文章编号:1671-4598(2018)02-0068-04 DOI:10.16526/j.cnki.11—4762/tp.2018.02.018 中图分类号:TP393.08 文献标识码:A

大型数据库加密传输数据智能监测系统设计

胡晓东
(山西经济管理干部学院 电子信息工程系,太原 030024)

摘要:为解决传统加密传输数据监测系统在数据传输过程中易产生数据丢失、损坏等问题,提出并设计大型数据库加密传输数据智能监测系统;给出系统整体框架结构,硬件部分主要由四部分组成,用户登陆模块主要对访问角色进行划分,生成该身份对应的权限;密匙管理模块对权限信息进行保护和储存;文件安全传输模块对数据进行安全传输;系统软件部分主要对平分的64bit数据进行双路加解密,完成大型数据库加密传输数据智能监测系统设计;实验结果表明,该系统数据丢失率低、数据损坏少,有效提高了数据传输安全性,充分满足加密传输数据监测系统的设计需求。

关键词:数据库;加密传输数据;智能监测;系统设计

Design of Intelligent Data Monitoring System for Encrypted Data Transmission in Large Database

Hu Xiaodong
(Shanxi Institute of Economic Management, Taiyuan 030024, China)

Abstract: In order to solve the problems of data loss and damage in data transmission process of traditional encrypted transmission data monitoring system, a large database encryption transmission data intelligent monitoring system is proposed and designed. The whole frame structure system is given, the hardware part is mainly composed of four parts, the user login module mainly to access role division, generating the corresponding identity permissions; key management module for the protection and storage of information rights; secure file transfer module for data security transmission system; the software part of the double split 64bit data Luke decryption, complete large database encryption intelligent monitoring system data transmission design. Experimental results show that the system has low data loss rate and less data damage, effectively improves the security of data transmission, and fully meets the design requirements of encrypted transmission data monitoring system.

Keywords: database; encrypted transmission data; intelligent monitoring; system design

0 引言

大型数据库具有数据多、结构复杂等特点,为保证存储在大型数据库中数据的完整性,通常在数据传输过程中对数据进行加密处理[1]。但随着数据传输的范围不断扩大,网络应用环境越来越复杂,数据处理技术的飞速发展,即使是加密数据在传输的过程中,其安全问题依然存在[2]。在传输的过程中,导致数据传输不安全的因素主要包括数据丢失、受到非法篡改及窃取等。对数据库中加密数据的传输过程进行监测,是保障数据安全传输的有效方法。很多业内人士和专家学者已设计出一些加密传输数据监测系统,对加密传输数据进行有效监测[3]。文献[4]设计了一种基于SM4并行的数据库加密传输数据智能监测系统,该系统结合IEC104和ModBus协议,创建数据库自动重连机制,以数据交换界面形式将数据呈现给用户,该系统有效保障了数据传输安全性,但实时性较低。文献[5]设计了一种短距离数据库加密无线数据传输监测系统,将密钥存放在加密系统的USBkey中,采用Noekeon算法对数据进行加密[6],设计USB1001无线数据传输模块对加密后的数据传输过程进行监测,该系统数据传输可靠性高,但数据传输所用的时间较长。文献[7]设计了一种基于ISCSI的数据库加密传输数据智能监测系统,该系统采用ISCSI构建加密模块完成数据库中数据的加载,该模块在系统中是独立存在的,不需要对系统的内核进行更改,优化了系统的读写性能,但该系统的监测过程较为复杂[8]。为解决上述问题,设计出一种大型数据库加密传输数据智能监测系统,分别对系统硬件和软件部分进行优化,实现智能监测系统的设计。实验结果表明,改进系统数据丢失率低、数据损坏少,大大提高了数据传输的安全性。

