计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190600075

基于区块链与人工智能的网络多服务器SIP信息加密系统设计

任 仪
河南省人民医院 郑州 450000

摘 要 采用传统加密系统只能实现单个信息共享,无法保证多个信息共享安全,为了解决该问题,文中提出并设计了基于区块链与人工智能的网络多服务器SIP信息加密系统。在网络多服务器SIP条件下,设计USB模块,在该模块中安置状态寄存器静态转换开关,判断USB信息存储状态,在USB模块中搭建信息接口,使用A/D转换器进行信号转换,为任务调度提供基本信息传输信号。添加调度规则,将经过调度的信息分成若干个数据块,依据锁盒思想,使用功能调用函数集合检查访问权限,生成认证密钥,设计加密执行模块,按照时间顺序将分解的信息以一定顺序组合成链式数据结构,通过计算最初数据矩阵,获取初始指纹,依据该指纹设计具体加密执行方案,通过区块链与人工智能技术实现信息的加密。通过实验对比结果可知,该系统的信息传输完整性较高,具有良好加密效果,且该系统的读写效率始终保持在90%以上,增加了信息的读写效率。

关键词:区块链;人工智能;移动agent技术;网络多服务器SIP;加密;USB;调度规则
中图法分类号 TP309

Design of Network Multi-server SIP Information Encryption System Based on Block Chain and Artificial Intelligence

REN Yi
Henan Provincial Peoples Hospital,Zhengzhou 450000,China

Abstract The traditional encryption system can only realize single information sharing and can not guarantee the security of multiple information sharing. In order to solve this problem,network multi-server SIP information encryption system based on block chain and artificial intelligence was put forward and designed. Under the condition of network multi-server SIP,USB module is designed and a state register static switch is installed in the module to judge the storage state of USB information,build information interface in the USB module,and use A/D converter for signal conversion,to provide basic information transmission signals for task dispatching. Add dispatching rules,divide the dispatched information into several data blocks. According to the lock box idea,use the function call function set to check the access rights,generate the authentication secret key,design the encryption execution module,according to the time sequence,combine the decomposed information into chain data structure in a certain order,to get the initial fingerprint by calculating the initial data matrix,specifically and secretly execute scheme according to the fingerprint design,and realize the information encryption through block chain and artificial intelligence technology. Experimental comparison results show that the system has high information transmission integrity and good encryption effect,and the reading and writing efficiency of the system is always maintained at 90% and above,which increases the reading and writing efficiency of information.

Keywords Block chain technology,Artificial intelligence,Mobile agent technology,Network multi-server SIP,Encryption,USB,Scheduling rules

以往网络存储技术虽然在信息管理与共享方面具有良好性能,但是,新的安全隐患也随之而来,用于存储信息的服务器可能不在用户控制的范围之内,传统的加密系统在数据安全方面做得不够全面,随着计算机处理技术不断提高,人工智能化不断发展,信息保密性受到了人们严重质疑,为此,设计了加密系统[1-2]。使密钥扩展到112位,信息加密程度的提升也导致系统复杂度提高,在常规电脑上实现加密系统的设计已经无法满足系统实时性要求[3-5]。因此,将加密系统分为非共享系统和共享系统。其中,非共享系统不可以被多用户共享,而共享系统则可以被共享,前者虽然不需要考虑加密密钥管理问题,但是这种系统无法满足企业复杂环境下的数据共享需求;而后者必须管理加密密钥,保证每个用户都能得到访问信息的基本权利[6]。采用传统加密系统只能实现单个信息的共享,一旦某个用户从组合中退出,那么将不再拥有访问权限。文献[7]提出一种针对采样报文关键内容进行微型加密算法(TEA)运算的加密方法,并利用循环冗余校验(CRC)验证码进行解密后的报文完整性检查。但是该系统的网络负载率较高。文献[8]提出了一种基于移动通信设备认证的动态加密方案,采用分组密码体制,在分组中添加移动设备身份识别信息,然后使用动态加密方案对信息进行加密。但是该方

本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。

基金项目:河南省科技攻关计划项目门诊预约挂号自助软件平台研究
This work was supported by the Application of Self-service Software Platform Outpatient Appointment Registration.

