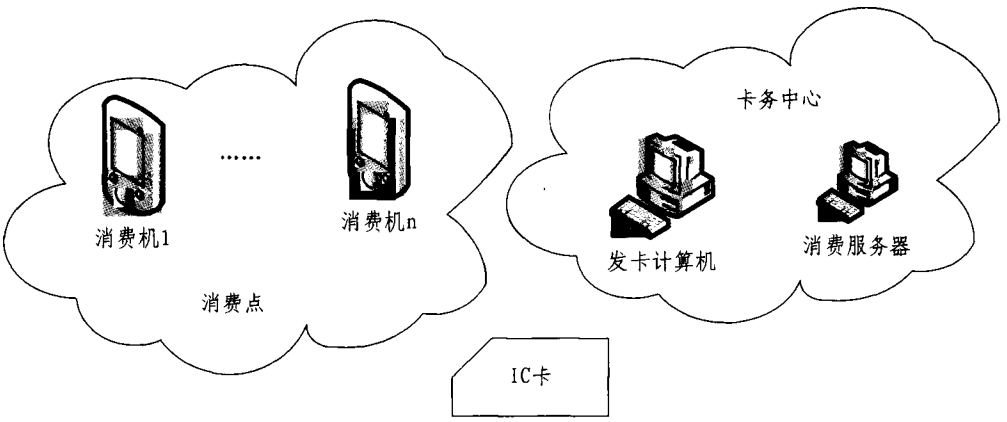

图2 系统拓扑结构图

Fig. 2 The Topological Structure Figure of System

值,并在发卡的时候,用户信息和卡信息关联,实时传递充值信息给消费服务器。

消费服务器。用来接收消费机里的消费记录及发卡机充值的钱,并完成电子钱包的消费结算。

消费机。主要安装于各个消费点,方便用户刷卡消费,目前主要有按键消费机、按次消费机和按时消费机三种机型,每种机型都带有32 kB的存储器,用来脱网存储在本机的消费记录和消费记录总额。

2.2 读写器(ICR/W)

一个标准IC卡应用系统的最基本构件为IC卡、读写器和个人计算机(PC)。其中,IC卡由执卡人掌管,存储着个人电子钱包或其它与执卡人相关的信息;PC机完成对信息的汇总、统计、计算,系统的监控管理甚至卡的发行等操作;读写器是IC卡与PC机的通信桥梁,也是IC卡的能量来源。IC卡里的信息,只有用一定的读写器才能读出来;本系统采用符合14443-B标准的非结触IC卡读写模块,例如RD-500,FM-1200。该IC卡读写器具有以太网/INTERNET接口、以及485接口(用于在不在消费时联网状态备份数据),用来实现与ICR/W的通讯和IC卡读写操作(潘仕彬等,2002)。其逻辑结构图如图3所示。其主要功能就是消费者刷一下卡,读写器(消费机)自动减去电子钱包里的钱,并把所有消费详细记录和在本消费机里的消费总额存储在消费机里。