收稿日期:2017-11-18; **修回日期**:2017-12-06。

作者简介:胡晓东(1980-),男,山西五台县人,硕士研究生,讲师,主要从事数据库、数据挖掘方向的研究。

1 整体框架设计

数据库加密传输数据智能监测系统由用户登录认证模块、密钥管理模块、混合加密模块和文件安全传输模块构成。大型数据库加密传输数据智能监测系统具体参数如表1所示。

表1 大型数据库加密传输数据智能监测系统具体参数

参数名称	参数数据
CUP	P50GHz
内存	145GB
连接口	COM1
波特率	19300Bd

大型数据库加密传输数据智能监测系统的整体设计如图1所示。

数据库加密传输数据智能监测系统通过用户登录认证模块对访问系统的用户进行认证,实现了系统用户与访问权限之间的逻辑分离。采用密钥管理模块对密钥进行生成、保存、查修、分发和修改等操作[9]。混合加密模块的主要功能是对大型数据库中的数据和文件进行加密和解密,并将完成加解密文件传送到系统的接收终端。文件安全传输模块由服务器端的应用

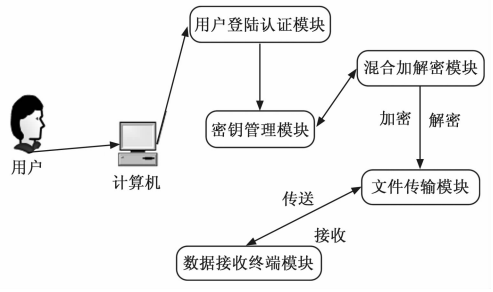

图 1　加密传输数据智能监测系统整体框架设计图

程序和客户端的应用程序构成，是大型数据库加密传输数据智能监测系统的重要组成部分，通过文件安全传输模块对数据文件传送和接收的结果进行传递，完成大型数据库加密传输数据智能监测系统设计。

2　硬件设计

要改善传统系统数据丢失率高、数据损坏量大等问题，提出设计一种大型数据库加密传输数据智能监测系统。用户登录认证模块、密钥管理模块、混合加密模块和文件安全传输模块是构成改进系统硬件部分的 4 大主要模块。对这 4 个模块进行优化设计，为改进的智能监测系统创建良好硬件环境。各模块的具体描述如下：

2.1　用户登录认证模块设计

在大型数据库加密传输数据智能监测系统中，系统的安全性极为重要[10]。如果不对系统进行用户登录认证，那么会有非法的用户冒充系统用户的身份对系统进行非法访问，对系统中的信息进行盗取和修改等非法操作，对用户造成严重的损失，因此系统必须配备用户登录认证模块。用户对系统进行访问的方式分为三种，分别是强制访问控制、自主访问控制和基于角色访问控制。强制访问控制和自主访问控制的安全性较低，由于用户使用强制访问控制和自主访问控制时添加用户和功能操作的过程较为复杂，所以在大型数据库加密传输数据智能监测系统的用户登录认证模块中采用的是基于角色访问控制。基于角色访问控制中，在系统的访问许可权和用户之间引入角色的概念。角色指的是拥有责任和权限的一个特定职位。基于角色访问控制方式把对系统内资源的使用权赋给角色，使角色具有该权限。在整个系统访问控制过程分为了角色与用户关联和角色与访问权限相关联两个部分，实现了系统用户与访问权限之间的逻辑分离。大型数据库加密传输数据智能监测系统用户登陆认证模块如图 2 所示。

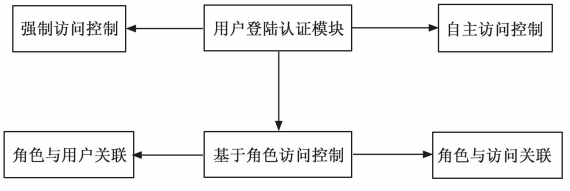

图 2　监测系统用户登录认证模块设计图

2.2　密钥管理模块设计

密钥管理模块的功能包括密钥的生成、保存、查修、分发和修改。其中最难操作的是密钥的保存和密钥的生成。密钥管理模块对系统的安全影响很大，并且影响着系统的有效性、经济型和可靠性[4-5]。大型数据库加密传输数据智能监测系统不能避免人事上、物理上和规程上的一些问题。密钥管理模块使用大型数据库加密传输数据智能监测系统数据库中的用户公钥表和用户密钥表对用户的密钥信息进行储存。用户密钥表包括私钥、公钥和会话密钥。用户的 ID 与大型数据库加密传输数据智能监测系统的用户表相关联，可以识别密钥信息属于哪个用户。公钥表是用来储存用户发布的公钥信息，用户可以在加密数据之前查询公钥表获取用户的公钥信息。大型数据库加密传输数据智能监测系统的密钥管理模块设计如图 3 所示。

