doi:10.3772/j.issn.1002-0470.2019.06.003

基于 RFID 技术的身份证识别门禁系统开发①

王 兴②[*,**] 侯礼宁[**] 白 雪[***]

([*]中国科学院大学 北京 100049)

([**]太原科技大学计算机科学与技术学院 太原 030024)

([***]山西瑞诺风电子科技有限公司 太原 030043)

摘 要 智能门禁系统是当前的热门技术,是安防领域未来的发展趋势。本文针对目前智能门禁系统领域广泛使用 IC 卡刷卡进门存在的问题,提出以 RFID 技术为核心,利用二代身份证的高安全性、高防伪级别和唯一性,设计并研发了一款将二代身份证作为门禁卡进行识别的智能电子锁,进而创造了一种新型的智能门禁系统,门禁系统各部分通过 HTTPS 协议进行通信。本文详细阐述了以 RFID 技术为核心的身份证识别的过程,身份证识别的防碰撞算法的实现,并介绍了智能锁 HTTPS 通信协议的设计方法。测试结果表明本门禁系统运行流畅,开锁效率极高,满足了人们对安全快捷的开锁方式的追求,为现代社会的安全防范发展提供了借鉴。

关键词 电子锁, 智能门禁系统, RFID 技术, 二代身份证, HTTPS 通信协议

0 引 言

随着物联网与高新技术的蓬勃发展,智能化社会的建设被提上日程。智能门禁系统是智能化社会建设和物联网建设的典型代表,已经在诸多领域得到应用,并取得了可观的社会、经济效益。门禁系统是人民生命财产安全的一道重要关卡,是人们稳定生活的保障。目前酒店的门禁系统广泛采用刷 IC 卡进行开锁。这种门禁系统造成了不必要的人力资源的浪费。并且此类 IC 卡防伪性能低下,易被复制,容易消磁、芯片容易脱落等导致无法开锁,且这种门禁系统不可以进行远程控制。为此,笔者设计了一种基于 RFID 技术的身份证识别门禁系统,利用第二代身份证刷卡开锁,结合云服务器,实现了对电子锁的远程控制和状态监控。作为射频卡的一种,二代身份证继承了射频卡的优点,采用了数字防伪技术和印刷防伪技术,安全性得到了较大程度的提高。鉴于其安全性、普及型及唯一性,二代身份证可以应用在安防系统中作为个人身份识别的唯一标识[1]。这种基于 RFID 技术的身份证识别门禁系统不仅提高了酒店住宿的安全程度,同时规范化了酒店对每个门禁和员工的管理体制,在一定程度上促进了社会经济的发展。

1 系统总体设计

1.1 系统总体架构

基于 RFID 技术的身份证识别门禁系统主要由电子锁、手机订房客户端、电子锁管理系统和 tomcat Web 服务器组成。系统总体架构如图 1 所示。

1.2 系统工作原理

客户利用身份证通过手机上的订房客户端预订房间,订房客户端向 Web 服务器发送请求命令,电子锁管理系统生成该用户的开锁身份证信息指令,

① 国家国际科技合作专项(2014DFR70280)资助项目。

② 男,1981 年生,博士生,副教授;研究方向:物联网与传感网技术;联系人,E-mail: www.17904856@qq.com

(收稿日期:2018-09-21)