通信作者:任仪(147060458@qq.com)

法的数据传输安全性较低,降低了信息的读写效率。

对于以上问题,本文设计了基于区块链与人工智能的网络多服务器 SIP 信息加密系统。基于区块链与人工智能的网络多服务器具有分布式、可编程的特点,方便用户完成地址注册,保障信息传输安全;移动 agent 技术是系统构建中的新兴力量,具有智能性、自主性以及可移动性,最显著的特点就是降低了网络负载。

1　系统设计

信息加密系统是通过对数据加密转化,保证只有拥有权限的用户才能获取文件信息,利用区块链与人工智能,改变信息负载数码结构,实现对原始信息的保护[9]。系统集成 USB 接口权限模块,采集并存储用户特征值作为基础登录的凭证,采用区块链与人工智能技术对网络多服务器 SIP 信息进行加密处理,加密密匙靠指纹特征值实现,并利用人工智能中的移动 agent 实现信息的加密传输,弥补了传统加密中密匙分发应用第三方引起的不足,提供一个直接的安全信息传输机制,改善了原有传输模式下网络负荷增加与安全性完全依赖于第三方的不利。指纹采集模块负责采集和存储用户信息,在系统加密过程中,将返回存储的指纹特征运行在用户终端上,通过软件功能中的加密算法实现对用户重要信息的加密。

1.1　硬件结构设计

网络多服务器 SIP 信息加密系统是一个面向互联网的多媒体实时业务控制协议系统,在服务模式下,分析了 SIP 网络体系结构。用户代理和 SIP 网络服务器组成了硬件结构,其中用户代理又是由用户客户端、代理服务器构成的,用户客户端负责发起 SIP 呼叫请求,代理服务器负责对呼叫请求作出回应,社交网络服务为用户代理提供注册、认证和路由服务[10]。

1.1.1　USB 模块

加密系统硬件结构主要是由数字信号处理器的加密模块和 USB 数据传输模块组成的,如图 1 所示。

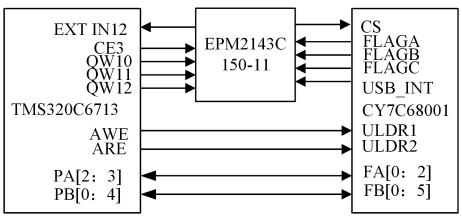


图 1　USB 模块硬件连接图

Fig. 1　USB module hardware connectivity diagram

由图 1 可知:数字信号处理器核心模块采用的是 TI 公司生产的 24 位 TMS320C6713 型号芯片,主要频率高达 350MHZ,通过数字信号处理器外部存储接口的外扩同步动态随机存储器可将存储容量提升 2M。为了实现系统智能上电,需在 CE3 空间外部扩展 AM29F800 型号的 FLASH 芯片;USB 传输采用某公司生产的 CY7C68001 型号芯片,该芯片集成了 USB2.0 收发接口和串行引擎接口,在链路层具有 4 kB 的 FIFO 存储器,支持信息高速传输[11-13]。USB 模块通过复杂可编程逻辑器件接入到 EMIF 接口处的 CE3 空间;而复杂可编程逻辑器件经过数字信号处理器接入到外部中断的 EXT_INT6。因此在复杂可编程逻辑器件中安置一个状态寄存器静态转换开关,用于判断 USB 中各个 FIFO 对信息的存储状态,方便系统在其它设备下快速查询外部中断源。

1.1.2　接口模块

在设备中搭建信息接口,需要使用 A/D 转换器进行电流、电压转换,接口电路图设计如图 2 所示。

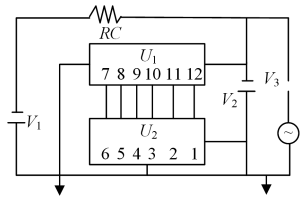


图 2　接口电路图

Fig. 2　Interface circuit diagram

保证设备接口电路 A/D 转换器输入总值达到 2.5V 左右,持续周期为 20ms,电路中的直流偏移量为 3.0V 正弦信号,经过设备接口 A/D 转换器的信号转换,可将 14 位数字信号传送至 D/A 转换中作为输入值,根据电路信息完成 D/A 转换后的信号模拟,通过接口电路中的 RC 信号滤波器进行信号输出处理,为模块调度提供支持[14]。