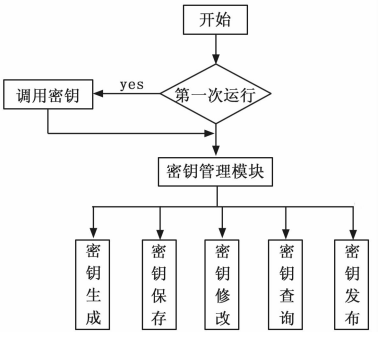

图 3　加密传输数据智能机制系统密钥管理模块设计图

第一次运行大型数据库加密传输数据智能监测系统时，系统将为用户创建一对密钥，作为与其他用户进行联系的开始。创建完密钥后系统将进入密钥管理模块。用户可以在系统管理、帮助、密钥管理、文件传输和混合加密的五项功能中进行选择。大型数据库加密传输数据智能监测系统在管理模块中具有退出系统和用户管理的功能，并提供了查看密钥的选项。

2.3　混合加密模块

使用大型数据库加密传输数据智能监测系统的混合加密模块生成会话密钥，并对大型数据库中的明文进行加密和解密，利用混合加密模块中的公钥对会话密钥进行加密，并将加密后的会话密钥保存到大型数据库加密传输数据智能监测系统的数据库中，与加密后的密文合并。将大型数据库中的加密数据传送到接收终端，接收终端通过生成私钥对密文进行解密。大型数据库加密传输数据智能监测系统的混合加密模块设计如图 4 所示。

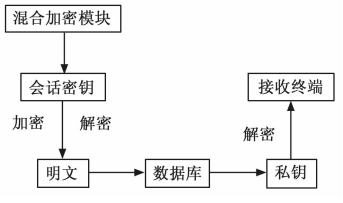

图 4　智能监测系统混合加密模块设计图

2.4　文件安全传输模块设计

文件安全传输模块是大型数据库加密传输数据智能监测系统的重要组成部分[7]。文件安全传输模块的功能由两部分构成。一部分是加密传输数据智能监测系统服务器端的应用程序，服务器端的应用程序始终处于监听的状态，主要用来接收数据库加密传输数据智能监测系统客户端的连接请求，接收大型数据库加密传输数据智能监测系统客户端的数据信息和各种加密文件，并向大型数据库加密传输数据智能监测系统客户端发送应答的信息和接收的结果等。另一部分是数据库加密传输数据智能监测系统客户端的应用程序，大型数据库加密传输数

据智能监测系统客户端应用程序主要的功能是申请连接服务器、向服务器提供传送加密文件和数据的各种要求、处理服务器的接收结果和信息等。大型数据库加密传输数据智能监测系统文件安全传输模块设计图如图 5 所示。

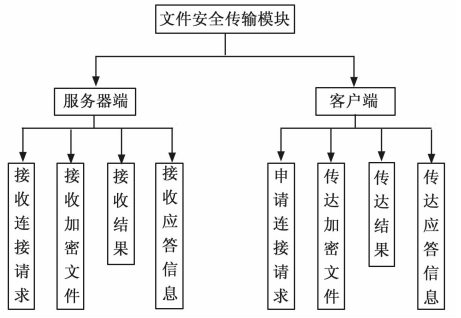

图 5 智能监测系统文件安全传输模块设计图

综上所述，完善各模块的功能设计方案，使各模块在完成其自身功能的基础上，高效配合，实现大型数据路加密传输数据智能监测系统硬件部分的设计。为改进系统的软件设计提供最优良的硬件环境。