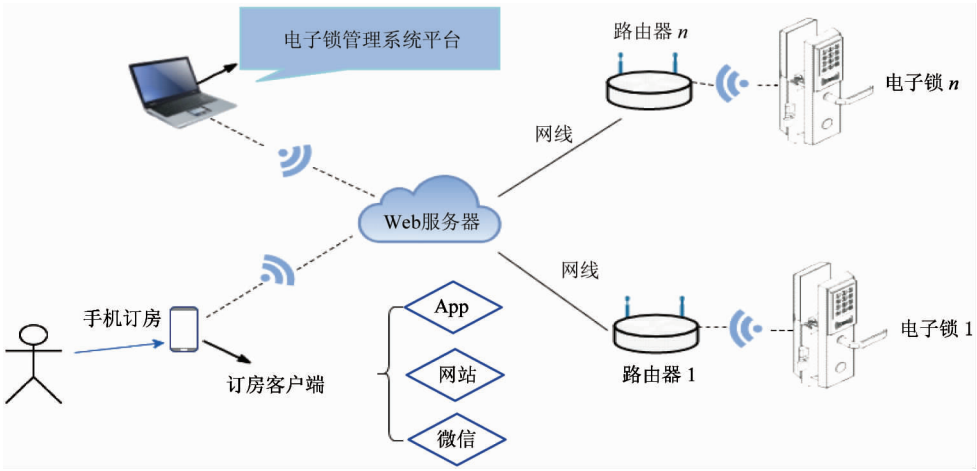


图 1　系统总体架构图

暂时保存于电子锁管理系统的数据库中,并通过 Web 服务器向客户订房客户端返回响应的信息(如订房成功,开锁身份证信息等)。电子锁每 10 min 请求一次 Web 服务器,Web 服务器通过调取电子锁管理系统数据库中存储的开锁身份证信息数据发送给电子锁,存储到电子锁的控制主板中。当用户使用身份证在电子锁的身份证刷卡区域刷卡时,经过 RFID 系统的作用,对存储在控制主板里的开锁身份证信息和读取到的身份证信息进行比较,若一致,电子锁开锁电路控制门锁打开,用户入住。系统工作原理流程图分为两部分:第一部分是用户订房流程图,如图 2 所示;另一部分是用户开锁流程图,如图 3所示。

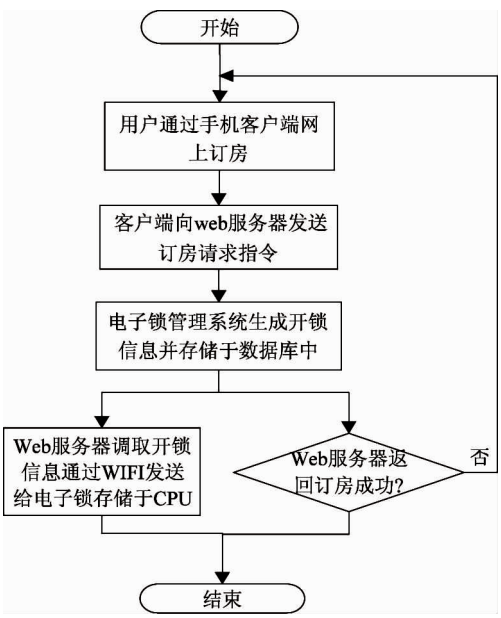


图 2　用户订房流程图

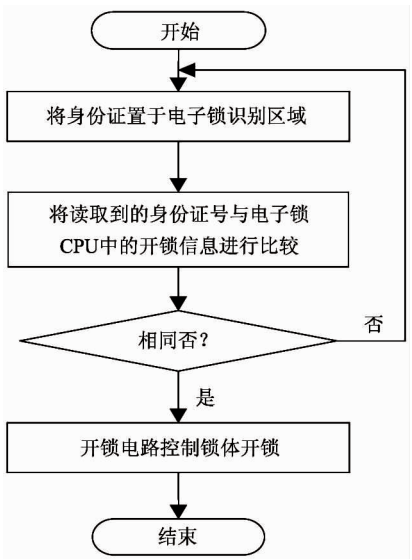


图 3　用户开锁流程图

1.3　身份证开锁安全性能分析

目前,酒店行业亦广泛采用基于 APP 手机认证的房间开锁方式。在这种方式下,手机 APP 要求获取机主手机号码,这样会造成机主行踪和消费信息的泄露等;而且手机电池属于有源设备,一旦电量耗尽,将无法进行开锁。而对于识别身份证进行开锁的方式,用户需要提供自身的身份证号码,在刷身份证时也需要对身份证号码进行识别。但是,本系统用来识别身份证的读卡器是交由公安部门进行管控的,系统各部分之间的通信都经过了 SSL 数字证书加密处理,不会泄露用户的身份证信息,而且实现了实名制开锁,有利于强化社会管理,也是人们财产安全的一种保障。