1.1.3　调度模块

通过接口电路设计,可对经过的电流和电压值进行控制,管理调度其他涉及到的设备的信息流程,执行信息调度。依据系统软件部分的信息加密流程,设置相关调度规则,合理控制调度时间,以达到网络多服务器 SIP 信息加密的要求,补充信息调度的规则,删除多余信息调度规则,重置相关信息规则[15]。依赖接口模块,通过产生的中断方式为任务调度提供基本信息传输信号,该调度通常分为两种,事件驱动调度和非集成事件驱动调度。其中,事件驱动调度是对优先处理的事件进行中断处理,使其与任务优先级相对应,只有当优先级高于正在进行任务级别时,才会被制止,等待优先级事件先行处理后,才可由后续事件进行处理;而非集成事件驱动调度是通过中断外部活动,才能保证优先级任务执行的有效性,由此设计锁盒子和访问控制模块。

1.1.4　锁盒子和访问控制模块

将经过调度的网络多服务器 SIP 信息分成各个数据块,每个数据块都具备一个随机产生密钥,根据锁盒子思想,单个文件中的所有文件块密钥都存放在其所对应的锁盒子之中,使用该文件的密钥进行加密处理,每个文件块密钥仅对应一个版本号,为用户权限修改提供保障。在锁盒子中的文件块密钥具有散列值,用来矫正数据块的完整性,将文件中所有的数据块散列值组织成默克尔散列树,散列值树的根用文件专属密钥进行加密后才可存储到控制模块之中[16]。

每个数据块都对应一个访问控制模块,用来控制用户获取文件签名密钥和锁盒密钥。访问控制块中所包含的文件具有访问属性、文件版本号和完整性标识,其中文件签名密钥和锁盒密钥都是使用功能调用函数集合来维护加密密钥,只有功能调用函数集合才能解密。访问控制属性是由文件拥有者创建的,并由功能调用函数集合检查访问权限;完整性标识是用来防止对访问空间的控制,由此生成的认证码具有认证密钥,并由功能调用函数集合维护,有效避免了文件信息输入都是由功能调用函数集合重新生成访问控制块的繁琐程序。

1.1.5　加密执行模块

网络多服务器 SIP 信息加密执行模块设计如图 3 所示。

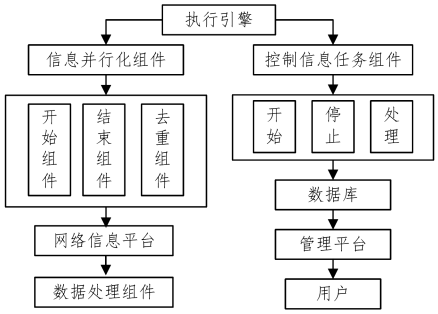


图 3 网络多服务器 SIP 信息加密执行模块

Fig. 3 Execution module of network multiserver SIP information encryption

加密执行是在锁盒子和访问控制模块的基础上实现的，具体执行两个步骤：信息数据处理节点的并行化和信息流程任务的控制[17]。其中，信息数据处理节点的并行化组件包括开始、信息结束、去重和排列，从网络中获取规则信息，分解处理相应信息，使其形成有序的信息处理组件节点，完成对数据处理组件的加载；在信息流程任务的控制中，主要是信息流程任务中的信息开始、停止和清理以及将该状态延续到存储过程，直至将全部数据存储到数据库中。

1.2 系统软件功能设计

SIP 服务器功能设计是为了给系统提供被加密信息的位置，使硬件和软件能够成功建立加密连接，实现对信息的认证、管理和收集等功能[18]。由于网络多服务器 SIP 是由多个服务器构成的，通过客户机发送的基于 SIP 请求可完成服务功能，并将完成信号送回相应的服务器之中，利用区块链以及人工智能实现软件功能的设计。

