文章编号:1671-4598(2017)08-0147-04 DOI:10.16526/j.cnki.11—4762/tp.2017.08.038 中图分类号:TP311 文献标识码:A

网络计算环境下大容量数据安全存储策略研究

徐 艳,王 茜
(电子科技大学成都学院 微电子技术系,成都 611731)

摘要:近年来,随着计算机技术的发展,网络环境下的数据运算能力愈来愈强;加之,大数据时代的来临将人们日常生活、工作、学习的物质化信息转化为数据化关联性链条,通过网络进行大数据资源共享,简化了工作学习的繁杂,提升了工作学习效率;但是,传统的网络储存策略常常出现数据泄露、储存服务器数据溢出等一系列储存安全问题;针对问题产生原因,提出网络计算环境下大容量数据安全存储策略研究方法;通过采用数据修正单元、逻辑补偿单元与节点加密单元,对传统网络储存策略进行动态化针对性解决;通过仿真实验证明,提出的网络计算环境下大容量数据安全存储策略研究方法,具有数据储存响应速度快、反渗透逻辑性强、数据安全级别高、易用性强的优点。

关键词:网络计算环境;数据安全;存储策略;数据溢出

Large Capacity Data Storage Strategy under Network Computing Environment

Xu Yan, Wang Qian
(Department of Microelectronics Technology, Chengdu College, University of Electronic Science and Technology, Chengdu 611731, China)

Abstract: In recent years, with the development of computer technology, data computing power under the network environment become more and more strong. In addition, the advent of the era of big data will turn people's daily life, work and study the materialization of information into digital correlation chain, big data through the network resource sharing, simplifies the learning multifarious work, improve the efficiency of work and study. However, the traditional network storage strategy often leaks of data overflow and a series of storage, storage server data security issues. In view of the problem, put forward under the network computing environment, large capacity data security storage strategy research methods. By adopting data correction unit, logic compensation unit and node encryption unit dynamic targeted to solve the traditional network storage strategy. Through the simulation experiments show that under the network computing environment of large capacity data storage strategy research method, a data storage response speed, reverse osmosis, strong logicality, the advantages of high data security, ease of use.

Keywords: network computing environment; safety data storage strategy; data overflow

0 引言

随着科技迅猛发展,海量数据也出现飞速发展态势,同时,海量数据存储也受到越来越严峻的挑战,其爆炸性的数据一直冲击着我们的生活,同时,各行各业对海量数据的安全性要求越来越高。作为一种新兴的技术理念,大容量数据存储技术不断改变着人们使用传统存储的使用方式和提供方式[1]。

全球存储行业技术产品的应用范围不断扩大,大容量数据存储技术逐渐成为全球存储行业的潮流,同时客户群不断细分,导致各行业用户对大容量数据出现千差万别的需求,可见,只有各行业用户采用弹性架构系统,才能满足存储系统的动态增长需求。然而,采用统一监控管理平台和分布式存储技术[2],同时通过结合大容量数据存储系统架构,能帮助各行业实现一种新模式,例如海量数据存储、备份等。

不同于传统的存储系统,本文针对多媒体应用的特性和大规模分布式数据处理而设计。元数据服务器包括名字空间、存储位置、文件系统中所有的元数据等组成[3-5]。存储服务器集群通过直接访问这些存储服务器节点完成数据存取,将要与之进行交互的存储服务器节点的信息,每当客户端访问系统时,能有效防止服务器元件负载过重,提高系统效率[6]。

但是,经过长阶段用户应用于数据反馈发现,在大数据计算下,传统大容量数据存储技术的部分数据存储机制策略存在协议点混乱的问题[7],导致数据存储安全机制遭到破坏,极易被不法分析利用渗透攻击程序[8]进行数据窃取。

针对上述问题,经过对传统大容量数据安全的存储策略的深入分析,找到导致传统大容量数据存储技术中存储数据在网络计算环境下,部分数据出现储存逻辑混乱的根源,并提出网络计算环境下大容量数据安全存储策略研究方法。采用数据修正单元对传统网络存储机制进行数据协议排列重组,从数据底层进行优化改进;通过逻辑补偿单元对数据外围安全机制进行升级,添加动态节点检测逻辑,实时监测机场节点数据动向;最后,采用节点加密单元对存储服务器中的数据进行交互协议加密,保护数据在访问交互过程中的安全。通过三位一体的数据存储策略改进,彻底解决传统大容量数据存储策略存在的一系列安全性问题,增强外侵数据是编入防御,彻底杜绝数据泄露。

