**重庆邮电大学本科生堂下考试答卷**

**2020-2021学年第 1学期**

**课程名称：计算机网络**

**姓 名：姜岙**

**年 级：2018**

**学 号：2018211406**

**专 业：计算机科学与技术**

**2020年12月6 日**

**网络传输层密钥数据库安全加密系统设计**

姜岙

（重庆邮电大学）

**摘 要：** 传统数据库安全加密系统对于存储信息的存储量较小、工作效率低。针对上述问题，设计一种新式 安全加密系统，分别设计了系统的硬件和软件两个部分。系统的硬件部分主要包括数据库加密模块、证书 块、数据库加密技术系统结构、密钥模块，各模块权责分明，共同致力于数据库的信息安全加密保护。软件 过数据库系统进行安全加密算法设计，有效隔离且明确密码系统各个模块之间的职责与任务，提供加密与 序，进而使数据库存储的信息更加安全可靠。与传统的数据库安全加密系统进行实验对比，结果表明，密钥 安全加密系统设计能够在短时间内存储更多的数据信息，保证存储的数据信息的安全性。

**关键词：** 传输层，安全加密设计，数据库；

**Design of network transport layer key database security encryption system**

**Jiang Ao**

*(*Chongqing University of Posts and Telecommunications*)*

**Abstract:** the traditional database security encryption system has small storage capacity and low efficiency. In view of the above problems, a new security encryption system is designed, including hardware and software. The hardware part of the system mainly includes database encryption module, certificate block, database encryption technology system structure and key module. Each module has clear rights and responsibilities, and is committed to the information security encryption protection of database. The software designs the security encryption algorithm through the database system, effectively isolates and clarifies the responsibilities and tasks of each module of the password system, provides encryption and order, and makes the information stored in the database more secure and reliable. Compared with the traditional database security encryption system, the results show that the key security encryption system can store more data information in a short time, and ensure the security of the stored data information.

**Key words:** transport layer;security encryption design; database;

**1 引言**

在数据库信息系统不断发展的当代，数据安全对人们的生活产生着重大的影响，数据库信息把握着企业甚 的机密要闻，对数据信息安全的加密措施成为了较为重要的任务 。传统的网络链路传输层密钥数据库安全 统运行工作时间长、运行效率低。

**2 安全加密系统硬件设计**

**2.1 数据库加密模块设计**

数据库加密模块负责创建加密字典模式，利用数据系统搜索访问引擎对已完成的数据进行加工处理，系统 密模式分析处理数据 。加密字典主要由专门人员进行管理，使用者可将此项权责交由管理员处理。数据库 块由用户登录模块、加密字典信息配置模块、加密定义信息修改模块、表检索模块、加密文表配置模块共同 ，如图1所示。

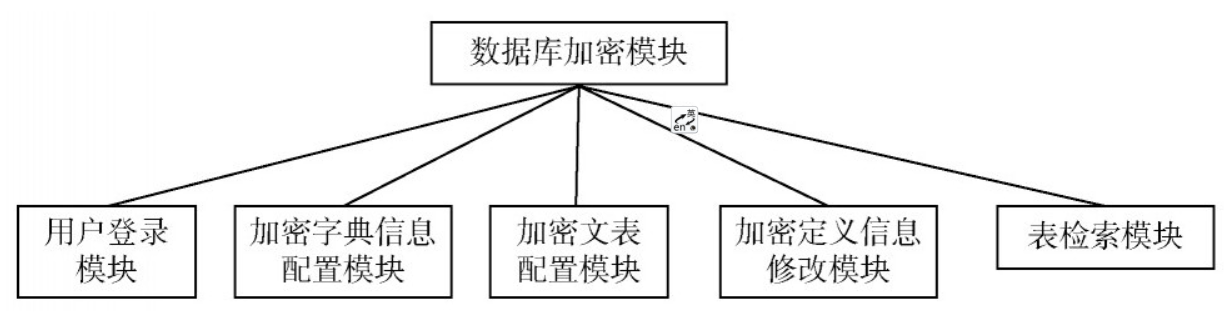


图1

用户登录模块主要由管理人员经由加密系统管理中进行必要的加密字典程序权限认证，对身份进行验证， 可以防止其他人员对加密字典的越权使用，进而提高加密字典的安全可靠性。身份验证均可通过对CA证书的 证进行处理分析，即系统专属管理人员通过处理验证，提交CA证书，进而确认使用者身份，经过用户登录模 证后的数据信息，若此方式操作成功，则可以继续访问，反之则不可继续访问。该模块担任着整个系统的先行 件 。加密字典的配置经由系统管理人员在数据库中创建加密字典，先通过初始系统信息处理，在不使用时 字典主要信息进行删除.

**2.2 证书管理模块设计**

证书管理模块是数据库加密系统中的核心部分。将身份认证模块作为本模块的主要入口，在权限控制的基 为整个数据库加密系统提供权限控制以及身份认证的方式，进而对数据信息进行安全加密处理 。 身份验证的主要流程是用户提供自己的服务器名称地址、用户名以及密钥的大体位置信息，接着向服务器 送登录信息的申请，服务器经过CA认证得到用户证书，进一步验证其有效性，在验证完成后，取出用户所放 钥，与此同时，生成的密钥经过进一步的加密程序后发送给使用者，使用者采取类似方法获取证书，进而获得 公钥，服务器根据自身私钥解密得到的数据获取密钥，如果与最初形成的密钥一致，则通过验证，反之则不 。证书管理模块如图2所示。

