DOI:10.16652/j.issn.1004-373x.2021.23.014
引用格式:高静.基于物联网技术的数字化校园网信息安全加密系统[J].现代电子技术,2021,44(23):67-71.

基于物联网技术的数字化校园网信息安全加密系统

高　静
(南京理工大学 信息化建设与管理处, 江苏 南京　210094)

摘　要: 校园网信息系统安全程度较低,加密所需时间过长,为此,基于物联网技术提出一种新的数字化校园网信息安全加密系统。在硬件设计方面,分别设计MF RC500射频芯片、TIMSP430微处理器、硬件接口;在软件设计方面,结合加密程序和显示程序,实现数字化校园网信息安全加密系统设计。对比实验结果表明,基于物联网技术的数字化校园网信息安全加密系统的加密安全程度得到有效提高,所需时间大大缩短。

关键词: 信息安全; 加密系统; 数字化校园网; 物联网技术; 数据分析; 程序设计
中图分类号: TN915.08-34; TP399　　**文献标识码:** A　　**文章编号:** 1004-373X(2021)23-0067-05

Digital campus network information security encryption system based on the Internet of Things technology

GAO Jing
(Division of Informationization Construction and Management, Nanjing University of Science & Technology, Nanjing 210094, China)

Abstract: The security degree of the existing campus network information system is low and its encryption duration is excessively long. In view of this, a new digital campus network information security encryption system is proposed on the basis of the Internet of Things (IoT) technology. In terms of the hardware, RF chip MF RC500, microprocessor TIMSP430 and hardware interface are designed. In terms of the software, the encryption program and display program are designed. The digital campus network information security encryption system is achieved in combination with the hardware devices, encryption program and display program. A contrast experiment was set up. The experimental results show that the encryption security degree of the designed system based on the IoT technology has been effectively improved, and its encryption time required has been greatly shortened.

Keywords: information security; encryption system; digital campus network; IoT technology; data analysis; program design

0　引　言

数字化校园网以计算机网络技术为基础,采用先进的数据处理手段和工具对学生信息、设备、活动等相关数据进行全面数字化,对于提升教育效率和管理水平具有重要意义。数字化校园网包含大量学生以及教师的个人信息,是信息窃取主要的攻击对象,因此,保证数字化校园网信息的安全成为一大难题。物联网技术是目前应用广泛的一种信息技术,在适当网络环境下,采用物联网技术能够提升系统的安全性与稳定性。

收稿日期:2021-05-31　　**修回日期:**2021-06-17
基金项目:赛尔网络下一代互联网技术创新项目:基于IPv6的SDN研究(NGII20150117)

文献[1]探讨数字化院前急救平台的设计,梳理优化急救医疗业务流程,实现时间自动采集等系统间协同,在多学科及院内外急救体系方面信息共享和流程优化。文献[2]为了实现对饮水机系统的智能管理,采用超文本传输协议,在综合分析物联网关键技术的基础上,对后台数据中心服务器进行数据交互,保障了信息传送的安全性,实现了大数据的统一管理和维护。

以上方法都应用物联网技术进行多方面研究,为减少信息泄露,保证个人信息安全,本文整合上述研究经验,利用物联网技术的优势,使用信息传感设备,根据相关协议,设计了一种基于物联网技术的数字化校园网信息安全加密系统,对其硬件组成结构和重要的软件程序进行了详细设计和介绍,实现了对信息的智能化识别、

加密、显示和监管功能，提升了信息的安全性，保证信息的安全传输。

1 基于物联网技术的数字化校园网信息安全加密系统硬件设计

为了保证本文研究的数字化校园网信息安全加密系统能够正常运营，提升系统对数据的处理能力，为程序的运行构建物理基础，本文通过与物联网技术相融合的理念设计了该系统所需要的硬件设备，该硬件设备主要包括MF RC500F射频芯片、TIMSP430微处理器、硬件接口三大部分，通过各设备之间的协调工作，能够有效提升系统的工作效率和稳定性[3]。

1.1 MF RC500F射频芯片硬件设计

本文应用的MF RC500F射频芯片是根据1MF RC500射频芯片原理进行自主设计的一种新型射频类芯片，可以在满足本文设计系统应用要求的条件下剔除一定的电路结构从而达到简易便捷的目的，它的应用对本文研究的数字化校园网信息安全加密系统有着非常重要的作用，其具体结构电路图如图1所示。