收稿日期:2017-02-10; **修回日期**:2017-03-02。
基金项目:四川省教育厅科研项目(16ZB0443)。
作者简介:徐 艳(1979-),女,四川成都人,硕士,副教授,主要从事网络计算技术与应用方向的研究。

1 网络计算环境下大容量数据安全存储策略研究

1.1 数据修正单元

提出的网络计算环境下大容量数据安全存储策略研究方法中，数据修正单元设计的前提和设计目标主要包括以下几点[8-9]：

1.1.1 硬件容错

数据修正单元的数据支撑平台的服务器存储着修正单元的部分数据，数据支撑平台是由许许多多的服务器构成，因此，数据修正单元的数据支撑平台不能像 IOE 架构一样具有高成本。

这些数据支撑平台存储着修正单元部分的数据，包括许许多多服务器，假设条件硬件错误是常态而非异常，每个服务器上都存储着数据修正单元的部分数据。因此，我们面对的现实是构成系统的组件数目是巨大的，而且任何一个组件都有可能失效，这意味着随时有一部分硬件不能正常工作[10]。因此，硬件容错、保障数据部丢失、错误检测和快速、自动的恢复是分布式存储最核心的架构目标。

1.1.2 数据访问要求

数据修正单元设计的主要目的是保证网络计算环境下海量储存数据的安全，也就是说在其上能够存储很大量文件（可以存储 TB 级的文件）。数据修正单元将这些文件分割之后，存储在不同的 DataNode 上，具体每个 Block 放在哪台 DataNode 上面，对于开发者来说是透明的。

数据修正单元的设计中，由于解决了数据访问的低延迟问题，同时处理了批量数据，而非解决了用户交互处理问题，因此，解决了数据访问节点的逻辑混论问题。

1.1.3 大规模数据集

数据修正单元上的一个典型数据修正逻辑一般都在 G 字节至 T 字节。在数据修正单元上的数据点具有很大的数据集。因此，数据修正单元被调节以支持大数据下节点逻辑的错误纠正。在高的数据传输带宽的网络运算中，保证扩散数据点的安全性与访问权限。一个单一的数据修正单元能支撑数以千万计的节点交互逻辑纠正。

1.1.4 简单的一致性假设模型

到容量数据储存安全索引文件需要一个“一次写入多次读取”的文件访问安全性模型。一个文件经过创建、写入和关闭之后就不需要改变[11-12]。这一假设简化了数据一致性问题，并且使安全访问节点的数据访问成为可能。

因此，对提出的网络计算环境下大容量数据安全存储策略研究方法中，数据修正单元采用 master/slave 架构。一个数据修正单元是由一个 Namenode 和一定数目的 Datanodes 组成。

Namenode 是一个中心服务器，负责动态管理文件系统的名字空间（namespace）节点数据以及客户端对文件的访问逻辑。集群中的 Datanode 一般是一个节点一个，负责管理它所在节点上的存储安全逻辑。

数据修正单元以文件形式对存储数据进行逻辑纠正，能检测出暴露文件系统名字的空间数据后，把这些块存储在一组 Datanode 上，把一个文件被分成一个或多个数据块，Namenode 负责确定数据块到具体 Datanode 节点的映射，比如关闭、目录、重命名文件或打开等。同时，Datanode 也可以在统一调度的情况下进行读写安全性扫描请求，动态纠正错误逻辑数据块。数据修正单元架构图如图 1 所示。

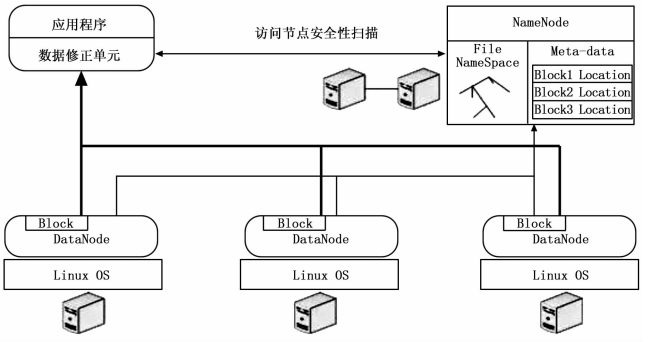

图 1 数据修正单元架构

对提出的网络计算环境下大容量数据安全存储策略研究方法中，数据修正单元进行仿真性能测试。分别对数据修正单元的数据访问点扫描响应时间、运算处理时间、逻辑纠正准确度、稳定性等项目进行测试，并与传统大容量储存安全机制数据进行对比，具体仿真测试参数如表 1 所示。