2　门禁系统硬件设计

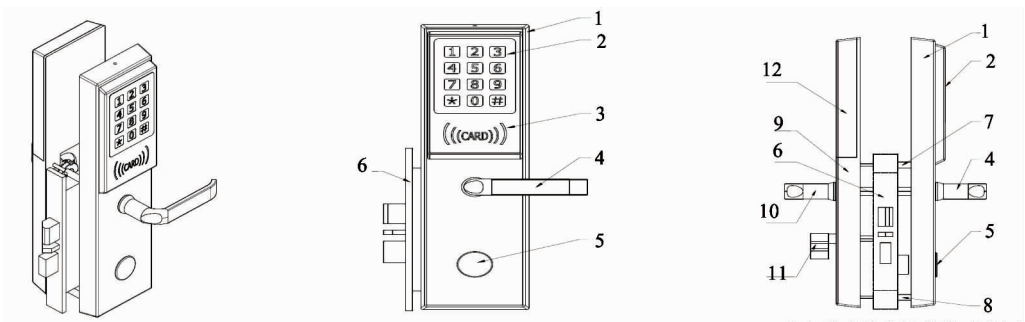
电子锁是该门禁系统的核心结构,主要由门锁模块,WIFI 模块,RFID 读卡器模块,CPU 模块,电源模块等组成。电子锁主要组成如图 4 所示。

2.1　RFID 读卡器模块

RFID 技术是 21 世纪十大重要技术之一[2]。它是一种无线、非接触式的自动识别技术,具有使用简便、识别率高、寿命悠长等优点,也是本智能门禁系统的核心技术。本门禁系统的 RFID 系统由身份证、身份证信息处理器和电子锁管理系统系统组成。

2.2　RFID 系统频段选择

对一个 RFID 系统来说,它的频段的概念指的是:读卡器通过天线发送和接收并识读的射频卡信号的频率范围[3]。ISM 频段,是由美国联邦通信委员会(FCC)定义出来的一种特别开放给工业、科学和医用 3 个主要机构使用的频段,使用者没有许可证限制,无需专门寻求获取使用授权[4]。因此 RFID 系统选择此频段不会对其他无线电服务造成影响和干扰。本系统采用身份证作为电子标签,即采用 13.56 MHz的 ISM 频段。该频段在其他领域如办理机动车驾驶证、个人信贷业务等方面,已经得到普遍的应用,技术成熟度高。



(a) 本文发明的结构示意图　(b) 本文发明涉及的前面板外部结构示意图　(c) 本文发明的左视结构示意图

1. 前面板; 2. 密码按键; 3. 身份证刷卡区域; 4. 前面板把手; 5. 钥匙孔盖; 6. 锁体; 7. 上连接螺柱
8. 下连接螺柱; 9. 后面板; 10. 后面板把手; 11. 反锁旋钮; 12. 电池盒后盖

图 4　电子锁主要结构示意图

2.3　TTF 身份证读取

RFID 系统主要有两种工作方式,一种是阅读器先发言(reader talks first,RTF),另一种是标签先发言(tag talks first,TTF)[5]。本系统识别身份证是属于 TTF 方式。二者之间的识别工作原理图如图 5 所示。当二代身份证靠近电子锁的感应区附近时,身份证与身份证信息处理器进行电磁耦合,身份证信息处理器产生电磁波,身份证被激活,身份证将自身编码等信息通过卡内置发送天线发送出去。身份证信息处理器接收天线接收到的从身份证发来的调制信号,该调制信号通过数据线进入身份证信息处理器的射频模块并进行 A\D 转换,完成模拟信号向数字信号的转换,再经过逻辑处理单元进行处理,通过身份证信息处理器接口电路将所读取的身份证号信息传送至 CPU 模块进行数据处理,若所读取的身份证号与内存中预置开锁身份证号相同,则再通过开锁关锁电路发送开锁信号,控制锁体开锁,反之不执行开锁动作。

2.4　身份证识别防碰撞算法

RFID 系统在进行工作时,当有多个身份证进入了身份证信息处理器的作用范围之后,这些身份证在同时发送自身信息编码时就会出现通信方面的冲突,发送的数据进行相互干扰(即产生了碰撞),致使门禁系统失灵,无法正常工作。

二进制树型搜索算法可以解决这一问题,该算法目的在于从多个电子标签中选出任一个电子标签。二进制树型搜索算法的基本思路是,多个电子标签进入读写器工作范围后,读写器发送带有某一限制条件的询问命令,所有满足限制条件的电子标签进行响应,如果有多个电子标签做出响应,则发生