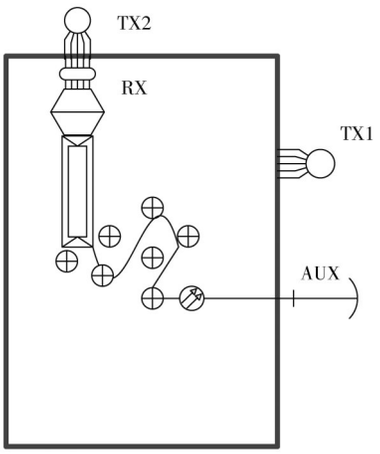

图1 MF RC500F射频芯片的电路图

当系统应用于数字校园网信息加密时，芯片可以根据用户发送的信息设置，对TIMSP430需要发送的数据进行调制，得到特定的无线信号，接收到无线信号后，通过天线TX1将特定的无线信号发送到与AUX引脚无线连接的射频卡的一端A，射频卡的A端将这些无线信号转换成相关的数据集M，芯片的AUX引脚也会产生同一组相关的数据集M，芯片会对这组数据集M进行校验，在确认机器没有错误处理后，再从RX引脚和天线TX2以无线信号的形式发送给TIMSP430微处理器[4-5]。

1.2 TIMSP430微处理器核心硬件设计

为了满足本文系统的快速集成以及加密安全要求，本文选用了MSP430微处理器系列中的TIMSP430微处理器作为该系统的主要微端处理器，它的主要作用是存储数据、处理数据以及控制流程，同时也是本文设计的数字化校园网信息安全加密系统中无线传输控制的核心部分之一。其中，JTAC调试模块具有程序下载与仿真调试的功能；ZigBeeCC2420无线传输模块则具有以射频脉冲形式接收与传输无线信号的功能；串口模块则是计算机与读写器之间的连接；电源管理模块的主要功能是为各部分及时提供所需能源；复位电路则起到了弥补各部分能源误差，增强整体寿命的作用；TIMSP430微处理器作为该硬件的主要核心进行整体的运转[6]。当TIMSP430微处理器核心硬件通过ZigBeeCC2420无线传输模块接收到射频芯片传输的无线信号后，ZigBeeCC2420无线传输模块会将无线信号根据射频脉冲原理进行转化，进而得到相应的存储数据N与命令数据D，再将存储数据N与命令数据D传输给TIMSP430微处理器进行处理，TIMSP430微处理器在该硬件结构中有着核心大脑的作用，它首先会对存储数据N进行备份保存，然后根据命令数据D依次对JTAC调试模块和串口模块进行命令下达，完成下载调试和计算机整体信息连接的任务，保证数字化校园网信息安全加密系统的正常运行[7-8]。

在本文设计的数字化校园网信息安全加密系统的硬件中，MF RC500F射频芯片硬件与TIMSP430微处理器核心硬件之间的具体配合关系如图2所示。

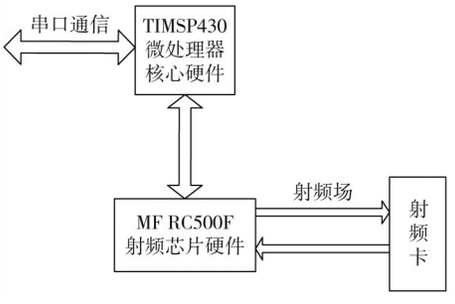

图2 射频芯片硬件与微处理器核心硬件的配合关系

1.3 硬件接口设计

本文设计的硬件接口采用了将MF RC500F射频芯片硬件和TIMSP430微处理器核心硬件以SPI通信理念进行连接的方式，将二者结合，只以一个SPI接口与微处理器的串口进行连接并通过这个接口完成设置和收发数据的工作。在TIMSP430微处理器核心硬件与MF RC500F射频芯片硬件的通信过程中，TIMSP430微处理器核心硬件为主机，MF RC500F射频芯片硬件为从机，MF RC500F射频芯片硬件在接收TIMSP430微处理器核心硬件的数据信号的条件下进行工作，二者之间的I/O连接示意图如图3所示。