3 软件设计

在大型数据库加密传输数据智能监测系统中，文件安全传输是加密传输数据监测系统的重要组成部分，可以保障需要传输的加密数据可在大型数据库和接收终端之间的安全传输，因此系统软件部分对数据传输加密过程进行深入分析。

数据加密标准（DES）是以 64bit 分组对大型数据库中的数据进行加密[11-12]，在 6bit 分组中存在 8bit 的奇偶校验，其有效的密钥长度为 56bit，DES 算法对大型数据库中的数据进行加密和解密时所用的算法是相同的，大型数据库加密传输数据智能监测系统的密钥保障了 DES 算法的安全性。DES 算法的具体过程是将 64bit 数据分成两部分 32bit 进行运算，用符号 ⊕ 进行表示，数据的加密过程如下。

将大型数据库中 64bit 明文进行初始的变化，记作 IP。在大型数据库中进行 16 次操作，分别用 $T1,T2,\cdots,T16$ 进行表示，每次进行操作时都分为两个部分，每个部分 32bit，用 (L_n,R_n) 进行表示。相邻两次操作的关系计算公式如下：

$$L_n = R_{n-1} \tag{1}$$

$$R_n = L_{n-1} \oplus F(R_{n-1},K_n) \tag{2}$$

式中，K_n 所表示的是 16 次操作中使用大型数据库中 16 个 48bit 长度的系统子密钥。每个子密钥都是不同的，都是由大型数据库中的 56bit 密钥转换产生的。

大型数据库中的数据将经过一个末变化处理 IP^{-1}。数据的初始变化和末变化之间属于逆变化，计算公式如下：

$$IP\ IP^{-1} = 1 \tag{3}$$

大型数据库加密传输数据智能监测系统中 DES 算法的加密公式如下：

$$E(m) = IP^{-1}(T_{16}(\cdots(T_2(T_1IP(m))))) \tag{4}$$

大型数据库加密传输数据智能监测系统中 DES 算法的解密公式如下：

$$D(c) = IP(T_1(T_2(\cdots(T_{16}IP^{-1}(c))))) \tag{5}$$

大型数据库加密传输数据智能监测系统中数据通过 DES 加解密算法完成数据的加解密，使大型数据库中的数据可以安全的传送到接收终端。通过上述完成了加密传输数据的智能监测系统软件设计部分。

根据以上步骤，完成了大型数据库加密传输数据智能监测系统的设计。

4 实验结果分析

4.1 实验环境及实验步骤

为了验证所设计的大型数据库加密传输数据智能监测系统的性能，本次实验选用 Xilinx 平台完成，主机为 windows 系统，连接口为 COM1，波特率为 19300Bd。以某公司的数据库加密传输数据智能监测平台为架构，启用频外加密，进一步保护数据库，对改进系统的性能进行测试。

实验过程主要分为以下 4 个步骤：

1）分别采用改进系统和传统系统进行数据丢失率测试。

2）分别采用改进系统和传统系统进行数据损坏程度测试。

3）分别采用改进系统和文献［8］系统、文献［9］系统进行监测精度测试。

4）分别采用改进系统和文献［10］系统进行数据传输信号测试，分析两种系统的监测强度。

4.2 实验结果

对所设计的大型数据库加密传输数据智能监测系统的数据丢失率进行测试，分别采用改进系统与传统系统监测加密数据的传输过程，测量并记录两种系统数据丢失率的实验结果，得到两种不同系统数据丢失率的对比结果如图 6 所示。

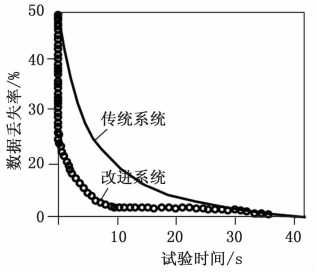

图 6 两种不同系统数据丢失率对比结果

由图 6 可知，对同一段数据传输过程分别采用传统系统和改进系统进行监测，在初始状态相同的情况下，传统系统的数据丢失率随实验时间的增加而下降，当实验时间为 20 s 时，出现下降拐点，此时数据丢失率为 10%。随后数据丢失率下降速度越来越缓慢，曲线波动很小。改进系统的数据丢失率也随实验时间的增加而下降，观察其数据丢失率曲线，当实验时间为 2 s 时便出现了下降拐点。改进系统数据丢失率达到 10% 的时间为 10 s，仅仅是传统系统的一半。对比两个系统的数据丢失率，明显看出改进系统数据丢失率较低，且达到数据丢失率为 0%的速度更快，实验结果表明，改进系统的加密传输数据智能监测系统监测效果更好，验证了改进系统的可行性。

