文章编号：2096-1472(2018)-04-33-03
DOI:10.19644/j.cnki.issn2096-1472.2018.04.009

# 基于网络安全技术的软件开发系统设计分析研究

李 根
(广东工商职业学院计算机应用技术系，广东 肇庆 526020)

**摘 要**：基于网络安全技术的软件开发系统设计，需要考虑网络安全性对软件功能的影响，充分利用大数据环境资源，提升软件程序使用功能稳定性是网络安全技术应用的主要方向。本研究主要论述了基于网络安全技术基础上的软件系统开发原理，包括开发环境中存在的病毒风险，并以SAT算法为例，整理出网络安全技术构建软件系统的主要功能设计方向，帮助提升网络安全技术在软件程序开发中的融合度。

**关键词**：大数据分析；网络安全技术；软件开发；系统设计
**中图分类号**：TP301 **文献标识码**：A

# Design and Analysis of the Software Development System Based on Network Security Technology

LI Gen
( *Department of Computer Application Technology,Guangdong College of Business and Technology,Zhaoqing* 526020,*China*)

**Abstract:**Design of the software development system based on network security technology shall take the effects of network security on software functions in account.The main direction of network security technology is to make full use of big data resources and improving the stability of the software program.This paper focuses on the principles in the development and design of traditional network security software,including the risks of virus in the developing environment. Through using SAT algorithm,the paper mainly discusses the design direction of the main functions of the software based on network security technology,helping improve the integration of network security in the process of software development.

**Keywords:**big data analysis;network security technology;software development;system design

## 1 引言(Introduction)

传统大数据环境下的软件程序构建，采用BSP计算模式进行框架设计，会首先对整体处理任务进行单元格划分将需要处理的数据库视为整体，在此基础上构建出以单元格为核心的数据库分散模块[1]。需要进行数据处理时会按照单元格的先后顺序来依次完成运算，虽然在精准程度上可以达到使用安全规定，但面对大量数据处理任务需要构建出数据库之间的相互作用体系，增大了大数据分析的任务[2]。在单元格之间的相互转换，以及运转中时间与速度都得到延长，采用BSP模型方法开展的大数据分析处理会在同步处理中，进行全局通信联系，将各个单元格之间建立起通信联系系统，这样在接收到处理任务时单元格内也会自动划分任务处理规定，划分出多核处理器。传统的大数据软件构成模式中，对于数据信息的处理已经能够实现多个单元格之间平行进行，将数据库整合形成大的数据信息处理层，但由于传统的BSP计算模式中并没有应用神经元网络系统，运算和框架构建中仍然会从各个单元格数据库中提取信息。需要较大存储功能的处理器才可以完成这一任务，BSP计算模式提出后大幅度增强了大数据处理环境下的软件系统构件稳定性，单元格划分的数据库模式也为软件运行中提供更稳定的参数基础。

## 2 BSP模式中存在的缺陷和隐患(Defects and hidden dangers in BSP mode)

BSP模式运行中，虽然会进行各个数据单元模块之间的相互转换联系，但由于所需要面对的数据库基础单元量比较大，大数据分析运算中仍然需要大量时间。数据库联系期间信息内容转换中，由于程序系统所处环境的存储功能有限，很容易因数据存储上限而造成有效信息丢失的问题。BSP模式中所开展的各项程序运算构建，通常会针对基础单元数据库进行安全审核，将可靠的数据库通过运算隔离层进入到总控制系统中，基于网络环境下进行数据资源获取，注意开展安全审核增大了网络平台下的资源消耗量，也需要说构建系统自身具有极强的稳定性，这样才能精准判断数据是否符合安