系统程序设计根据调用微软 USB 接口，在主机与总线之间交换数据，使用某公司提供的驱动程序，为 USB 设备请求和数据传输提供支持，也可直接用来开发上层软件功能。主机通过调用设备驱动完成硬件模块的控制，保证所有接口函数都应用在文件通用驱动程序源码中，通过对 USB 设备进行标准测试，使 Sx2SendVendorReq() 函数能够直接访问寄存器，查询系统工作 USB 标准；调用 Sx2GetDeviceDesc() 函数可查询设备具体信息，其中包括端口配置信息、字符串信息，通过数据包发送 SIP 命令，并直接访问设备命令端口，在大数据传送方式下，调用 Device Control() 函数可向驱动程序发送读写内容，以实现明文密钥发送。

系统软件功能设计流程如图 4 所示。

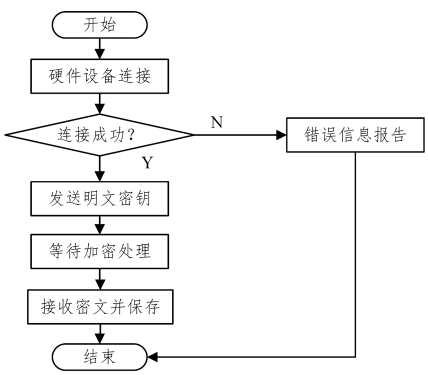


图 4 系统软件功能设计流程

Fig. 4 Functional design flow of system software

在信息加密过程中，使用区块链与人工智能技术，按照时间顺序将要传输的信息分解成毫无关系的数据，并以一定顺序组合成链式数据结构，以加密方式保存分布式信息。具体过程如下所示。

将信息源节点 Q 分解成 m 份数据，分别记为 $k_1, k_2, \cdots, k_m$，将分解后的数据全部发送至目标节点之中，在发送此信息之前，Q 会产生 r 个 m 维向量，其中每个数据向量都具有 m 个小分量，将这些分量记为 $w_1, w_2, \cdots, w_r$，由此获取的具体加密计算公式为：

$$w=(w_{i1}, w_{i2}, \cdots, w_{im}), i=1,2,\cdots,r \tag{1}$$

经过信息编码处理的矩阵为：

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_r \end{bmatrix} = \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1m} \\ w_{21} & w_{22} & \cdots & w_{21} \\ \vdots & \vdots & & \vdots \\ w_{r1} & w_{r2} & \cdots & w_{rm} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} \tag{2}$$

将加密过程中的 r 个 m 维向量代入上述公式中进行编码计算，由此可获取在 t 时间内 r 个经过编码处理后的数据包，记为 $b_1, b_2, \cdots, b_r$，计算公式为：

$$b_i = w_i (a_1 a_2 \cdots a_m)^t, i=1,2,\cdots,r \tag{3}$$

信息源节点 Q 完成编码的数据与对应的编码信息向量进行统一打包处理，由此可获取 r 个经过编码后的数据包，将这些数据包传送到目标节点之中。目标节点接收到信息后，进行编码处理后所产生的向量是无线性的，因此可获取最初数据矩阵，如下所示：

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} = \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1m} \\ w_{21} & w_{22} & \cdots & w_{21} \\ \vdots & \vdots & & \vdots \\ w_{r1} & w_{r2} & \cdots & w_{rm} \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_r \end{bmatrix} \tag{4}$$

根据式(4)最初数据矩阵选择密钥用户存储的初始指纹，该指纹是由 512 个字节组成的，对于设备密钥存储来说是相对安全的。在安全加密环境下，使用区块链与人工智能技术设计具体加密执行过程，如下所示：