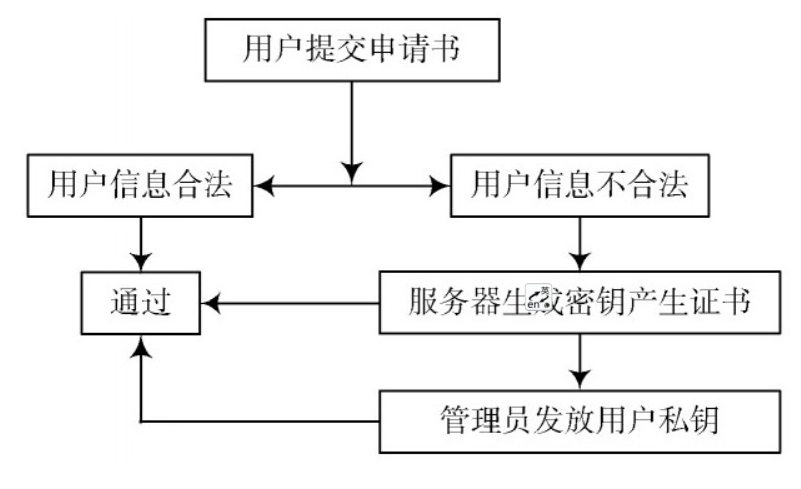


图2

**1.3 数据库加密模块设计**

数据库安全加密系统体系结构中，加密模块程序在数据运用搜索引擎与数据库的使用过程中占据着主要地 两个方面研究质量的优劣，影响着整个数据库安全加密系统的安全性以及实际应用系统中执行任务的速度 库安全加密系统中，数据加密引擎的整合、研发程序运用以及服务器运行系统，是数据库安全加密系统的核心 主要整合后台信息并且加工处理，其他专职管理人员无主要权利。数据库安全加密系统引擎主要存在于系 中，通过内存储系统接口与加密字典相互联系，主要信息运用程序共同操作完成，没有自身独立的操作程序系 运行操作的过程中，根据系统操作方法自行加载完成。

**2.安全加密系统软件设计**

一级密钥是系统主密钥，二级密钥主要为系统数据密钥，又称为工作密钥。数据库安全加密系统主要采取 钥系统处理措施。一级密钥通过专业方式对二级密钥进行分析解密处理，使其转换成工作密钥。一级密钥对工 进行保护处理，工作秘钥以此保护信息的脆弱程度。数据库安全加密系统依赖两种密钥，主要采用IDEA与对 算法对数据进行加密保护。对称加密算法的运算速度要远远高于普通共用的加密算法，对于高层次的数据信息 用，因此，该算法经常在高层次数据系统中使用。

绝大部分的数据库系统的加密处理是为了保护数据信息的安全机密性能，这也是对称算法的主要功能。D 法形式已经逐渐无法适用于当前的信息安全加密保护，而其完美程度与优越性可以很好地体现于对称算法之中 次数据库数据信息内容庞杂，系统的安全管理效率较低，所以DES的算法无法适用于高层次庞大数据库信息量 保护措施。因此，采取对称算法对数据信息进行加密，作为公开、公用的算法，自生成以来未发生过大的问题 法主要有流加密与块加密两种形式。流加密是对数据信息逐次加密，具有一定的层次性，而块加密是对固定比 进行整合加密。块加密所处理的数据按照处理要求划分为大小各异的差异块，进而采用对称加密算法对每一组 据进行深层次加密。因为所记录的数据要按照单位比例进行分析处理，为了更加有利于数据库系统操作，数据 密信息长度主要选择叠加字段的基本形式，每种字段记录的数据长度大体上是相同的，大体为16 bit。深层次 处理系统中主要针对更长的数据块进行分析加密，加密算法中的128 bit可以被认为是比较安全的数据分组长度。

**3 结论**

数据库安全系统的核心是数据库安全加密设计，与其他方法相比较，在安全信息、建造成本、修理与维护 合考虑，对数据库安全系统加密是最合适不过的数据安全保护手段，而且此方法的性价比较高，更有利于技术 研究。在费用投入方面，传统系统投资基本为短周期循环投资，本文方法适用于长远投入，对于信息的安全保久有效。在系统安全方面，大多数系统方法需要不断升级，本文方法可通过一种手段来应对系统的升级变化， 因系统升级而造成的数据损失或破坏，节省了与恶意攻击系统者的纠缠时间。数据库信息在加密的过程中可以息管理专职人员对于某些信息查询管理不明晰、无法查询问题原因等问题，并且根据我国近段时间的研究，数 全加密系统拥有着更加成熟的条件，可以很好地为使用者提供更加安全可靠的信息加密措施。 然而，本文方法在数据库系统对深层次系统信息文件进行加密的过程中，数据库安全系统中的某些保留功 受到一定的损失，并且该方法存在着一定的隐藏风险，需要对其进行进一步的风险评估与技术研究，进一步完理念设计，着手把握大数据发展趋势，使数据库安全加密系统设计具有更加广阔的市场前景。

**参考文献**

[1]米捷，刘道华.一种奇异值填充加密的大数据量化编码方法[J].河南工程学院学报（自然科学版），2018,19(11):75-80.

[2]刘叶，秦丽明，汪莎莎，等.ZigBee网络物理层安全传输方法设计[J].山西电子技术，2017,11(4):69-71.

[3]李兴志，金梁，钟州，等.基于物理层密钥的消息加密和认证机制[J].网络与信息安全学报，2018,4(8):31-38.

[4]李自清.基于网络的数据库敏感数据加密模型研究[J].计算机测量与控制，2017,25(5):184-187.

[5]马唯唯.移动互联网下信息采集安全加密研究[J].电子设计工程，2018,26(23):52-56.

[6]宋天煜，杨庚.面向密文数据库的中间件系统设计与实现[J].计算机应用，2018,38(12):3450-3454.

[7]杨扬，杨茂强，张子平.无线通信系统物理层安全传输方法综述[J].通信技术，2017,50(7):1351-1356.