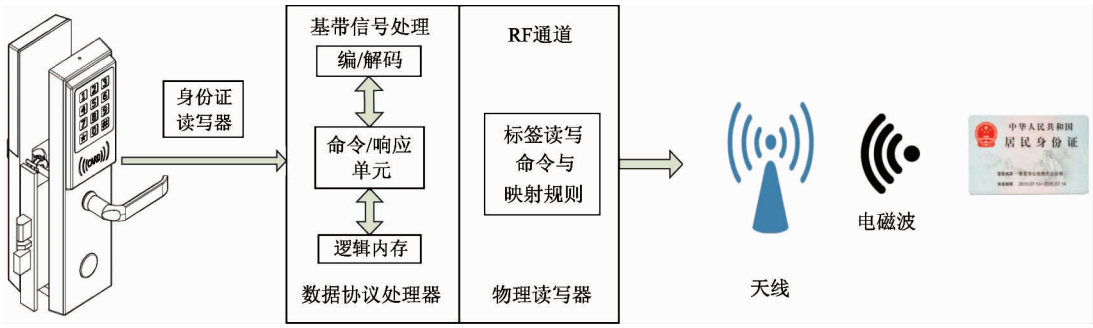


图 5　电子锁识别身份证原理图

了碰撞,则根据产生错误的比特信息再对限制条件进行修改,再一次发送询问命令,直到只有一个电子标签进行响应,并完成对该标签的读写操作[6-8]。对剩下的电子标签反复进行以上操作,直到完成对所有电子标签的读写操作。但是若想使用该算法,必须要能够识别出读写器中数据发生碰撞的比特的确切位置,Manchester 编码正好可以做到这一点。为了实现二进制树型搜索算法,就选用了 Manchester 编码。

从多个电子标签中选择一个单独的电子标签,需要重复的执行该算法,其平均次数 L 取决于读写器作用范围内电子标签的总数 N:

$$L(N) = \log_2 N + 1$$

不难看出,利用二进制树形搜索算法可以在短时间内解决身份证识别的碰撞问题。

2.5　RFID 系统调制方法

调制是将射频卡要发送的信息寄托在载波信号的某一参量上(如连续波的频率、相位或振幅)进行发送,调制后的信号具有两个特征,携带信息和适合在信道中传输[9]。身份证到身份证信息处理器的信号传输采用的调制方法采用二进制移相键控(BPSK)。BPSK 方式是根据数字基带信号的两个电平(或符号),使载波相位在两个不同的数值之间切换的一种相位调制方法。

在 BPSK 方式中,通常使用初始相位 0 和 π 分别表示二进制数的“0”和“1”。设信息源(即身份证)发出的序列是由二进制符号 0 和 1 组成,且假设 0 符号出现概率为 P, 1 符号出现的概率为 $1-P$,二者彼此独立。则 BPSK 信号 $e_0(t)$ 可以表示为一个双极性全占空矩形脉冲序列与一个正弦载波的乘积,即

$$e_0(t) = \left[\sum_n a_n g(t - nT_x)\cos\omega_c t\right]$$

其中,$g(t)$ 是脉宽为 T_x 的单个矩形脉冲,a_n 的统计特性为

$$a_n = \begin{cases} +1 & \text{概率为 } P \\ -1 & \text{概率为 } 1-P \end{cases}$$

即,在某一个码元的持续时间 T_x 内观察时,$e_0(t)$ 为

$$e_n(t) = \begin{cases} \cos\omega_c t & \text{概率为 } P \\ -\cos\omega_c t & \text{概率为 } 1-P \end{cases}$$

发送二进制符号 0 时(a_n 取 +1),$e_0(t)$ 取 0 相位;发送二进制符号 1 时(a_n 取 −1),$e_0(t)$ 取 π 相位。

3　系统通信协议的设计

HTTP 协议具有通信开销小、简单快速、传输成本低、使用灵活、节省传输时间等优点,但是其信息传输过程中的明文传输方式使得传输安全性得不到保障。安全套接层(secure sockets layer,SSL),是为网络通信提供安全及数据完整性的一种安全协议。本系统选择并购买了全球第二大数字证书颁发机构 Geo Trust 旗下的更适合企业使用的专业 OV SSL 数字证书,将其部署安装在门禁系统的 tomcat Web 服务器上,实现网站的 HTTPS 可信访问。网站的 HTTPS 化,使网站变得可信,并可防劫持、防篡改、防监听,大大提高了身份证信息和开锁指令在传输过程中的安全性。

电子锁和 Web 服务器,以及 Web 服务器和电子锁管理系统之间的通信都是按照 HTTPS 协议进

行通信的。

在本系统中,电子锁以 10 min 为周期定时向 Web 服务器发送经过加密的请求命令,云服务器接收到请求命令,便会做相应的应答操作,返回相应请求的文档,完成通信。电子锁主要请求命令为电子锁的功能指令。例如请求开锁身份证号、开锁密码、开门指令等操作。门禁系统通信原理图如图 6 所示。

