基于人工智能的企业网络多服务器SIP信息加密系统设计

杨鑫 王力 王亚伟 王郑 营海生
中国移动通信集团内蒙古有限公司 内蒙古 呼和浩特 010010

摘 要 传统网络存储技术虽具备良好的信息管理与共享能力，但仍面临安全隐患：存储服务器脱离用户直接控制，传统加密系统效率低下。随着计算机处理技术的提升，信息保密性进一步受到挑战。为此，针对企业现有加密系统对网络攻击敏感性不足的问题，本文提出一种基于人工智能的多服务器会话发起协议（SIP）信息加密系统。该系统在多服务器SIP架构下，集成通用串行总线（USB）模块、调度模块、锁盒式访问控制模块、加密执行模块、接口及加密服务器，实现企业网络数据的信号转换与动态任务调度。系统将任务划分为多个数据块，基于锁盒机制校验访问权限，并利用人工智能生成并执行自适应加密算法。实验结果表明，本文所提的系统在保障信息传输完整性与加密效率方面表现优异，能够有效满足企业网络安全运行需求。

关键词 人工智能；企业网络；信息加密；网络服务器

Design of a Multi-Server SIP Information Encryption System for Enterprise Networks Based on Artificial Intelligence

Yang Xin, Wang Li, Wang Zheng, Ying Hai-sheng, Han Jin-liang
China Mobile Communications Group Inner Mongolia Co., Ltd., Hohhot 010010, Inner Mongolia Autonomous Region, China

Abstract While traditional network storage technologies offer competent information management and sharing capabilities, they still face security vulnerabilities: storage servers operate beyond the direct control of users, and conventional encryption systems suffer from low efficiency. With advancements in computer processing technology, the challenge to information confidentiality has further intensified. To address the insufficient sensitivity of existing enterprise encryption systems to network attacks, this paper proposes an artificial intelligence-based multi-server Session Initiation Protocol (SIP) information encryption system. Operating within a multi-server SIP architecture, this system integrates a Universal Serial Bus (USB) module, a scheduling module, a lock-box access control module, an encryption execution module, interfaces, and an encryption server to achieve signal conversion and dynamic task scheduling for enterprise network data. The system partitions tasks into multiple data blocks, verifies access permissions based on a lock-box mechanism, and utilizes artificial intelligence to generate and execute adaptive encryption algorithms. Experimental results demonstrate that the proposed system excels in ensuring information transmission integrity and encryption efficiency, effectively meeting the security operational requirements of enterprise networks.

Key words Artificial Intelligence; Enterprise Network; Information Encryption; Network Server

随着网络技术的发展，企业信息安全日益受到重视。保护网络免受盗用、篡改与破坏，是企业稳定发展的关键。网络多服务器SIP信息安全性，对于保障企业各环节网络资源不受干扰、破坏和威胁至关重要[1]，已成为研究热点。当前，隐藏网络信息的方法存在安全风险，必须通过加密手段防止信息泄露。加密技术通过特定算法改变数据格式，确保即使未授权用户获取加密参数，在无解密公钥的情况下也无法解读信息内容。密码学中的加密方法能有效隐藏明文，保障网络传输安全[2]。

现有研究，如可提取哈希证明系统提出多策略加密方案并加以验证，但针对企业网络多服务器SIP信息加密的研究尚不充分。为此，本文设计了一种基于人工智能的网络多服务器SIP信息加密系统，旨在弥补该领域的研究空白。

1 企业网络多服务器SIP信息加密系统的总体框架

在企业生存与发展的过程中，商业机密是企业重点内容，与企业的成败息息相关。在商业竞争中，时常会出现商业机密失窃等情况。所以，为了避免数据泄密、被盗取，要求企业安全技术部门研究一种适用于企业的信息保护方案，其落地应用对保障企业数据安全，具有重要意义。

在系统开发前，要先设计系统总体框架，作为后期系统的软硬件设计指导。本文系统的设计包括3层架构，每层处理的作业各有不同：①数据库层，此层处于系统的最底层，主要功能为企业敏感数据的存取，并连接下层数据库加密服务器，便于企业信息读取；②数据库加密服务层，存储企业敏感数据，方便读取信息；③显示控制层，将操作指令发送到其他层。

2 企业网络多服务器SIP信息加密系统的硬件结构

2.1 USB模块

本文所设计加密系统的主要构成为USB数据传输模块、加密模块，由TI公司生产的TMS320C6173型号芯片作为数据信息处理器的核心模块，频率最高为350MHZ，并利用外部存储接口扩充存储器的容量为2 M。利用CE3空闲外部扩展的FLASH芯片，实现系统上电的智能化；将CY7C68001型号芯片作为USB传输接口，提高信息常数效率。将状态寄存器的静态转换开关安装在复杂可编程器件中，对USB中信息存储状态进行分析，便于系统对外部中断源的查询[3]。

