 DOI: https://doi.org/10.12349/iser.v5i4.2422

# Design of Network Information Security System Based on Big Data Algorithm

**Zhuangzhuang Xu**

Taishan College of Science and Technology, Tai'an, Shandong, 271000, China

**Abstract**

In view of the huge loss caused by network information security, the following paper designs the corresponding network information security system based on big data algorithm, and introduces the software and hardware design of the system in detail. On this basis, the system is tested, the test results show that the system has good performance and high stability, which can provide some theoretical support for computer network information security protection.

**Keywords**

big data algorithm; network information; security system

# 基于大数据算法的网络信息安全系统设计

徐壮壮

泰山科技学院，中国·山东 泰安 271000

**摘　要**

针对网络信息安全引起的巨大损失，论文依据大数据算法设计相应的网络信息安全系统，详细介绍系统软、硬件设计情况。在此基础上，对系统展开测试，测试结果证实，所用系统性能较好、稳定性高，能够为计算机网络信息安全防护工作提供一定的理论支持。

**关键词**

大数据算法；网络信息；安全系统

## 1 引言

在互联网快速发展背景下，其广泛用在不同的领域。但针对各种数据信息安全方面的问题日益显现出来，如果网络信息泄露，会给个人或企业带来严重的问题。针对上述情况，越来越多的学者开展这方面的研究工作，如韦瀛寰研究中采用 RSA 及 CSC 算法对网络信息进行加密，研究结果证实，所用网络信息安全性较高，运行速度满足实际要求 [1]。有学者研究指出，设计网络信息安全系统旨在对网络传输内容实施监控，做好网络上流通数据监视工作，达到对可疑网络行为进行捕捉的要求，从而及时发现网络安全存储方面的问题 [2]。论文根据网络信息安全常见的问题，依托大数据算法设计相应的网络信息安全系统，为系统实现奠定相应的理论基础。

## 2 系统设计需求分析

随着计算机网络技术的快速发展，越来越多的人使用网络存储各类信息，网络安全问题受到更多的重视及关注。依托优化网络信息安全设计，有利于预防网络信息安全隐患，确保用户的信息安全。基于此，所设计系统要配置友好的界面，方便开展系统控制、管理工作，在网络环境中，能够准确捕捉需要监控的各种信息，若存在入侵检测行为进行响应，支持开展还原网络数据等一系列操作。详细需求如下：由于每个用户的身份有所不同，实际管理工作比较麻烦。基于此，必须建立全局的统一身份，从而更好完成用户信息管理工作，也支持整合统一网络下相关信息。由于不同类型信息比较混乱，要采用行之有效的解决对策，如通过管理系统各项数据，包含硬件、人员等。在此基础上，做好系统信息储存、传送等环节的保护工作，有利于提升所用信息安全性。如果遇到非法访问者，系统会将其阻挡在内部网之外，确保网络正常运行。必须注意，网络内部涉及大量的网络设备、服务器，确保这些设备稳定运行，成为企业对于网络最基本的安全需求。系统能够识别不同的攻击模式，借助 Internet 实施更新处理，有助于扩充检测库，尽可能防范入侵的非法行为。若出现可疑信息，可以精准显示相关数据的来源，发出针对性的报警提示；判断是否有入侵行为，及时调整各项安全措施，便于及时发出报警信息，经系统进行阻断或管理者手动阻断。系统保存全面的日志记录，包含管理者日志等不同类型，包

【作者简介】徐壮壮（2004–），男，中国山东齐河人，本科，从事电子信息工程研究。

含较大容量的日志数据库，能全面记录非法行为。

## 3 系统硬件设计

### 3.1 加密芯片设计

网络信息加密操作中采用加密芯片与公、私钥进行对接，并把获取的信息传送至加密终端，开展加密保存处理。该系统所选加密芯片为 Cyclone III。系统使用 Cyclone III 芯片时要保证其有空余，避免出现时序收敛问题，促使信息获得良好的加密效果 [3]。进行加密操作中，芯片展现出阶段性变化，结合主动串行（Active Serial，AS）等混合加密模式，全面记录不同模式下输出状况，设计 Passive serial 表格，保证各加密接口使用安全的连接方法。

### 3.2 接口电路设计

为便于对加密错漏问题予以修改，动态化开展随机加密操作，以同步动态随机存取内存（SDRAM）接口电路予以设计。该电路与加密芯片达到时钟同步要求，支持数据线级联，一次最多可以获得 32 位数据。此外，该电路使用门阵列芯片进行现场编程，满足数据连接转化各项要求，从而提高系统的自适应性。