1)用户选择文件信息；

2)指纹身份识别；

3)是否注册新用户，如果是，则将该用户作为第一个指纹模板，如果不是，则说明程序异常，无法执行加密，需重新选择文件；

4)根据上述公式对文件进行加密；

5)是否删除源文件，如果是，则直接删除，如果不是，则说明程序正常，可直接完成加密处理。

在完成网络多服务器 SIP 信息加密处理后，利用人工智能中的移动 agent 实现信息的加密传输。通过主 agent 在本地设备上产生一对密匙，两个密匙的功能分别是用于加密的公开密匙、用于解密的私有密匙。前者由子 agent 携带到远程机器上，用于数据加墨，后者由主 agent 进行保管，存放在本地设备上，不在网络中传递。当子 agent 在远程机器上完成任务，将密文传递给主 agent 后，主 agent 使用解密密匙得到明文，完成一次安全的信息传输。在整个过程中，在网络上传递的只有用于加密的公开密匙以及加密后生成的密文，即使信息被截获，也无法破译，保证了信息在网络中传输的安全性。

根据 SIP 网络体系，设计 USB 模块，采用 TMS320C6713 型号芯片，通过数字信号处理器提升存储容量，经过复杂可编

程逻辑器件接入到 EMIF 接口,并在其中安置寄存器静态转换开关,用来判断信息存储状态;使用 A/D 转换器实现信号高效转换,通过接口电路中的 RC 信号滤波器进行信号输出处理,为模块调度提供支持[19-20]。根据网络多服务器 SIP 信息加密要求,添加相应调度规则,依赖接口模块,为任务调度提供基本信息传输信号,保证优先级任务执行的有效性。将经过调度的信息分成若干个数据块,依据锁盒思想,矫正数据块的完整性,由功能调用函数集合检查访问权限,完整性标识用以防止对访问空间的控制,由此生成的认证码具有认证密钥。在该条件下,设计加密执行模块,为软件功能设计提供平台。设计系统软件功能,在安全加密环境下,使用区块链与人工智能技术执行信息加密方案,由此实现网络多服务器 SIP 信息加密系统设计。

2　实验

在物联网环境下进行测试,以衡量使用区块链与人工智能技术对网络多服务器 SIP 信息加密系统性能的影响,实验内容主要针对加密程序的读写性能进行验证。

2.1　实验参数设置

采用 Intel PentiumIIIx4 型号处理器作为测试服务器的主要配置,运行内存为 1 GB,运行系统为 Redhat Linux,不同加密操作流程所耗费的成本都是由 Crypto API 库函数进行计算的。在该系统中,数据块大小为 4 kB,使用 128 bit 密钥进行加密计算,为了获取加密锁盒子耗费成本,假设使用的比特密钥长度也为 128,以保证系统性能测试不受到成本影响,具有精准测量结果。

2.2　性能测试结果与分析

使用文件系统的读写性能测试工具对系统性能进行实验验证分析,并与传统加密系统进行比较,实验环境由以太网进行连接,主要服务设备分别充当客户端和代理客户机。

将文件大小内存改为原来的 2 倍,避免文件缓存问题的产生,两种系统不同数据大小下的安全吞吐率变化结果如图 5 和图 6 所示。

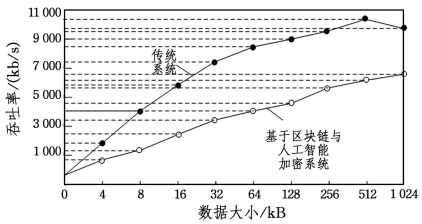


图 5　随机读性能对比分析

Fig. 5　Comparative analysis of random reading performance

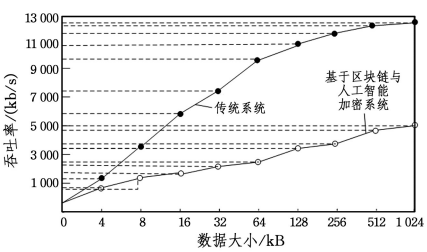
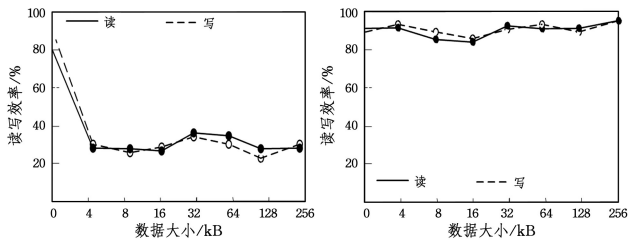