2.2 调度模块

利用接口电路控制网络中的电压与电流值，有效管理设备信息流程的调度。通过系统软件功能对信息流程加密，并删除多余的调度规则，从而满足网络服务器SIP信息加密的需求。以中断方式实现任务调度信号的传输，主要模式有非集成事件驱动与事件驱动两种。前者在中断外部活动后，优先级任务的执行效率更高；后者通过对比不同任务优先级，高优先级任务完成处理后，再对后续事件处理。

2.3 锁盒与访问控制模块

调度网络多服务器SIP信息后，划分不同数据块，并赋能随机密钥。以锁盒理念将单一文件的密钥块存储在锁盒中，并进行加密。通过密钥散列值判断数据块的完整性，并在控制模块中存储专用密钥。通过设置数据块访问控制功能，对文件签名与锁盒密钥进行加密，并设置文件的访问权限。完整性标识能够避免不法人员对企业网络访问，所以生成认证密钥认证码，可保证控制块访问的安全性[4]。

2.4 加密执行模块

基于锁盒与访问控制模块，设计加密执行模块，详见图1。在信息数据处理节点中，由信息的开始、排列、结束、去重等操作构成并行化组件，并得出规则信息。通过信息分裂设计信息处理的组件节点，对信息流程加载，将所有数据存储在数据库中。

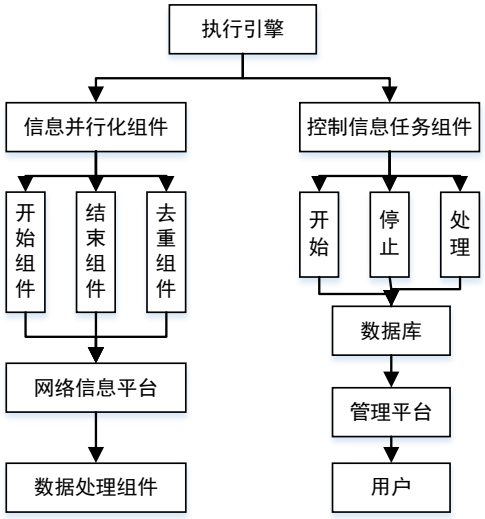

图1 加密执行机构的架构

2.5 接口与加密服务器

利用A/D转换器实现电压、电流的转换，并创建信息接口，保证接口电路转换器的总输入量为2.5 V，直流偏移量为3.0 V。A/D转换中输入14位数字信号，并模拟电路信息。

由数据加密卡、网络接口卡、工业控制计算机构成加密服务器，选择1900-15型号的工业控制计算机，为加密服务器提供分辨率为1 024 × 768的计算机平台；使用LRES1010PF型号网络接口卡，处理系统的加解密请求。此卡可在数据传输前对其进行加密处理，并智能化判断文件是否允许被打开[5]。

3 企业网络多服务器SIP信息加密系统的软件功能

3.1 企业通信数据收集

本文设计了多层次数据收集方案，为加密系统提供高质量的网络通信数据基础。在网络核心节点与出口边界部署采集设备，实时捕获企业全网流量；在服务器与终端侧安装客户端，采集进程行为、网络会话和系统日志等安全相关数据，兼顾全面收集与隐私保护；同时通过流量代理收集病毒、分布式拒绝服务攻击（DDoS）及僵尸网络等恶意流量，拓展数据维度，支撑威胁感知与分析。所有异构数据汇聚至平台，依托分布式消息队列实现高效读写，保障智能算法的低延迟、高可用数据访问。

3.2 信息安全加密模块

利用分组迭代加密算法，能够灵活改变数据块与密钥的长度，利用网络构造轮函数执行算法，包括非线性层、线性混合层与密钥加层：①非线性层能够利用混沌算法随机生成S盒，具有混淆作用；②密钥加密层的主要功能为密钥变换，使轮密钥与中间状态进行异或操作；③线性混合层实现行移位与列混淆的变换，保证多轮算法具备高度扩散性[6]。

在系统加密过程中，利用变换操作得出4行的二维矩阵，列数为*Nb*列，计算公式为：

$$Nb=\frac{E}{32} \tag{1}$$

式中，*E*—数据块的长度。

在128位明文快长度下的状态公式为：

$$B=\begin{Bmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} & b_{0,4} & b_{0,5} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} & b_{1,4} & b_{1,5} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} & b_{2,4} & b_{2,5} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} & b_{3,4} & b_{3,5} \end{Bmatrix} \tag{2}$$