### 3.3 存储器设计

网络信息经过加密处理后必须传送至相应储存空间，并通过存储空间传送到信息提取终端，上述操作配制性能、承载力好的存储设备进行支持 [4]。基于此，选取 C5402 数字信号处理设备作为系统的核心存储器，达到各种数据格式的要求。系统投入工作后，存储器可采用并读取设备的内部信息，把冗余信息传输至外部储存器，有利于降低系统所用存储成本。

## 4 软件设计

### 4.1 私钥选取流程

为高效率处理原始网络信息，采用私钥生成器当做相应的生成中心，可选用密钥管理系统对私钥进行处理。私钥与系统多个部分联系起来，见图 1。实现流程如下：建立原始的 PKG 管理中心，准确输入账号、密码后管理者进入系统，达到处理密钥相关信息的要求。设置密钥筛选指标后，工作人员开展初步筛选工作。此外，输入相应的筛选号码，并把生成与标准密钥对比，从而获得密钥准确输入终端，满足网络信息加密操作要求。

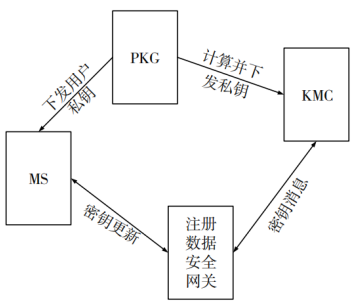


图 1 网络信息加密私钥连接效果

### 4.2 大数据下加密算法

基于大数据针对网络信息安全设计相应的加密算法。根据网络信息传输情况设置加密控制参数，其求解公式如下：

$$z=\frac{a}{3a+1} \tag{1}$$

α 表示经过加密节点的数量。这种情况下，不同加密节点处在初始状态，极易受到网络异常的影响。对已有加密异常节点数量 $n$ 进行求解，计算公式如下：

$$n=\frac{3a+1}{b} \tag{2}$$

上述式子中，$b$ 代表出现异常节点的控制参数，依据发生异常的加密节点数据，联合计算操作生成详细的加密指标 $b_i$，计算公式如下：

$$b_i=\omega(a_1+a_0)^2 \tag{3}$$

上述式子中，ω 表示经过加密处理的编码参数；$a_1$、$a_0$ 分别表示开展加密操作前、后的数据信息。根据上述环节，满足及时处理原始数据信息的要求。在此基础上，根据加密指标对各项信息展开处理，从而改善系统的性能。

### 4.3 入侵检测功能

数据检测是开展入侵检测不可缺少的内容，主要包含基于规则建立、规则检测，其中规则经文本实现，依据不同组完成分类，具有较好的可读性，且达到修改要求。规则集合作为经常遭受攻击的特征库，每一条规则均有相应的攻击标识，依托其准确识别出现的攻击行为 [5]。必须注意，规则库作为文论文件，当使用入侵检测功能时，读取全部的规则文件并实施解析处理，创建三维规则链表，大大提升匹配检测速度。入侵检测是系统一项重要的内容，可以准确提炼与之对应的入侵行为特征码，并将其归结到不同字段特征值，撰写出相对简单的检测规则，通过预处理数据包与规则库每一条规则匹配状况实施判断，判定是否存在入侵行为。如果确定是入侵行为，会调动事件响应功能予以处理。捕获和解析作为入侵检测模块的基础功能，其根据协议分层原理对数据包内的数据信息进行处理，将协议结果存储至相应的数据库内，为后续开展各项操作提供一定的支持。

### 4.4 数据包预处理

该功能旨在将数据包传送到数据检测前，提供与之对应的报警、丢弃数据包等操作框架。具体功能如下：对 TCP 协议进行重组处理，提供与之对应的会话信息，对一些协议传输过程中的特殊编码数据予以检查。

### 4.5 数据还原功能

该功能旨在对网络传输环节的数据包实施捕捉处理，支持数据包由下至上逐层展开，并把相应的协议内容实施处理，保存到相对应的变量内，顺利开展读取、还原处理，并把相应结果存储至数据库，便于管理人员查看、操作 [6]。

### 4.6 日志审计功能

日志审计作为系统安全结构中重要的组成部分，其包含文件访问、内存管理等内容 [7]。日志审计管理需要采用 syslog-ng 日志工具，其具有强大的功能，支持过滤信息、输出选择等，安全将信息传送至远端。

## 5 数据库设计

数据库主要功能在于保存相应的数据包及用户信息、日志等，方便系统管理人员及使用者开展查询、分析工作[8]。该系统选用 My SQL 数据库，其具有多线程、多用户等特点，能够迅速组织、管理大量的用户，支持采用不同语言查询各类数据操作。系统所用数据库创建相应的数据表，主要功能在于保存处理、分析等信息。其中，日志审计表涉及用户名、日志描述等内容，见表 1。