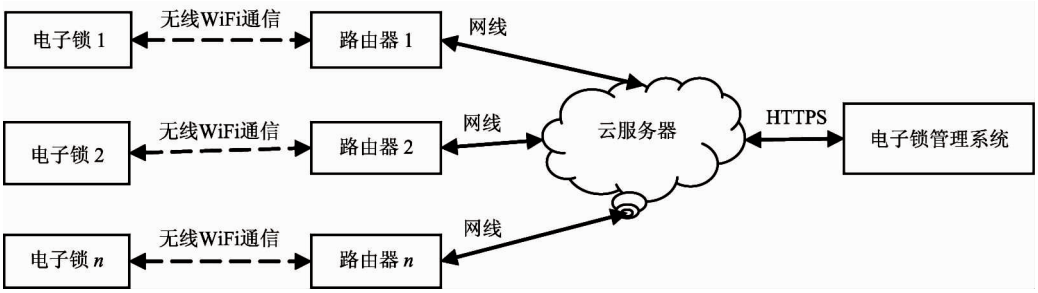


图 6　门禁系统的通信原理图

Web 服务器和电子锁管理系统之间的通信也是按照 HTTPS 协议,遵循请求(Request)/应答(Response)模型进行通信。通信步骤与电子锁和云服务器之间通信原理一样。电子锁管理系统向 Web 服务器实时发送请求命令,Web 服务器接收到请求命令便会做相应的应答操作,返回相应请求的文档,完成通信。

电子锁管理系统主要由电子锁管理员进行操作,管理员通过电子锁管理系统软件,将新的开锁身份证信息、开锁密码信息、远程开锁等指令进行生成,暂时保存于电子锁管理系统的数据库中,电子锁定时发送请求命令给 Web 服务器,通过 Web 服务器调取电子锁管理系统的数据库中存储的操作命令,完成电子锁管理系统对电子锁的操作。

服务器端 HTTPS 访问请求设计如下:

(1) 请求方法:Https Get 方法

(2) 请求的 URL:https://ip:port/网页的相对路径。

ip:Web 服务器的地址

port:端口号

网页的相对路径:相对于整个项目工程而言。

示 例: https://47. 94. 83. 90: 8080/electronicLock/lock. htm

(3) 请求的参数:

LockId = R0014&type = 1&content = ORDER

锁 ID:lockId

请求类型:type

请求内容:content

具体的请求说明设计如表 1 所示。

表 1　服务器端访问请求说明

请求类型	Type	备注
获取命令	Type: A id:锁号(R0001) content :ORDER	获取当前锁所有待执行命令,返回结果多条
命令回写	Type: B id:锁号(R0001) content:执行成功的命令 id(10000001)	执行成功的命令 id 为获取命令中的命令 id
开门日志	Type: C id:锁号(R0001) content:开门情况 0 + 密码或 1 + 身份证(0123456 或 1730184198501184124)	
低电压报警	Type: D id:锁号(R0001) content:POWERDOWN	

请求示例如下:

(1)获取命令

https://ip:port/electronicLock/lock. htm? lockId = R0014&type = 1&content = ORDER

返回值:#命令条数 + 命令|命令|命令 $

例如:返回多条命令时,多条命令按指令序号顺序执行,执行成功的命令 id 为获取成功的命令 id。命令示例及说明如下:

#00600000001R00141142631199505027 42X00000000000000|00000002R00142000000000000000000012345600000000|00000003R0014314263119950502742X55279301350000|00000004R0014A000|00000005R0014B000|00000006R0014C000 $

设置管理员开锁身份证号(18 位)

#00100000001R00141142631199505027 42X00000000000000 设置管理员开锁密码(6 位)

#00100000002R00142000000000000000000012345600000000 设置住房人员开锁身份证号(18 位)及开锁密码(6 位)及有效时间(分钟):

#00100000003R00143142631199505027 42X55279301350000 $

远程开锁:#00100000004R0014A000 远程封锁(禁止非管理员开锁):#00100000005R0014B000 远程解锁(解除非管理员开锁限制):#00100000006R0014C000(2)命令回写(无返回值)

https://ip:port/electronicLock/lock.htm?lockId=R0014&type=2&content=00000001

(3)开门日志(无返回值)

https://ip:port/electronicLock/lock.htm?lockId=R0014&type=3&content=142631199505027 42X(身份证)

https://ip:port/electronicLock/lock.htm?lockId=R0014&type=3&content=123456(密码)