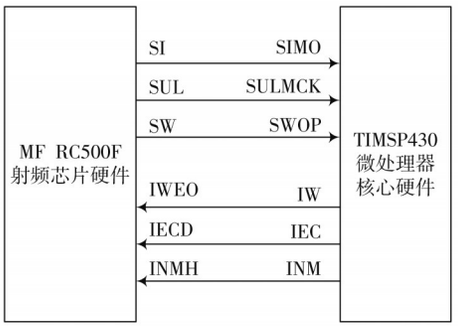

图3 MF RC500F射频芯片硬件与TIMSP430微处理器核心硬件的I/O连接示意图

2 基于物联网技术的数字化校园网信息安全加密系统软件设计

本文在系统硬件设计的基础上,融合物联网技术,设计软件程序协同硬件系统工作。为保证校园网信息安全,设计加密程序对敏感和隐私数据进行加密,即使发生数据泄露,在没有解密文件的情况下也无法读取和还原信息。因此,设计显示程序对敏感和隐私信息的显示进行控制,两种程序的设计和实现方案如下。

2.1 基于物联网技术的数字化校园网信息安全加密程序设计

加密程序的设计与实现流程如图4所示。

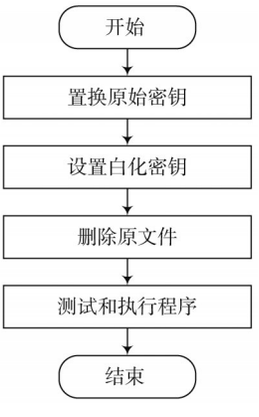

图4 加密程序的设计与实现流程

1)置换原始校园网的密钥。对用户输入的信息解锁密钥,将一半偶数位置的字符与另一半奇数位置的字符进行位置置换,置换公式如下:

$$\mathrm{pos}[i] \Leftrightarrow \mathrm{pos}[\mathrm{len}-i-1] \tag{1}$$

式中:i表示字符标号;len表示字符串长度。

2)设置白化密钥。利用C语言的操作函数读取加密信息内容,将信息内容白化,由用户设置6个字符长度的白化密钥,并允许用户在指定条件下对白化密钥进行修改[6,9]。

3)删除原始文件。对未实行加密的源信息文件进行删除,避免源文件的泄漏,并随机对原始文件进行覆盖,根据信息种类的不同,覆盖次数也存在差异,覆盖次数的计算方式如下:

$$a = \frac{d}{g}\left(\sqrt{e} + \frac{\sin k}{\cos l}\right) \tag{2}$$

式中:a表示覆盖次数;k表示信息编号;l表示信息识别码;d表示信息的敏感程度;g表示信息的隐私程度;e为计算常数[10]。

4)测试和执行程序。采用测试软件对程序进行测试,对比加密文件和源文件的信息,保证信息的完整性。

2.2 基于物联网技术的数字化校园网信息安全显示程序设计

显示程序的工作是读取指定页面内的校园网信息,根据数据加密设计,在指定地址输入解密密码,显示需要的信息,对敏感数据和隐私数据进行隐藏,通过身份认证后可显示全部数据信息,合成信息显示界面,由硬件设备中的输出设备进行显示。程序开始运行时,显示程序通过设备访问请求匹配请求信息所在的编号,程序根据编号所在位置和识别标志调用配套程序提取字符显示的代码,放入信息显示缓冲区域,然后计算界面存放的起始地址,起始地址的计算公式如下:

$$H = (c - 32) + n \tag{3}$$

式中:H表示起始地址所在编号;c表示IP地址;n表示子机数。

确定起始地址后,从当前页面地址显示信息,读取信息的ASCII码判断所需显示信息是否包含敏感信息和隐私信息,若包含,显示程序自动隐藏,由用户选择是否继续显示隐藏信息,若用户发送请求,则需进行信息认证,在认证成功后显示全部信息;若用户没有发送请求,界面显示完成,安全退出显示程序,回到系统主程序。显示程序的工作流程如图5所示。