表 1 数据修正单元性能测试参数

测试项目	传统大容量储存安全机制	数据修正单元
数据访问点扫描响应时间	1.43s	400ms
运算处理时间	21.3s	650ms
逻辑纠正准确度	无此功能	100%
稳定性	差	良好

通过上述测试数据证明，数据纠正单元具有动态数据安全性逻辑纠正功能。并且，具有数据访问点扫描响应时间快、运算处理时间段、逻辑纠正准确度高的优点。从问题根源提升了大容量存储安全策略的逻辑严谨性。

1.2 逻辑补偿单元

传统的大容量存储空间中采用的安全逻辑属于单一静态化安全逻辑，此逻辑具有高度执行性与执行响应速度快的特点。但是，如表 2 所示，当数据的安全逻辑链的部分逻辑出现错误时，逻辑整体就会出现运存错误与误判，造成不必要的损失。传统方式下，此种问题需要程序开发人员与维护人员一同进行错输逻辑数据的修正与维护升级，消耗人力资源巨大。

表 2 传统数据储存安全逻辑参数

项 目	运行参数	消耗资源量
安全节点处理逻辑调用时间	1s	核心处理资源 61.2%
逻辑运算连通性	一般	13.4%
升级维护	人工	3－10 人
逻辑稳定性	差	

通过表 2 可以发现，传统数据存储安全逻辑机制存在严重的稳定性问题，其无法进行自我升级修复。为此，提出的网络计算环境下大容量数据安全存储策略研究方法中，采用逻辑补偿单元进行逻辑错误修正与逻辑自主修复功能提升。从内外逻辑入手，彻底解决传统数据存储安全逻辑策略存在的问题。

逻辑补偿单元分为底层逻辑补偿和数据外逻辑补偿两部分。底层逻辑补偿是指在存储空间架构内部利用 SGV 构建的

存储架构子逻辑进行逻辑调整补偿的方法。数据外逻辑补偿是指通过访问节点数据的端口外部的访问逻辑或设备感知电频信号传导特性然后进行信号电位补偿的方法。底层逻辑补偿的架构模式和处理运算都较复杂，且逻辑补偿效果仅限于 VBD 阈值数据和 DVE Gvd，逻辑补偿范围偏小，在提出的网络计算环境下大容量数据安全存储策略研究方法中，将逻辑补偿单元中底层逻辑补偿作为内部低层数据逻辑的第一补偿处理方式也足以满足需求。而数据外逻辑补偿具有架构组成简单，响应速度快和补偿范围大的优点，但缺点是外围数据逻辑补偿资源消耗偏高，在网络计算环境下的大容量存储安全策略应用中，数据外逻辑补偿是较佳的补偿方案。

数据外逻辑补偿运行机制采用网络数据交互过程中产生的电信数据信号差进行错误阈值的识别，从而进行外部节点错误逻辑的补偿，即通过底层逻辑补偿的 VBD 阈值通过底层数据回传至数据教交互端口，由逻辑代码激活数据外逻辑补偿，计算需要补偿的节点逻辑字节与外部数据访问关联节点状态是否相符。当发现外部访问节点数据相符时，进行逻辑开放，对访问节点放行；若外部访问节点数据出现不符，数据外逻辑补偿自动进行差别节点的逻辑修正，并进行逻辑性防御保护，避免恶意数据对存储空间的数据进行破坏或读取。数据外逻辑补偿需要内部数据信号提取 IC 硬件的支持。

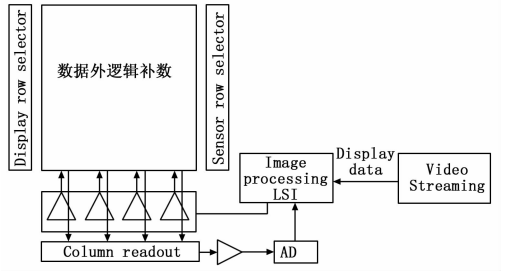

图 2　数据外逻辑补偿原理

图中 Column readout 作用是监测动态监测外部访问节点的逻辑安全性，检测内部数据安全机制标准回馈；Image processing LSI 作用是根据监测结果计算补偿量，并将补偿量和初始数据整合输出给 Data Driver。