公式中的$b_{0,0}$到$b_{3,5}$为数据库字节的映射顺序，在结束加密操作后，根据相同的顺序抽取密文状态。以二维字节数列构成加密密钥，有4行，*Nk*列，公式为：

$$Nk=\frac{P}{32} \tag{3}$$

式中，*P*—密钥块的长度（单位：位）。

在有128位密钥块长度时，密钥公式为：

$$C=\begin{Bmatrix} C_{0,0} & C_{0,1} & C_{0,2} & C_{0,2} \\ C_{1,0} & C_{1,1} & C_{1,2} & C_{1,3} \\ C_{2,0} & C_{2,1} & C_{2,2} & C_{2,3} \\ C_{3,0} & C_{3,1} & C_{3,2} & C_{3,3} \end{Bmatrix} \tag{4}$$

公式中的$C_{0,0}$到$C_{3,3}$为密钥块的字节，数据块列数*Nb*与密钥列数*Nk*共同决定，表示为*Na*。

3.3 身份加密体制

在信息加密模块下，加密体制中的原始数据量越大，就会增加平台中传输的文件量。例如，将系统视为独立的数据参量处理平台，则加密算法能够决定平台运行的能力。在既定网络环境中，信息孤岛会提高数据参量的加密压力；在信息量不断增加时，原本加密模块的信息负载压力也会增大，进而影响了系统运行能力。对此，可以在原本加密体制下，使网络信息划分为多个待执行的结构，分别存储并处理数据参量，直到能够控制信息孤岛的问题，改善企业网络环境。

系统中的加密数据参量为β，将设备加密数据样本的条件作为 $\hat{q}$ ，系统稳固加密体制的定义为：

$$R=\frac{\sqrt{(\beta-1)\left|D\times\hat{q}\right|}}{f^2\left(k_1+k_2\right)^2} \tag{5}$$

式中，*f*—系统数据保障的参量值；k_1与k_2—不同数据信息模块的加密系数。通过该公式对系统中的物理系数值进行处理、计算，保证系统的设计效果。

4 系统的性能测试

4.1 实验准备

为验证系统性能，构建含18个节点的数据中心网络环境，对比本文加密方法与传统方法，以评估企业网络数据的隐私性与安全性。实验数据容量在[1,10]范围内随机生成，确保结果代表性。系统运行于Windows 10环境，配置为32 GB内存、3.58 GHz CPU，满足实验需求。

4.2 实验结果

实验以信息数据丢失量为指标进行对比。结果显示：数据总量为1.5×10^6 bit时，本文系统与传统系统丢失量分别为12 bit和125 bit；数据总量为3.0×10^6 bit时，丢失量分别为13 bit和167 bit；数据总量为4.5×10^6 bit时，丢失量分别为15 bit和198 bit。实验表明，本文系统在不同数据规模下均表现出更低的数据丢失率，说明其在企业实际应用中具有更安全的信息共享能力[7]。

5 结束语

本文基于人工智能技术，设计了企业网络多服务器SIP信息加密系统。该系统可满足多信息数据的共享，并提高数据共享的效率与安全性。另外，系统还能够完善身份认证功能，避免外界攻击，提高加密系统密钥管理的安全性。测试结果表明，本文系统运行性能良好，文件安全性高。在后续研究中，将核心文件加密处理作为重点，对锁盒方法优化，降低存储成本，扩展加密方案。

参考文献

[1]奚宇航,黄一平,苏检德,等.基于国密算法的即时通信加密软件系统的设计与实现[J].计算机应用与软件,2020,37(6):303-308,327.

[2]庄惠雯.基于云计算的现代企业人力资源信息管理系统设计[J].信息记录材料,2023,24(4):143-145

[3]杨晓云,徐国华.基于循环移位运算的多服务器的密钥认证方案[J].计算机工程与设计,2022,43(10):2756-2761.

[4]付智慧,陆朝珍.基于稳固加密技术的网络信息安全传输系统设计[J].信息与电脑(理论版),2022,34(17):24-26.

[5]王钰,朱琳.基于物联网技术的造纸企业网络信息安全加密系统设计[J].造纸科学与技术,2022,41(3):34-38,49.

[6]袁科,程自伟,杨龙威,等.基于多时间服务器的时控性加密体制研究[J].电子与信息学报,2022,44(12):4319-4327.

[7]龙浩,张书奎,张力.群智感知网络中基于隐私保护的数据融合方法[J].计算机工程与设计,2020,41(12):3346-3352.

（本文编辑　曹　阳）