**表 1 日志审计表**

| 字段名 | 分类 | 默认值 | 说明 |
|---|---|---|---|
| host | Varchar（32） | NULL | 用户名称 |
| level | Varchar（10） | NULL | 危险等级 |
| msg | Text | | 日志内容描述 |
| tag | Varchar（10） | NULL | 标识 |
| seq | Int（10） | unsigned | 存储日志序号 |
| date | date | NULL | 存储日志日期 |

用户管理表主要涉及用户名、访问权限等信息，通过该表实现用户管理功能，详细信息见表 2。

**表 1 用户管理表**

| 字段名 | 类型 | 默认值 | 说明 |
|---|---|---|---|
| username | char（8） | | 用户名称 |
| Password | char（64） | NULL | 密码 |
| enable | char（1） | 0 | 普通和特权用户标识 |
| locked | char（1） | 0 | 该用户名是否可用 |
| Login_num | Int（11） | 0 | 已登录系统用户数量 |

## 6 系统性能测试

### 6.1 搭建测试平台

为验证此次设计系统的加密情况，配置相应的测试平台，并将其与文献[9,10]中的常规系统进行比较。系统开展初期测试时，要确定针对性的测试指标。由于网络负载与系统运行状况存在一定的关联，以网络负载率作为重要的测试指标，设计包括各种虚拟机组成的一体化测试平台。该平台配置 INTEL8 核处理器作为主处理器，内存设定为 16GB。测试平台通过层叠样式表进行编程，选取 PYUmbral 作为加密工具，对平台实施设置后，检测实验数据的吞吐情况，有利于降低实验误差。所用实验数据的吞吐关系如图 2 所示。

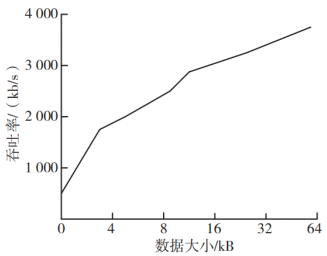


**图 2 实验数据吞吐关系**

通过分析可知，随着数据量日益增加，测试平台的吞吐率明显提高，满足系统测试的实际需求，支持后续开展相应的测试工作。

### 6.2 测试结果分析

顺利完成上述实验准备工作后，顺利进行下一环节测试，即分别使用论文设计的系统文献对各种数据展开加密操作，获取与之对应的网络负载情况，如表 3 所示。通过分析发现，文中所用系统进行加密后，不同数据量下系统负载率较低，即使数据量增加其未出现明显的改变；使用文献[9]系统实施加密，基于不同数据量下系统的负载率比较高，但由于数据量增加其波动比较大；采用文献[10]系统加密处理后不同数据量下负载率偏高，但变化波动最大。

**表 3 不同系统网络负载率对比分析**

| 数据 /kB | 文献[6]系统 | 文献[7]系统 | 论文系统 /% |
|---|---|---|---|
| 4 | 24.543 | 55.325 | 11.547 |
| 8 | 31.245 | 61.446 | 13.215 |
| 16 | 39.264 | 62.247 | 16.269 |
| 32 | 41.895 | 66.875 | 22.443 |
| 64 | 45.246 | 79.265 | 24.699 |

## 7 结论

常规网络信息安全系统由于自身的网络负载高，无法满足信息动态化实施加密操作的要求。论文根据大数据算法设计相应的网络信息安全系统，详细介绍系统各功能及数据库情况。分析系统测试结果可知，系统具有良好的性能及可靠性，满足对网络信息安全传输及存储的要求。

## 参考文献

[1] 张国萍.基于大数据的网络信息传输安全态势感知算法[J].电子设计工程,2022,30(12):185-188+193.

[2] 韦瀛寰.融合大数据算法的网络信息安全系统设计[J].电气自动化,2023,45(2):11-14.

[3] 唐博海.计算机网络信息安全防护使用大数据聚类算法的策略分析[J].通信电源技术,2021,38(18):155-157.

[4] 李旭晴.顾及大数据聚类算法的计算机网络信息安全防护策略[J].九江学院学报(自然科学版),2019,34(2):77-79.

[5] 郭畅.基于大数据聚类算法的计算机网络信息安全防护研究[J].现代信息科技,2022,6(7):141-143.

[6] 刘浚哲,刘伟.基于大数据的计算机网络信息安全防护与信息评估算法研究[J].网络安全和信息化,2023(8):136-138.

[7] 何海祝,乔世成.基于大数据的网络信息安全认证仿真研究[J].计算机仿真,2023,40(8):398-402.

[8] 陆斌彬.基于大数据的网络数据信息安全实时监测方法[J].数字通信世界,2023(1):40-42.

[9] 李波,赵瑞锋,卢建刚,等.基于聚类算法的电力大数据信息分析系统研究[J].自动化仪表,2023,44(8):84-90.

[10] 陈吉祥,刘永.计算机网络中隐私信息安全存储系统设计[J].信息记录材料,2023,24(1):132-134.