(4)低电压报警(无返回值)

https://ip:port/electronicLock/lock.htm?lockId=R0014&type=4&content=LOW-VOLTAGE

相关的 HTTPS 返回错误码设计如表 2 所示。

表 2 HTTP 返回错误码

错误代码	错误信息
L200	成功
L201	请求类型不存在
L202	请求类型有误
L203	接口输入参数存在空值
L204	获取命令接口参数有误
L205	命令回写接口参数有误
L206	开门日志接口参数有误
L207	低电压报警接口参数有误
L208	接口锁号参数有误
L209	系统错误

4 结 论

本文主要利用 RFID 系统的特征和工作原理,开发了一款识别身份证的智能电子锁,同时设计并实现了一种基于 RFID 技术的身份证识别门禁系统。该系统可以采用身份证作为识别的门禁卡,实现了实名制开锁。系统手机客户端、Web 服务器、电子锁,电子锁管理系统之间通过 HTTPS 协议进行通信,实现了门禁系统的远程控制和智能化。该系统已在现实生活中投入使用,成功的案例有北京“拾号公寓”,太原“逸客短租”等公寓采用的门禁系统。事实表明,系统软硬件运行稳定流畅,很好地满足了用户的需求。接下来,根据用户的反映、后台管理软件的监测等情况,将对本系统及时进行更新换代,进一步降低身份证的误识率,使这种门禁系统更安全、更可靠、更快捷、更智能。

参考文献

[1] 胡晶宇,付志远,陈绪兵. 基于 RFID 的图书馆自习室座位管理系统的研究[J]. 现代电子技术,2014,37(20):38-40

[2] 李如年. 基于 RFID 技术的物联网研究[J]. 中国电子科学研究院学报, 2009,4(6):594-597

[3] 沈文龙. 实现以 RFID 卡仿真磁卡的模块设计[J]. 福建农林大学学报:自然科学版, 2007,36(4):435-439

[4] 方箭,王坦,黄标. 高频段宽带无线通信前瞻[A]. 电信科学,2014:109-113

[5] 杨娅雯,赵珂,肖志涛,等. 基于 AES 算法的移动门禁认证技术研究与应用[J]. 南昌航空大学学报:自然科学版, 2017,31(3):100-112

[6] 元媛,姜岩峰. 射频识别(RFID)技术综述[J]. 半导体技术,2006(11):801-804

[7] Gaukler G. Establishing dynamic expiration dates for perishables: an application of RFID and sensor technology [J]. *International Journal of Production Economics*, 2017

(11): 617-632

[8] Qin W, Zhong R Y, Dai H Y, et al. An assessment model for RFID impacts on prevention and visibility of inventory inaccuracy presence[J]. *Advanced Engineering Informatics*, 2017(8):70-79

[9] 黄玉兰. 物联网射频识别(RFID)核心技术详解[M]. 北京:人民邮电出版社,1979. 206-211

Development of ID card identification access control system based on RFID technology

Wang Xing[*,**], Hou Lining[**], Baixue[***]

([*] University of Chinese Academy of Sciences, Beijing 100049)

([**] Taiyuan University of Science and Technology, Taiyuan 030024)

([***] Shanxi Renovo Electronic Technology Co. Ltd., Taiyuan 030043)

Abstract

The intelligent access control system is currently the hot technology and is the development trend of the security field in the future. In view of the problem of the widespread use of IC card in the field of smart access control systems, this paper proposes to use RFID technology as the core, using the high security, high anti-counterfeiting level and uniqueness of the second-generation ID card, designs an intelligent electronic lock which uses a second-generation ID card as an access card to discern, and creates a new type of intelligent access control system. Every part of the system communicates via HTTPS communication protocol. This paper also explains in detail the process of ID card identification based on RFID technology, and ID card recognition anti-collision algorithm, introduces the design method of smart lock HTTPS communication protocol. The test results show that the access control system runs smoothly and is extremely efficient, realizing people's pursuit of safe and fast unlocking methods and providing a reference for the security development of modern society.

Key words: electronic locks, intelligent access control system, RFID technology, second-generation ID card, HTTPS communication protocol