检测出节点异常逻辑后，数据外逻辑补偿借动态根据节点错误逻辑运算量决定是否调用内部额信心处理器，进行大数据量的逻辑补偿处理，对网络计算下的大容量数据外节点错误安全逻辑实施补偿。数据外逻辑补偿的技术难点在于实现高精度和高速的外节点异常量参数读取，网络数据交互信道上的寄生效应会影响读取速度并造成信号衰减，交互数据节点逻辑量的误差会造成输出滞后，相邻信道频段或外界环境的干扰波会干扰交互节点逻辑识别的准确性。

逻辑补偿单元中底层逻辑补偿和数据外逻辑补偿运算关系式如下所示：

$$latt = (cv)^{\wedge} \frac{f\sum(T-1)\iint_{t} shife}{\iiint(f/T)^{\alpha}} \tag{1}$$

$$latte = (dv)^{\infty\sqrt{T}} \overset{(t-1)}{\underset{\Leftrightarrow}{f}} \left(\iiint \frac{1}{did(t)} \mid T \mid \right)^{\sum_{n^{\alpha}}} \tag{2}$$

对提出的网络计算环境下大容量数据安全存储策略研究方法中，逻辑补偿单元进行仿真性能测试。将传统数据存储安全逻辑测试数据作为测试本例，将测试本例用数据逻辑补偿单元进行优化处理后测试。测试数据与测试本例数据进行对比，具体测试参数如表 3 所示。

由表 3 数据对比可以证明，提出的网络计算环境下大容量数据安全存储策略研究方法中，逻辑补偿单元具有较强的储存安全逻辑修正能力，同时添加了逻辑自我修复能力，节省了后期维护的人力资源消耗。从根源彻底解决传统数据存储策略在网络计算下存在的逻辑缺失、错误等一系列问题。

表 3　逻辑补偿单元性能测试参数

测试项目	测试本例数据	逻辑补偿单元
逻辑语句连贯性	一般	良好
安全逻辑链完整度	96.7%	100%
逻辑语句衍生性	无	良好
逻辑执行率	93.6%	100%
瞬态逻辑检索量	5000 万字串	150000 万字串
逻辑自我修复性	无	较好
海量处理下逻辑稳定性	差	较好

1.3　节点加密单元

1.3.1　网络数据加密现状

当前，网络安全环境日益恶化，如何确保大容量数据存储的数据安全，防范遭受攻击而导致信息泄露，正成为众多政企部门纷纷关注的重点。在各种安全防护技术手段中，加密技术不仅是不可或缺的防护关键手段，而且还成为阻止网络存储空间数据“裸奔”的最后一道防线。

虽然过去 10 年间，使用加密技术的网络存储空间数量正不断增加，不过需要注意的是，目前仍有 39% 的网络存储空间以明文方式存储数据。正如上周某电商平台曝出有千万条账户泄漏，除了密码经过了 MD5 加密外，其他如用户名、真实姓名、邮箱地址、QQ 号、电话号码、身份证等数据均采用明文形式存储。在此种情况下，一旦该企业数据遭受“撞库”，攻击者便能够轻松掌握到用户的大量相关信息，并前往其他网站撞库。

反之，如果将存储空间中的海量数据都进行加密处理，即便攻击者获得了也需要耗费大量时间精力进行 2 次破解才能获得数据，而且能够有效降低后续的关联性攻击，无形中就会为数据防护构建起一道新的安全防线。

根据调查发现，现在不论个人还是企业都开始逐步意识到这一点，并开始使用加密技术提升数据信息的安全性，因此加密性能的强弱也变成了很受关注的问题。对于网络大容量存储空间而言，当提及加密技术时，首先是关注其加密性能如何，其次才会是能否支持网络存储空间内部部署或者云部署等问题。