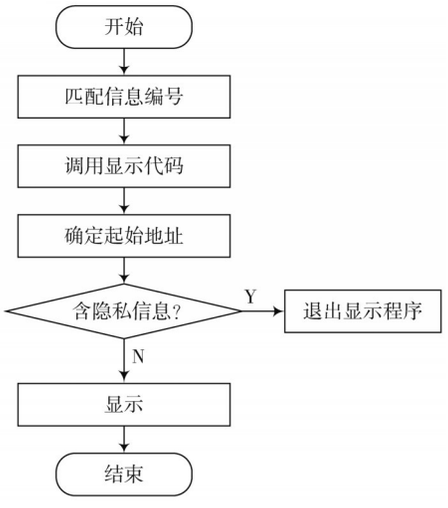

图5 显示程序的工作流程

3 实验与研究

针对加密系统信息设置相应的系统检验操作，构建对比实验对加密系统的加密效果进行检验，并设置实验参数如表1所示。

表1 实验参数

参数	取值及设置
信息文件大小 /GB	10
密钥数量	6
网络连接	物联网系统连接
数据长度 /bit	64
结构关系	逻辑结构

对实验环境进行相应的规定，添加数据加密密码，并固定明文长度的密码应用形式，在格式化处理后，对明文长度进行分组切割操作。利用不同的加密密码信息对分组切割的数据进行整理，同时加密这些切割数据，根据不同的数据分组对加密密码进行系统转化，连接系统字码与密钥间的加密属性沟通通道，减少对数据的密码解析操作，进而降低数据分析的穷尽值。由此便于在进行实验研究的过程中更好地掌控研究系统的处理方式。

为进一步安全存储校园网信息，将独立的数据名单信息符号一一对应添加至校园信息数据库中，并在执行数据收录指令后开启系统的自主记录模式，避免因记录的数据重复而造成信息操作失败。重复以上系统实验操作，并获取检验的加密结果。对比不同加密系统的加密安全程度，实验对比结果如图6所示。

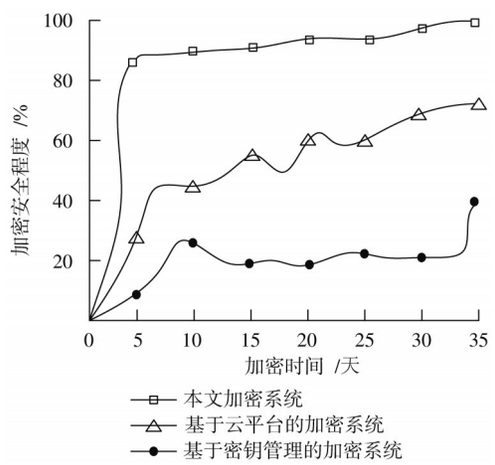

图6 加密安全程度对比

根据图6可知，本文基于物联网技术的数字化校园网信息安全加密系统的加密安全程度高于传统系统设计，表明本文系统设计具有更好的加密性能。造成此种差异的主要原因在于：本文系统设计对校园网的信息掌握程度较好，较高地利用了数据的初始性能，促使系统得到了更好的完善，提升操作的有效性，结合算法研究，增强操作结果的数据可行性，具有较高的加密安全性，当进行数字化校园网信息获取的同时，构建中心操控系统对校园外界信息进行阻拦，并清除与校园网信息无关的数据内容。

在执行数据审核的同时建立加密算法，在软件应用程序中对加密算法进行基础性整合。不同的终端数据存在着长度差异，为此，在进行分组时应将不属于同一组别的数据分离，同时在数据无法扩张的前提下执行特殊加密处理，确保加密算法的有效运行。

当执行数据加密指令时，利用中心系统将检测的数据信息由基础长度转化为二进制为主的64 bit数据，若出现加密数据数量过少的情况，则随机选择加密数据进行数据空间填充操作。由此，能够提升整体安全加密系统的空间修复能力，进而获取加密安全程度更高的校园网信息数据。

在完成上述实验操作后，检验加密系统的加密时长，以此分析加密系统是否能够适应后续研究的要求，并构建加密系统检验结构如图7所示。

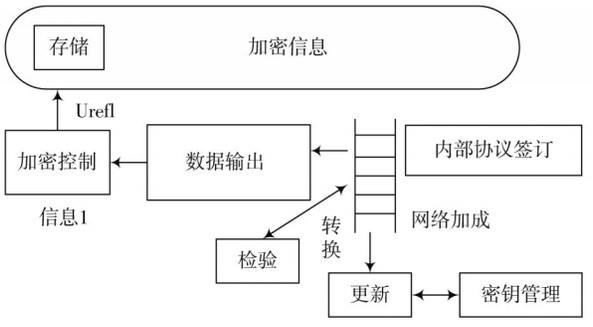

图7 加密系统检验结构

物联网的内部数据信息之间有着较为密切的逻辑连接关系，同时，不同的逻辑数据对应的数据关系不同，为此，在进行数据加密时，应注意对终端个体信息结构的调整与辨别，增强对密钥信息的管理力度，同时结合组织空间数据的存储特性对密钥状态进行特殊管理，在管理的同时注重对数据关系的维护，避免因数据关系破裂而造成系统密钥信息泄露现象，并维护实验检验系统的安全，避免因系统故障而导致的实验检测失败现象。以维护后的系统为操作对象，获取实验对比信息，并对比构建加密所需时长，如图8所示。