为了验证所设计的大型数据库加密传输数据智能监测系统的性能，数据损坏程度也是造成数据传输不安全的一项重要干扰因素。分别采用改进系统和传统系统对传输过程中数据损坏信号进行测试，得出两种系统数据损坏信号对比结果如图 7 所示。

观察图 7 可知，传统系统对加密数据的传输过程进行监测，其数据损坏信号波谱十分紧密，且波段出现频繁，当时间为 22 s 时，出现最大数据损坏信号为 100 dB，说明该数据已完全被损坏，从整体信号曲线看出，传统系统的数据损坏程度

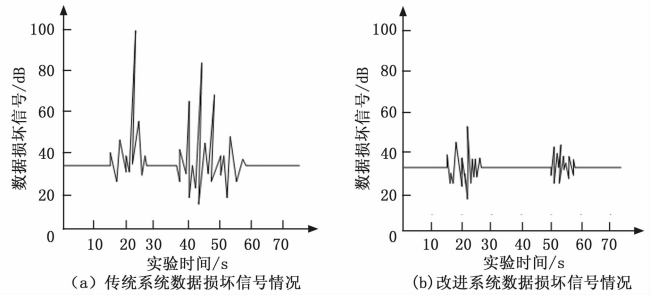

图 7　两种不同系统数据损坏信号对比结果

较大。改进系统的数据损坏信号波谱相对稀疏，且波段出现频率低，当时间为 25 s 时，出现最大数据损坏信号为 58 dB。对比两种系统的实验结果发现，改进系统的整体峰值较低，数据损坏信号段少且短，平均数据损坏信号值远远小于传统系统的品均数据损坏信号值，充分说明，改进系统的数据损坏程度低，数据损坏少，监测效果更好，验证了改进系统的实用性。

分别采用改进系统和文献［8］系统、文献［9］系统进行系统监测精度测试，测得三种不同系统的监测精度对比结果如图 8 所示。

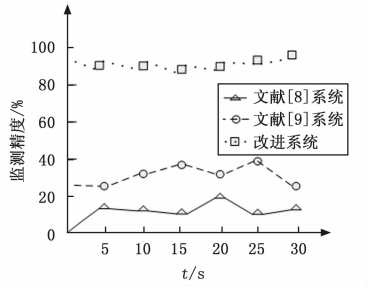

图 8　三种不同系统的监测精度对比结果

分析图 8 可知，采用文献［8］系统对大型数据库加密数据的传输过程进行监测，其监测精度平均值为 17%，当实验时间为 20s 时，监测精度达到最大值是 20%。采用文献［9］系统对大型数据库加密数据的传输过程进行监测，其监测精度平均值为 35%，当实验时间为 25s 时，监测精度达到最大值是 40%。对比文献［8］系统和文献［9］系统的实验结果，文献［9］系统的检测精度更高，监测效果相对更好。采用改进系统对大型数据库加密数据的传输过程进行监测，其监测精度接近达到 100%。且随实验时间的增加，监测精度保持稳定。对比改进系统和文献［8］系统、文献［9］系统的实验结果，改进系统的监测精度远远高于前两种系统的监测精度，结果充分说明改进系统的监测精度更高，监测效果更好。