全标准。传统BSP技术应用中，很难从框架构建中达到这一标准，尤其是在程序系统运行使用中的控制模式，缺乏对人工智能技术的应用。导致单位时间内程序系统所需处理的数据量急剧增大，数据信息分布不均衡，并不利于更深刻的程序控制任务进行。BSP模式中存在的缺陷，导致处于大数据分析下网络安全难以得到保障，基于传统程序开发设计技术中存在的隐患。当前技术已经逐渐向智能化方向发展，解决了数据库分析运算中的层次划分问题，可以实现平行运算节省时间应提升安全程度[3]。

## 3 基于大数据分析网络安全技术的软件程序设计构想(Design conception of software program based on big data analysis network security technology)

### 3.1 SAT模型和逻辑分层处理

BSP模式中存在的风险和缺陷，经过完善处理后形成了SAT模型，在此模型构建中将总数据库划分为三个结构，三个数据库功能层之间会通过信息传输来建立起联系。从而确保运行中数据交互换，以及相互运行转换可以更高效实现，尤其是针对网络环境下所存在的有效信息丢失风险，逻辑结构中形成了严谨的安全检验体系，避免在运行中产生影响数据稳定性的黑客攻击。首先是根据数据接收请求划分的A层，表示数据处理中，需要更新完善的内容进行数据预分层，为接下来更详细的子系统构建创造条件。大数据建模基础如图1所示。

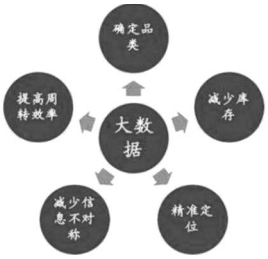


图1 大数据建模基础

Fig.1 Big data modeling foundation

其次是B层，表示数据分析处理中，所应对风险的规避能力，创建起数据库之间的相互结合，为基于大数据环境下开展的分析程序运行提供数据基础。最后是C层，也就是针对数据库所开展的各项转换和功能整合，根据以上两个逻辑层所提取，得到的数据参数进行网络环境中的大数据分析。从而判断接下来模型构建中可供利用的有效数据资源。通过详细的逻辑层划分也能对付具做出初步审核判断了解其中存在的隐患，在接下来的框架基础构件中重点针对隐患问题做出规避。

### 3.2 SAT大数据分析程序实现流程

(1)数据预处理

基于大数据分析下的网络安全技术应用在构建软件开发系统中，会利用SAT运算方法来建立起数据预处理功能层。数据系统运行使用中网络安全是需要重点研究的部分，由于数据库中包含大量数据信息，处于网络环境中数据库内涵盖的信息会实时更新，为避免网络环境中产生数据安全隐患，数据预处理中会对安全，以及所存在的缺陷做出初步判断[4]。接下来更为详细的数据分析任务进行也创造了基础条件，能够初步判断数据的属性，以及运行使用中所存在的参数误差问题，在进行详细数据处理中会针对误差隐患做出补偿。将数据信息控制在安全范围内，用于网络环境中的功能请求传达。数据处理流程如图2所示。


图2 大数据处理流程

Fig.2 Big data processing

模型建立初期需要确定数据资源库，对数据做出馄饨处理，将整体数据库做出拆分形成多个子系统。在针对子系统中涵盖的数据库做出详细特征提取。将归类一致的特征数据整合形成新的数据集合，大数据分析下的程序系统功能指令实现可以针对新形成的数据集合来开展。这样便避免数据信息传输中由于类型相近而造成的信道选择干扰。数据预处理属于软件开发中的初期程序，整体框架中也处于最低层，对这一部分功能进行开发时，要有明确的使用针对方向，结合环境特征提取来判断信息传输中可能会受到的干扰，以及数据丢失问题，在此基础上浆剂层框架与功能层之间建立起交换联系。运行使用中所存在的隐患，也能够通过数据之间的整合来有效避免，数据预处理与传统控制指令中，在功能层之间自身存在一定关联性，利用这一关联性SAT算法运行中可在更短时间内完成数据集合确定[5]。