有统计显示，在 2005 年只有 16% 的企业广泛使用加密技术。而经过 10 年发展，这一比例于去年逐渐增至 34%，2016 年已跃增至 41%。那么哪些行业最为关注加密技术呢？首当其冲的便是金融行业，56% 的金融公司广泛使用加密技术。其次，是医疗和制药行业，制造业则远远落后，使用加密技术的网络存储空间仅占 25%。在涉及特定应用时，数据库使用加密技术的比例最高，其次为互联网通讯、笔记本电脑硬盘驱动器以及备份系统。

1.3.2 节点加密单元设计

通过上述的数据介绍，充分证明数据加密对大容量网络存储空间的安全性具有决定性作用。针对现有网络大容量存储安全策略在网络计算环境下出现的数据防护部署性差、中途数据截取防护缺失的问题，在提出的网络计算环境下大容量数据安全存储策略研究方法中设置节点加密单元，进行数据存储全节点化加密保护，同时对数据交互过程中的动态节点进行实时传输加密运算，实现对数据安全的全方位防护。

节点加密单元采用 NIE－cas 节点双向加密算法，算法底层架构引用 RAS 加密技术运算逻辑，添加节点通讯协议规则，通过对存储数据外围访问数据节点交互过程中产生数据感应脉冲进行数据内核特征的判定。通过对正常数据几点外空间核进行绑定化密文处理，是数据处于实时保护的密闭特定数据域中，解密数据由算法根据逻辑补偿单元回馈信号进行认证式绑定释放。NIE－cas 节点双向加密算法分为三段式构成，分别是上传节点加密式、下载数据加密式、外链访问加密式。具体关系式如下所示：

$$C=(x)^{\varphi}\to\frac{f}{\dfrac{x(m-1)_{\max d}}{\sum_{m}f\Rightarrow x_{\min}}} \tag{3}$$

式中，x 为上传节点总量，f 为节点安全逻辑值，m 为节点数据密钥绑定系数。

$$\vec{C}=g\left(neafit/\frac{\sum(1-g)^{\infty}}{\vec{x}}\right)\iint\max \tag{4}$$

式中，g 为下载数据安全逻辑关系量，$\vec{x}$ 为密钥处理反馈系数。

$$C(\rho)=\sum_{\Leftrightarrow}\left(\frac{\int D\left(v^{n}\to\overset{v_1}{\underset{v_2}{\sum}}\max d\right)}{\oint(D^{\infty})\Rightarrow v}\right) \tag{5}$$

式中，D 为存储数据节点集合，v 为外链机密阈值系数。

为了确保提出的网络计算环境下大容量数据安全存储策略研究方法中，节点加密单元运行稳定且具有良好数据加密作用。故对节点加密单元进行安全性能仿真测试，测试对节点加密单元进行 10 组不同程度的攻击与破解，测试时间为 10 小时，对比最终测试结果。具体参数如下所示。

表 4 节点加密单元性能仿真测试

攻击程度	传统数据存储安全策略	节点加密单元数据状态
1 级	良好	良好
2 级	良好	良好
3 级	良好	良好
4 级	良好	良好
5 级	良好	良好
6 级	安全机制被攻破	良好
7 级	数据异常	良好
8 级	数据溢出	良好
9 级	数据暴露 16.7%	良好
10 级	服务器崩溃	良好

通过上述表 4 数据证明，节点加密单元具有良好的数据防护作用，能够对多种程度的数据攻击、窃取操作进行有效的防护。从策略底层解决了传统大容量数据存储安全策略在网络计算环境下的安全防护部分缺失以及防护策略薄弱的问题。

2 实验与结论

对提出的网络计算环境下大容量数据安全存储策略研究方法进行整体可行性、性能与稳定性仿真测试。测试采用连续性对比测试方式。测试平台为，Windows sever2016 内存 64 G 硬盘 300 TG；测试时间为 72 小时，对测试结果与传统网络存储安全策略数据进行对比，具体参数如下所示。通过对节点处理响应时间、安全逻辑整体响应、整体响应时间、逻辑链运行连贯性、逻辑链最大资源占有率、安全防护最大级别、网络运算下安全处理时间、全程资源平均开销、多级数据攻击防护性、整体性能平稳度、后期升级维护方式等几项指标的测试，比较传统的数据存储安全策略与网络计算环境下大容量数据安全存储策略研究方法。