2.3 系统功能设计

基于IC卡电子钱包消费系统的主要目的是使用电子货币取代校园社区中的现金交易,包括师生就餐、校内娱乐场所、澡堂、水房、小卖部的现金流

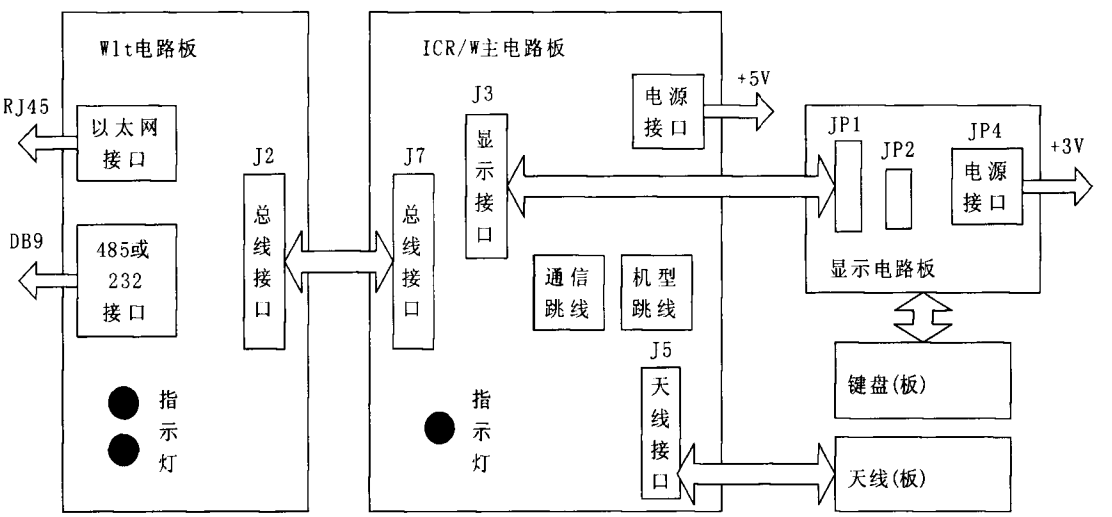

图3 非接触式IC卡读写器逻辑结构图

Fig. 3 The Logical Structure Figure of Untouchable IC Card ICR/W

通。师生员工可以在多个经营业主进行自由便捷的消费活动,同时也可以方便学校的财务管理,方便学校和多个经营者之间的财务结算。而要完成查询、统计等工作必须把消费记录存储到计算机里,通过上位机管理软件来实现。因此,可将整个IC卡消费系统分成消费信息处理和发卡管理两个子系统(Fred Barwell et al.,2002)。

(1)消费信息处理子系统。消费信息处理子系统是负责接收按键消费机、按时消费机和按次消费机的消费数据及总营业额,由于这些消费机平时都是脱网运行的,当存储数据快满或消费了一天时,要把这些消费数据下载到计算机,以便和用户信息相联系,形成消费记录,并可查询消费者的消费信息和统计出各消费点、各窗口机、经营业主的营业额(图4)。

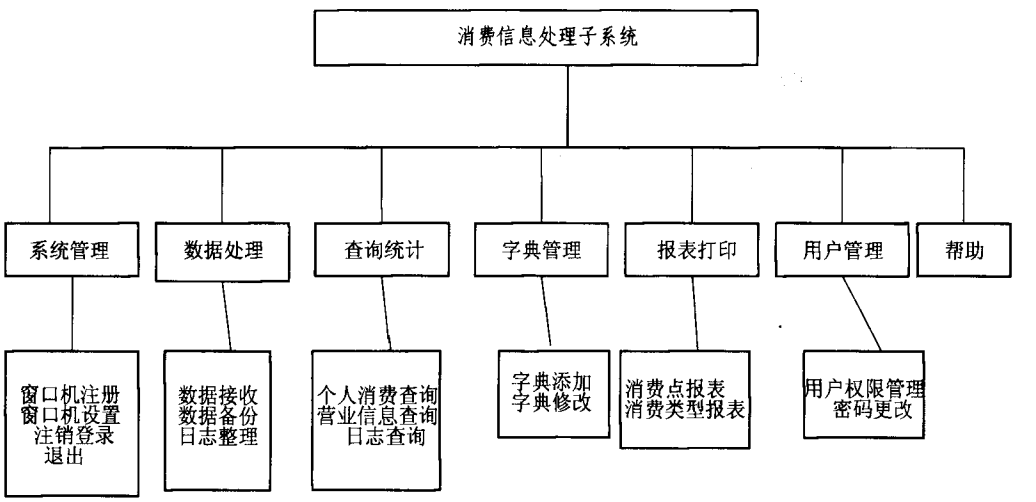

图4　消费处理子系统模块图

Fig.4　the Module of processing subsystem

(2)发卡管理子系统。完成发卡、充值、退卡等工作。

发卡包括卡的初始化,消费卡可多次使用,一个用户允许有多张消费卡,卡不允许挂失,但可退卡。卡只许现金充值,卡上的充值金额不许超过一定数额。发卡要记录消费者的姓名,用户号等信息,经充值后将卡片发给消费者,记录发卡数据并打印收据完成发卡工作。