(2)淘汰冗余程序

大数据分析下网络安全技术实现，需要删除大量的冗余程序，软件系统与网络平台相连接后，其内部程序也会自动向网络平台提出信息交换请求。这一过程中软件内的冗余程序也占据了大量的数据交换资源，由于这部分程序不常使用到，因此在软件系统运行中安全检测开展周期比较长。冗余程序中最容易产生网络病毒，单机状态下病毒并不会对其他程序造成攻击，但一旦与大数据网络平台相连接，冗余程序中所存在的病毒也会逐渐向其他有效程序蔓，最终造成计算机控制系统，整体瘫痪的严重问题。程序开发阶段可以预先构建出软件程序有效测评模块，对已经构建好的程序框架进行功能性测评，程序中会根据信息交换，以及所得到的参数结果来判断软件使用中是否存在冗余程序。程序构建中的逻辑层见图3。

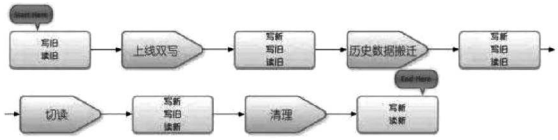


图3 冗余程序淘汰逻辑层

Fig.3 Logical layer of redundant program elimination

最终得到的结果形成数学分布模型，技术人员再根据模型中分布的各个点对应其所表示的出现次数，判断程序是否对于整体框架运行存在干扰。并结合测评结果与人工分析来将溶于部分软件删除，保障最终基于大数据网络安全技术中软件程序设计的有效性。构建程序测评体系，以及使用中的软件功能研制，是以功能为向导对网络环境的安全控制，在程序开发设计中信息资源安全隐患是难以规避的，其中也会存在大量的干扰信息。充分利用这一干扰信息构建出更长

期有效的控制体系，大数据分析处理中也能结合网络环境特征，建立起系统程序的内部安全防护。

(3)网络环境下数据包更新

程序开发系统设计中，充分利用大数据分析环境来对程序内部数据包做出更新，可以有效提升软件功能实现的先进性，能够与大数据分析一下网络平台发展方向保持一致，大数据分析环境下，程序构建需要一定的串码语言改变来确保程序先进行，优先利用网络资源来自动获取数据包更新，在程序系统开发中引入了学习功能。这样在程序运行中变不需要频繁更改内部程序，也确保硬件使用年限可以达到预期标准。程序系统构建中的数据包自动更新需要将源文件与系统中的文件相互联系，形成一个程序优先代码，这样程序在网络环境中运行使用也会针对这一代码来自动选择接下来的优化方向，对内部保存的数据资源做出更新。

程序设计后对于数据包自动获取更新的方向可以通过框架来进行约束，使之能够适应大数据网络环境。通过环境之间的程序相互整合来提升网络平台中的信息交换和传输能力，避免在交换传输中，由于部分有效信息丢失而造成整体程序指令功能错误。程序功能指令实现，还需要将数据包自动获取方向与大数据网络安全技术应用方向一致性构建。这样在使用中即使需要对部分程序进行优化也能在局部完成，不需要对整体框架做出改变，确保了程序系统在使用方面滴稳定性。

(4)程序运行初始化设计

程序设计完成后需要投入到仿真实验模拟中，程序系统设计初期的各项参数需要安全保存，形成初始化数据集合。在大数据分析下网络安全技术使用受环境因素干扰，可能会出现不同程度的误差，一旦程序软件中出现参数错乱，接下来的各项指令功能也将难以正常实现。构建出程序运行初始化参数集合后当程序使用中发生错乱，通过这种初始化恢复也能保障接下来的运行使用保持稳定。软件程序设计中的软件硬件集合见图4。