根据图8能够分析出，本文基于物联网技术的数字化校园网信息安全加密系统的加密所需时长短于其他两种传统系统的加密所需时长，由于本文系统在设计的过程中检验了不同网站中的校园网信息，同时结合物联

网的数据联合功能调整了安全加密系统的密保装置,当产生异常数据时,密保装置将自动启动密保模式,及时调整密保信息,并加强对校园网的保护力度。分配相应的密保数据信息,扩展密保的信息范围,管理系统内部的密钥形态,当密钥形态发生变化时,关键密钥将主动担任信息数据传输的功能,并将校园网信息安全传送至加密空间中,减少了不必要的操作麻烦,进而缩短了操作时间,加密所需时长较短。

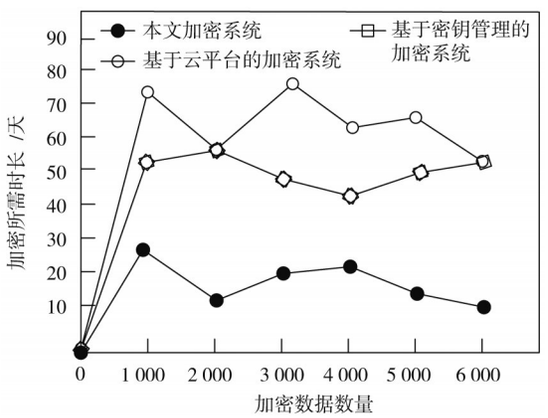

图8　加密所需时长对比图

综上所述,本文基于物联网技术的数字化校园网信息安全加密系统的加密安全程度较强,操作简便,可在不同的操作环境下执行加密指令,加密的数据具有更强的自主保护能力,符合后续研究的发展要求,具有良好的发展空间。

4　结　语

针对数字化校园网信息保护系统安全程度较低,加密所需时间过长,本文设计并实现了一种基于物联网技术的数字化校园网信息安全加密系统,以物联网技术为基础,采用核心硬件增强系统对数据的处理能力,为软件的应用提供运行平台,设计信息加密程序和信息显示程序,有效地对校园网信息进行加密保存和加密显示,保证信息的完整性和安全性,提升加密程度,对原文件进行彻底清除,满足用户的需求,促进了物联网技术的发展,更为其他形式的信息保护提供了借鉴。

参　考　文　献

[1] 连扬鹏.基于物联网技术的数字化院前急救平台的设计与应用[J].中国数字医学,2018,13(5):19-23.

[2] 夏鲲,付夏乐,陈昂辉,等.基于物联网的智能饮水机系统设计与实现[J].电子测量技术,2018,41(8):46-53.

[3] 牛犁青,杨毅.基于物联网的温室大棚数字化管理系统设计与仿真[J].电子设计工程,2019,27(3):76-81.

[4] 杨帆,宋开怀.基于物联网技术的幼儿园儿童监管系统设计[J].自动化与仪表,2018,33(8):84-88.

[5] 何业慎,梁琨,谭威,等.基于物联网技术的智能变电站安防监控系统[J].电信科学,2018,34(9):179-185.

[6] 张卫明.物联网视域下高校实验室安全智能化管理研究[J].微型电脑应用,2018,34(8):54-56.

[7] 黄国富,王莅雯.基于物联网技术的肉牛屠宰加工管理信息系统[J].青岛农业大学学报(自然科学版),2018,35(2):157-160.

[8] 徐越峰,冯杰,纪云鸿,等.基于物联网技术的电力现场作业安全管理系统设计[J].制造业自动化,2019,41(8):110-114.

[9] 张志强,黎忠文,巫恒强,等.基于物联网农田环境数据的安全访问控制[J].科学技术与工程,2019,19(31):206-214.

[10] 李玉文,李娜,谭慧,等.基于物联网技术的核应急现场辐射监测系统的初步设想[J].中国急救复苏与灾害医学杂志,2018,13(2):110-111.

作者简介:高　静(1980—),女,江苏邗江人,研究生,中级工程师,研究方向为数字化校园建设。