充值。根据消费者要求对卡进行充值,然后记录充值数据并打印收据完成充值工作。

退卡。消费者不要用卡了(如学生毕业等)可以退卡,此张卡可供另外一个消费者使用。

3　系统安全

3.1　IC卡安全性

(1)IC卡的安全性是系统安全性的基础。IC卡厂家一般会采取相应措施来阻止对IC卡的攻击。MIFARE-1型IC安全性高,卡片序号是唯一的,出厂后不可更改;IC卡与读写器之间采用双向互认验证机制,在通信过程中所有数据加密。到目前为止,还没有有关破译了其通信数据的报道。

(2)在设计IC卡的电子钱包中,可用电子钱包一个区中的两个块来存储电子钱包的金额,两个块存储相同的值。块2是对块1备份的同时,对每个块里面的数据又采取了正反取值,确保电子钱包金额的正确。

(3)本系统对IC卡中所存的钱有限制,只用一个块的两个字节来存储,也就是讲,只能存600元多一点,只能用于小额消费。

3.2　数据库安全性

本系统采用SQL Server 2000数据库,采用的是SQL Server和Windows结合使用(SQL Server and Windows)的安全模式,来保证数据库的数据安全。

3.3　程序安全

(1)用户认证。所有用户要进入系统,只有通过验证的合法系统用户才能进入系统,系统同时记录用户的身份信息和该用户的登录时间,否则拒绝登录请求。

(2)访问授权。用户进入系统后,系统根据用户的角色显示该用户在权限范围内的操作功能界

面,不显示用户无权操作的功能,增加系统的安全性。

(3)审计追踪机制。专门设计了一个操作日志表,用于记录用户的各种插入、删除、更新等操作,记录用户对表中数据执行操作类型和操作时间等信息。一旦数据出现问题,可以查看操作记录,找出原因,从而监督、约束系统内的每一用户。只有相应权限的管理员才能查看操作日志表。

4 结束语

利用IC卡本身的存储功能是安全可靠的,在小额消费领域,把钱直接存储在IC卡上,每次消费可直接在IC卡上支付金额。而基于IC电子钱包消费系统,就是以IC卡为支付主体的数据传递系统。所有消费的金额直接在卡上支付,不依赖网络通讯,且系统组建灵活,成本低,维护简单。

参考文献

王爱英. 2000. 智能卡技术_IC卡(第2版)[M]. 北京:清华大学出版社:1-100.

张冬梅,潘仕彬,何为民. 2003. 模拟I2C总线多主通信的实现. 单片机与嵌入式系统,12(1):23-24.

王进宏,等. 2004. 基于RF-IC卡智能门禁安全管理系统的开发[J]. 东华理工学院学报,27(3):289-292.

Fred Barwell Richard Blair 等. 2002. 张加荣 译. VB. NET高级编程[M]. 北京:清华大学出版社:1-812.

The Design and Implementation of Electronic purse Management System Based on IC

CAI You-lin[1], PAN Shi-bin[2], HE Wei-min[2], CAI Li-lin[3]

(1. Faculty of Mathematics and Information Science, East China Institute of Technology, Fuzhou, JX 344000, China;2. Hainan Vocational College of Political Science and Law, Haikou, HN 571100, China; 3. Shipping Management of Jiaxing, Jiaxing, ZJ 314000, China)

Abstract: This article introduces the IC card technology, proposes using the IC electron wallet as the direct payment means, then introduces the overall plan design and the function module design, and has related the realization system some security technologies. Consumption that the system based on the IC electron wallet, does not rely on the network communication. it also sets up nimbly. Its cost is low and its maintains is simply.

Key Words: electronic purse; IC Card; reader device