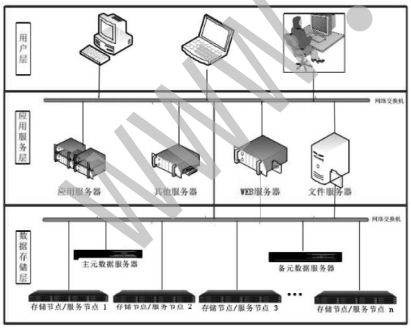


图4 软件程序设计中的软件与硬件集合

Fig.4 Software and hardware collections in software programming

程序初始化设计并不表示在软件恢复中需要将使用中的数据完全删除，而是将操作者设施所设计的参数恢复到初始状态中。通过这种恢复来删除操作中出现的错误数据，确保数据集合可以在预期有效安全范围内自动获取更新。初始化程序的设定，以及各项更新，程序设计人员要明确大数据网络环境中可供利用的资源范围，避免在资源使用中超出预期目标。系统集合方面可以参照最初构建的基础框架，初始化功能在安全框架基础上所开展的各项功能，也能保障安全不受影响，初始化恢复是对程序系统的一种自我修复与保护，可在程序内进行修护来提升对环境风险的抵御能力。这样基于大数据分析网络平台下所存在的各项安全隐患对程序做出攻击时，也能通过程序系统的内部强化来避免此类问题隐患进一步扩大。初始化功能能够对所分析的大数据文件进行恢复，节省大量信息筛选所用时间，并直接将系统运行中需要的信息引入其中。程序运行中初始化设计与整体框架构建可以结合起来，共同观察在系统设计中所存在的隐患。通过程序制定完善来帮助优化更有效的构建基础，在程序运行中基础防护，以及初始化功能均可以保证网络环境中数据更高效的获取，并在数据分析运算中避免隐患造成功能指令受阻。初始化具有清除和恢复功能，程序开发中设计多项控制功能，并将其规划到具体方案中，落实完善后才能达到更理想的程序使用效果，初始化过程中会自动恢复系统不需要的信息内容，以便节省处理空间，为所开展的各项设计任务建立一个适合的基础。检查过程也是一项筛选功能，判断所存在的问题，并加以优化解决。文件夹处理分析过程中程序内各个模块之间相互配合运行，共同参与完成信息检索任务。

## 4　结论(Conclusion)

互联网、物联网、云计算技术的快速发展，各类应用的层出不穷引发了数据规模的爆炸式增长，使数据渗透到了当今每一个行业和业务领域，成为重要的生产因素。为了应对不同的业务需求，以Google、Facebook、Linkedin、Microsoft等为代表的互联网企业近几年推出了各种大数据处理系统，深度学习、知识计算、可视化等大数据分析技术也得到迅速发展，已被广泛应用于不同的行业和领域。本文根据处理形式的不同，介绍了批量处理数据、流式处理数据、交互处理数据和图数据四种不同形式数据的突出特征和各自的典型应用场景，以及相应的代表性处理系统，并总结出引擎专用化、平台多样化、计算实时化是当前大数据处理系统的三大发展趋势。随后，对系统支撑下的深度学习、知识计算、社会计算与可视化四类大数据分析技术和应用进行了简要综述，总结了各种技术在大数据分析理解过程中的关键作用，即深度学习提高精度，知识计算挖掘深度，社会计算促进认知，强可视化辅助决策。

## 参考文献(References)

[1] 张森.大数据时代的计算机网络安全及防范措施探析[J].网络安全技术与应用,2018(1):55.

[2] 宁建创,杨明,梁业裕.基于大数据安全分析的网络安全技术发展趋势研究[J].网络空间安全,2017(12):21-24.

[3] 徐文涛,吴中超.基于scap网络安全大数据平台的研究与设计[J].网络安全技术与应用,2017(9):87-88.

[4] 杨玉新,马伟,赵阳.基于大数据分析的电网精准规划信息系统设计[J].现代电子技术,2017,40(7):155-158.

[5] 龚为纲,张严,蔡恒进.海外自媒体中涉华舆情传播机制的大数据分析——基于Reddit平台的海量舆情信息[J].学术论坛,2017,40(3):21-31.

## 作者简介：

李　根(1981-)，男，硕士，讲师.研究领域：大数据分析，网络安全.