分别采用改进系统和文献［10］系统进行数据传输信号测试，分析两种不同监测系统监测强度。得到两种不同监测系统数据传输信号对比结果如图 9 所示。

分析图 9 可知，文献［10］系统的数据传输信号波动较大，在时间为 18 s 时，出现坡峰，数据传输信号达到最大值 98 dB。在时间为 6 s 时，出现数据传输信号最小值为 15 dB。改进系统的数据传输信号波动较小，且随着时间的增加，数据传输信号变化十分平稳。数据传输信号值平均稳定在 40 dB 到 80 dB 之间。对比改进系统和文献［10］系统的实验结果可得，改进系统的数据传输信号变化稳定，说明改进系统具有极强的监测强度，充分说明改进系统可提高数据传输过程的安全

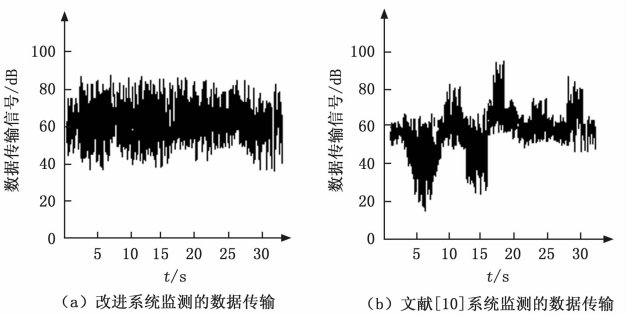

图 9　两种不同系统监测的数据传输信号对比结果

性，其监测效果更好。

综合以上实验，所得结果充分说明，所设计的大型数据库加密传输数据智能监测系统的数据丢失率低，数据损坏少，系统控制精度高，有效提高了数据传输过程的安全性，具有一定的实用性。

5　结论

针对传统的加密数据传输监测方法存在的一些问题，设计了一种大型数据库加密传输数据智能监测系统，该系统通过结合加密算法对数据进行加密，进而实现监测系统的硬件、软件设计，完成对加密数据传输过程的准确监测。通过对数据传输过程中各项干扰因素进行测试，得出改进系统具有数据丢失率低、数据损坏少，监测精度高等特点，在大型数据库数据加密方面，数据传输方面都有较好的实用性。但该系统在数据解密过程的安全性问题仍存在不足，针对该方向，将进行更深一步的研究。

参考文献：

[1] 张伯雍，何泾沙. 基于安全策略的动态加密技术研究［J］. 电子设计工程，2016，24（5）：19－21.

[2] 程志强，连鸿鹏. 物联网通信特征数据信息加密仿真研究［J］. 计算机仿真，2016，33（11）：324－327.

[3] 孙　媛. 大数据网络协作传输优化编码方法［J］. 科技通报，2017，33（3）：104－107.

[4] 余　容，黄　剑，何朝明. 基于 SM4 并行加密的智能电网监控与安全传输系统［J］. 电子技术应用，2016，42（11）：66－69.

[5] 何文才，田传凤，刘培鹤，等. 短距离加密无线数据传输系统的设计与实现［J］. 福州大学学报，2015，43（6）：767－771.

[6] 胡代弟. 远程实验数据传输中加密数据防丢失方法研究［J］. 科学技术与工程，2016，16（31）：61－65.

[7] 孟祥辉，曾学文，陈　晓，等. iSCSI 网络存储系统中加密方法研究与设计［J］. 计算机工程与科学，2016，38（12）：2456－2462.

[8] 司红伟，钟国韵. 基于双混沌系统的大数据环境并行加密算法设计［J］. 计算机测量与控制，2015，23（7）：2475－2477.

[9] 李吉广. IPTV 视频硬件加密传输系统的设计［J］. 电视技术，2016，40（5）：74－77.

[10] 周玉坤，冯　丹，夏　文，等. 面向数据去重的基于二次哈希的收敛加密策略［J］. 计算机工程与科学，2016，38（9）：1755－1762.

[11] 何书毅，吴春吉，龙致远，等. 区域电网光缆线路智能监测系统的数据传输技术研究［J］. 现代电子技术，2017，40（13）：118－121.

[12] 马李翠，黎妹红，杜　晔，等. 基于动态密钥的智能电网数据加密算法［J］. 北京邮电大学学报，2017，40（4）.