表 5 网络计算环境下大容量数据安全存储策略研究方法仿真测试

测试项目	传统数据存储安全策略	网络计算环境下大容量数据安全存储策略研究方法
节点处理响应时间	1.43s	400ms
安全逻辑整体响应时间	2.61s	1s
逻辑链运行连贯性	差	较好
逻辑链最大资源占有率	53.4%	8.7%
安全防护最大级别	5 级	12 级
网络运算下安全处理时间	21.3s	1.4s
全程资源平均开销	57.4%	18.3%
多级数据攻击防护性	差	较好
整体性能平稳度	差	较好
后期升级维护方式	人工	自主

通过仿真测试数据表 5 可以充分证明，提出的网络计算环境下大容量数据安全存储策略方法对解决传统大容量存储安全策略在网络运算环境下存在的问题具有良好的作用。其中，针对传统大容量存储安全策略存在的数据泄露、储存服务器数据溢出等储存安全问题具有数据储存响应速度快、反渗透逻辑性强、数据安全级别高、易用性强的优点。

3 结束语

针对现今传统大容量存储安全策略存在的问题进行深入分析，并结合现状针对性提出络计算环境下大容量数据安全存储策略研究方法。通过采用数据修正单元、逻辑补偿单元与节点加密单元对传统网络储存策略进行动态化针对性解决。通过仿真实验证明，提出的网络计算环境下大容量数据安全存储策略研究方法，具有数据储存响应速度快、反渗透逻辑性强、数据安全级别高、易用性强的优点，为日后网络计算下大容量存储安全策略研究与发展提供了新的思路。

参考文献：

[1] 钟 莲. 云计算环境下数据安全策略研究 [J]. 智富时代，2015，4 (12)：25－60.

[2] 叶礼斌，张 政. 云计算环境下数据安全策略研究 [J]. 信息与电脑：理论版，2016，12 (2)：213－214.

[3] 兰青青，周 萍，陈 坚. 云计算环境下的信息资源安全存储策略研究 [J]. 大科技，2015，6 (28)：256－263.

[4] 程代娣. 基于云存储技术的数据安全策略研究 [J]. 齐鲁工业大学学报，2015，29 (4)：62－65.

(下转第 158 页)

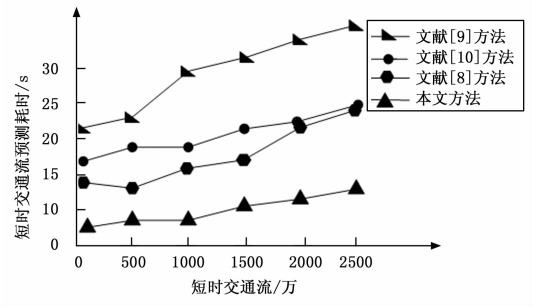

图 1 不同方法下短时交通流预测耗时对比

文所提方法进行短时交通流预测时，采用高斯过程回归法，并利用样本自相关函数法对选取的短时交通流数据进行详细分析，此操作减少短时交通流预测所用时间，提高预测效率，进一步证明本文所提方法的可扩展性。图 2 是不同方法下短时交通流数据聚类时间（s）对比。

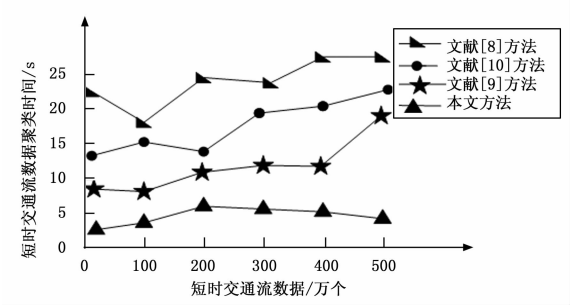

图 2 不同方法下短时交通流数据聚类时间对比

分析图 2 可知，文献［8］和文献［10］所提方法的短时交通流数据聚类时间，比本文方法的交通流聚类时间要多，文献［9］所提方法的聚类时间曲线波动虽然不大，但上升趋势很明显，与之相比的本文所提方法，在短时交通流数据为 200 万之前，聚类时间曲线略有上升趋势，但在 200 万之后得到了缓冲，聚类时间又有所减少，说明本文所提方法的数据聚类速度很快，为交通流的预测节省时间。图 3 是不同方法下短时交通流预测准确率（%）的对比。