图 6　随机写性能对比分析

Fig. 6　Comparative analysis of random writing performance

由图 5 和图 6 可知:使用区块链与人工智能设计的系统对吞吐率影响随着数据量的增加而逐渐变大,但最终稳定在 5 000～7 000 kB/s 吞吐率范围内。而传统系统随着数据量的增加,吞吐率持续增大,在随机读性能下,当数据量为 512 kB 时,吞吐率高达 10 500 kB/s;在随机写性能下,当数据量为 1 024 kB 时,吞吐率高达 12 000 kB/s。出现吞吐率过高的主要原因是传统系统加密出现延迟,导致数据响应时间随着数据量的增加低于线性变化范畴,因此,在该情况下,采用区块链与人工智能设计的系统随机读写性能较好。

进一步验证该系统的性能,需在不同数据大小下按照一定顺序分析读写性能,结果如图 7 所示。



(a)传统系统的读写效率　(b)基于区块链区块链与人工智能加密系统的读写效率

图 7　顺序读、写性能对比分析

Fig. 7　Comparative analysis of sequential reading and writing performance

由图 7 可知,在数据较小时,这时由于文件较小,数据被缓存在客户端中,不会触发加密操作。因此,在该情况下,两种系统读写性能都相对较好。随着数据大小的变化,可以看出,传统系统的读写效率下降速度尤为明显,而基于区域链与人工智能的加密系统的读写效率始终保持在 90% 以上,原因是移动 agent 将任务分解到了不同的设备上进行处理,避免了传输过程中第三方应用的风险,提高了数据传输的安全性,从而增加了信息的读写效率。为了验证该点,将两种系统信息传输中网络负载率进行对比分析,以此作为系统加密验证效果,结果如表 1 所列。

表 1　两种系统网络负载对比分析

Table 1　Comparative analysis of network load of twosystems

数据大小/kB	区块链与人工智能下的系统/%	传统系统/%
4	63	95
8	51	96
16	67	93
32	43	97
64	47	93
128	53	95
256	52	98

由表 1 可知:当数据大小为 4 kB 时,区块链与人工智能下的系统比传统系统网络负载率低 32%;当数据大小为 8 kB 时,区块链与人工智能下的系统比传统系统网络负载率低 45%;当数据大小为 16 kB 时,区块链与人工智能下的系统比传统系统网络负载率低 26%;当数据大小为 32 kB 时,区块链与人工智能下的系统比传统系统网络负载率低 54%;当数据大小为 64 kB 时,区块链与人工智能下的系统比传统系统网络负载率低 46%;当数据大小为 128 kB 时,区块链与人工智能下的系统比传统系统网络负载率低 42%;当数据大小为 256 kB 时,区块链与人工智能下的系统比传统系统网络负载

率低46%。由此可知,区块链与人工智能下的系统比传统系统网络负载率低得多。

2.3 实验结论

在随机性能读写条件下,传统系统是由于加密过程中出现延迟,导致数据响应时间随着数据量的增加而低于线性变化范畴,使吞吐率过高;而区块链与人工智能技术下的系统依据锁盒思想,不会出现加密延迟现象,具有稳定吞吐率。

按照一定顺序读写条件下,由于区域链与人工智能技术下的系统不依靠第三方进行信息传输,因此具有网络负载率较低,增加了系统使用上的灵活性。

结束语 采用区块链与人工智能设计网络多服务器SIP信息加密系统,可满足多个信息的共享,满足对加密系统密钥管理的安全性与高效性。同时SIP协议具有易扩展性,在完善传统系统信息共享的同时,还完善身份认证功能,以此抵抗各种攻击。在信令加密方面,该系统存在端和点之间的加密保护,保证SIP实体安全,隐藏SIP信息传输通道,进而使攻击者无法识别信息发送与接收的具体路由信息,也就无法进行主动攻击。在信息传输方面,该系统克服了传统系统需要引入第三方设备的不足,进一步增加了加密系统密匙管理的安全性。测试结果表明,该系统在提升性能的同时,也保障了文件的安全。

下一步计划研究具体某个文件名称的加密处理,因为文件名称数据也是攻击者恶意攻击系统的主要通道,所以在下一步工作进程中,优化锁盒方法,降低存储开销,扩展方案详细设计。

参 考 文 献

[1] SUN J G. Prospects for the development of blockchain technology [J]. China Finance, 2016, 262(8): 23-24.