通过图 3 可知，文献［8］所提方法在短时交通流预测准确率方面优于文献［9］和文献［10］所提方法，但是与本文所提方法做对比，预测准确率有一定的差距。本文所提方法相应的预测准确率较高，是因为利用对短时交通流的特征提取、交通流数据聚类等过程完成短时交通流预测。预测准确率变化曲线说明本文所提方法的适用性和实用性都很强，可以广泛地应用于短时交通流预测中。

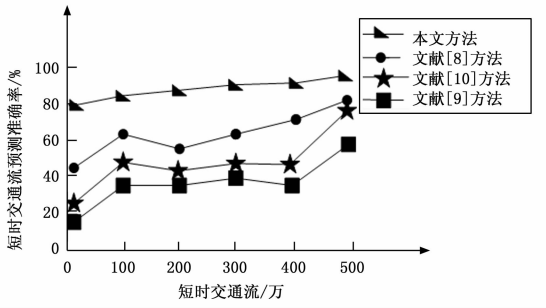

图 3 不同方法下短时交通流预测准确率对比

仿真实验证明，本文所提方法可以准确地对短时交通流进行预测，具有较好的稳定性和灵活性。

3 结束语

采用当前方法对短时交通流进行预测时，无法安全准确地对其进行预测，存在短时交通流预测偏差大的问题。提出一种基于模糊神经网络的短时交通流预测方法。并通过仿真实验证明，所提方法可以准确地对短时交通流进行预测，为该领域的钻研提供支撑和依据。

参考文献：

[1] 周 桐，杨智勇，孙棣华，等. 分车型的高速公路短时交通流量预测方法研究［J］. 计算机应用研究，2015，32（7）：1996－1999.

[2] 梁 轲，谭建军，李英远. 一种基于 MapReduce 的短时交通流预测方法［J］. 计算机工程，2015，41（1）：174－179.

[3] 康 军，段宗涛，唐 蕾，等. 高斯过程回归短时交通流预测方法［J］. 交通运输系统工程与信息，2015，15（4）：51－56.

[4] 张洪宾，孙小端，贺玉龙. 短时交通流复杂动力学特性分析及预测［J］. 物理学报，2014，63（4）：51－58.

[5] 杨春霞，符义琴，鲍铁男，等. 基于相似性的短时交通流预测［J］. 公路交通科技，2015，32（10）：124－128.

[6] 谭国平，刘如通，谭林风. 基于车辆合作的拥塞检测机制研究［J］. 电子设计工程，2016，24（21）：118－121.

[7] 袁 磊，梁丁文，蔡之华，等. 基于正交差分演化无迹卡尔曼滤波的短时交通流量预测方法［J］. 计算机应用，2015，35（11）：3151－3156.

[8] 黄 杰，李 军，郭 翔. 递推 SOM 神经网络在短时交通流预测中的应用［J］. 公路，2015，36（4）：1－5.

[9] 徐健锋，汤 涛，严军峰，等. 基于多机器学习竞争策略的短时交通流预测［J］. 交通运输系统工程与信息，2016，16（4）：185－190.

[10] 罗向龙，焦琴琴，牛力瑶，等. 基于深度学习的短时交通流预测［J］. 计算机应用研究，2017，34（1）：91－93.

（上接第 150 页）

[5] 杨 凯，辜季艳. 云计算环境下数据存储安全的关键技术研究［J］. 无线互联科技，2016，6（16）：103－104.

[6] 李 谦，李 蓓. 计算机网络环境下信息安全保护策略研究［J］. 信息与电脑，2015，10（18）：156－163.

[7] 李 健. 云计算环境下的信息安全问题及对策研究［J］. 科技展望，2016，26（29）：112－120.

[8] 贾花萍，孙卫喜. 网络可靠性预测模型［J］. 电子设计工程，2016，24（21）：21－23.

[9] 何 青，吴 征，苏淑靖. 基于 LabWindows 的大容量数据分析处理方法［J］. 计算机测量与控制，2014，22（11）：256－263.

[10] 马其琪，鲍爱达. 基于 DDR3 SDRAM 的高速大容量数据缓存设计［J］. 计算机测量与控制，2015，23（9）：3112－3113.

[11] 刘 珏，王 永. 网络疑似入侵环境下的最优接口访问控制模型仿真［J］. 计算机测量与控制，2016，24（11）：182－184.

[12] 何晓冬. 强干扰环境下网络情报数据滤波通信系统设计［J］. 计算机测量与控制，2016，24（10）：162－164.