[2] LI M, TANG Y. Design and Implementation of Distributed Web Search Model Based on Mobile Agent [J]. Computer Applications and Software, 2016, 33(4): 18-21.

[3] LI X G, SHEN Y L, KANG X Q. Hyper-chaotic two-way authentication private information security encryption algorithm [J]. Science bulletin, 2017, 33(8): 152-155.

[4] ZHANG X W, LI H K, YANG Y T, et al. Personal information privacy protection logistics system based on two-dimensional code technology [J]. Computer Applications Research, 2016, 33(11): 3455-3459.

[5] CHEN W X, ZHANG T J, LIN J Q, et al. Mobile Agent Based Opportunity Opportunity Transmission Control Method [J]. Journal of Jiangsu University (Natural Science Edition), 2018, 39(3): 66-72.

[6] GUO S N, JIANG X Q. Design of Information Encryption and Decryption System for Emergency Communication Network [J]. Modern Electronic Technology, 2017, 40(17): 94-97.

[7] WANG Z D, WANG G, LI Y C, et al. IEC 61850-9-2LE message encryption method based on micro-encryption algorithm [J]. Power System Automation, 2016, 18(4): 121-127.

[8] ZHANG B, WANG H. A dynamic packet encryption scheme based on mobile communication device authentication [J]. Electronic Design Engineering, 2018, 26(22): 68-71.

[9] MA W W. Esearch on Security Encryption of Information Collection under Mobile Internet [J]. Electronic Design Engineering, 2018, 26(23): 52-56.

[10] JIANG D D, SHANG Y L, TIAN Y, et al. Construction of electronic warehouse single flow platform based on blockchain [J]. Journal of Xi'an Engineering University, 2017, 31(6): 828-834.

[11] CAI K. Magos AI project brings artificial intelligence and neural network technology to the blockchain field [J]. Computer & Network, 2017, 43(18): 77.

[12] ZHOU R M, ZHANG W X. Analysis on Risks and Control of Financial Technology Innovation—Based on Big Data, Artificial Intelligence and Blockchain Research [J]. China Management Information Technology, 2017(19): 33-36.

[13] PAN J F, HUANG D C. Influence of Blockchain Technology on Artificial Intelligence [J]. Computer Science, 2018, 45(S2): 53-57.

[14] XIE W. GMIC Global Financial Innovation Summit: When Big Data, Artificial Intelligence, Blockchain Technology Meets Finance [J]. China Economic Weekly, 2016(18): 50-51.

[15] PENG J J, LONG R L. Research on Key Technologies of Security Protection in Blockchain Application Environment [J]. Network Security Technology and Application, 2018, 210(6): 29-36.

[16] YANG M J. Design of Data Transaction Platform Based on Password and Blockchain Technology [J]. Information and Communication Technology, 2016(4): 24-31.

[17] TIAN H B, HE J J, FU L Q. Privacy Protection Fair Contract Signing Agreement Based on Public Blockchain [J]. Journal of Cryptography, 2017, 4(2): 97-108.

[18] CHEN T, MA M, XU X L. Application Research of Blockchain in Information Sharing and Use of Smart City [J]. E-Government, 2018, 187(7): 36-45.

[19] ZHOU J. Application of Mobile Agent Technology in Enterprise Network Management [J]. Network Security Technology and Application, 2017(6): 155-156.

[20] YE X R, SHAO Q, XIAO R. Supply Chain Prototype System Based on Blockchain, Smart Contract and Internet of Things Based on Blockchain [J]. Science & Technology Review, 2017, 35(23): 62-69.

REN Yi, born in 1985, undergraduate, engineer, is a member of China Computer Federation. His main research interests include hospital informatization and so on.