文章编号:1671-4598(2024)08-0108-07 DOI:10.16526/j.cnki.11-4762/tp.2024.08.016 中图分类号:TP391 文献标识码:A

基于区块链技术的网络通信数据泄露自动检测系统设计

秦 浩,薛 伟,郭 振,陈 今
(安徽继远软件有限公司,合肥 230031)

摘要:网络安全环境不断变化,容易出现新的攻击技术和漏洞,而面对网络通信产生巨大的数据流量,会影响网络通信数据泄露自动检测的效果,故提出基于区块链技术的网络通信数据泄露自动检测系统设计研究;系统硬件部分基于区块链技术搭建网络通信数据存储结构,为网络通信提供更安全、可信和高效的数据存储方式,同时根据设计系统硬件需求设计网络通信数据流检测装置与污点分析器,实时监测并分析网络通信数据的流动,识别潜在的污染流,为后续的数据泄露检测提供了基础;系统软件部分利用污点分析法详细描述了网络通信数据泄露问题,通过追踪和标记数据流中的敏感信息,能够发现潜在的数据泄露路径;获取并验证潜在污染流,以此为依据,结合设计系统硬件检测数据,制定网络通信数据泄露自动检测程序,实现网络通信数据泄露的自动检测;实验数据显示:设计系统的网络通信数据泄露检测准确性为95%,数据泄露检测时延最小值为7.20 ms,3种对比方法的检测准确性分别为66、80、81%,检测时延最小值分别为15.4 ms、15.62~25.79 ms、12.56 ms;充分证实了设计系统应用性能更佳。

关键词:网络环境;泄露检测;通信数据;访问监控;区块链技术;数据泄露

Design of Data Leakage Automatic Detection System for Network Communication Based on the Blockchain Technology

QIN Hao, XUE Wei, GUO Zhen, CHEN Jin
(Anhui Jiyuan Software Co., Ltd., Hefei 230031, China)

Abstract: Due to the constantly changing network security environment, new attack technologies and vulnerabilities are prone to emerge. However, facing the huge data flow generated by network communication, it will affect the effectiveness of automatic detection of network communication data leakage. Therefore, an automatic detection system for network communication data leakage based on the blockchain technology is proposed. The system hardware is based on the blockchain technology to build the network communication data storage structure, providing a more secure, reliable, and efficient data storage method for network communication. At the same time, according to the hardware requirements of the designed system, it designs the network communication data flow detection device and stain analyzer to monitor and analyze the network communication data flow in real-time, identifies the potential pollution flows, and provides a foundation for subsequent data leakage detection. The system software uses the stain analysis to describe the network communication data leakage in detail. By tracking and labeling the sensitive information in the data flow, the potential data leakage paths can be identified. The potential pollution streams are obtained and verified, based on this, the system hardware detection data are combined to develop an automatic detection program for the network communication data leakage, and achieve the automatic detection of the network communication data leakage. Experimental results show that the network communication data leakage detection accuracy of the designed system is 95%, with a minimum data leakage detection delay of 7.20 ms. The detection accuracy of three comparative methods is 66%, 80%, and 81%, respectively. The minimum detection delay values are 15.4 ms, 15.62~25.79 ms, and 12.56 ms, respectively. It is fully verified that the designed system has better application performance.

Keywords: network environment; leakage detection; communication data; access monitoring; blockchain technology; data leakage

收稿日期:2023-08-01; **修回日期**:2023-09-05。

作者简介:秦 浩(1982-),男,研究生,高级工程师。

引用格式:秦 浩,薛 伟,郭 振,等.基于区块链技术的网络通信数据泄露自动检测系统设计[J].计算机测量与控制,2024,32(8):108-114.

0　引言

随着信息技术与网络技术的发展，网络通信数据量增长速度也不断提升。网络技术的广泛应用促使大量网络应用设备的产生，例如智能移动设备、传感器设备、电子商务网站等，不同网络应用设备之间存在互联关系，并且能够不受时间与领域的限制进行实时通信，持续产生网络通信数据。根据调查研究数据显示：在光纤网线基础设备的支撑下，中国网络每秒钟能够产生数千万到数十亿的通信数据，致使网络通信数据早已达到海量级别，这为网络通信数据相关处理、保护、监控等技术提出了更高的要求。网络通信数据包含了大量的隐私数据，对网络数据安全需求也在逐渐提升。由于网络环境较为公开，恶意攻击事件无法避免。恶意攻击事件主要是指攻击者利用网络技术漏洞，侵入网络内部，对网络通信数据进行窃取、篡改的过程。随着网络整体规模的不断扩大，再加之网络用户数量的暴增与网络技术的高速发展，使得恶意攻击事件发生率持续上涨，降低了网络通信数据的安全性与完整性，也对网络运行稳定性产生了一定的不利影响。尽管网络采用了多种防护措施（防火墙、访问认证等），通信数据泄露现象依然存在，成为制约网络后续发展的关键问题之一。除此之外，造成网络通信数据泄露现象的因素比较多，比较复杂，无法采取有效的措施对其进行应对。根据调研数据可知，引发网络通信数据泄露现象的最大原因是用户误操作，但是由于网络用户数量庞大，使得多种数据泄露阻止手段均存在着效果较差的问题。传统通信数据泄露处理方法注重于事后补救，通信数据泄露已经发生，其完整性与安全性遭到破坏，此种方式对于用户的意义不大。因此，需要对网络通信数据泄露进行实时、预防性检测，对网络安全运行具有现实意义。

文献［1］以提取的网络内部数据流为基础，应用 C++软件对其进行处理与分析，制定数据泄露静态检测程序，执行制定程序即可实现数据泄露静态检测功能；文献［2］有效结合专家经验与模糊推理方法，构建了数据脆性评估体系，计算网络通信数据的敏感度，以此为基础，挖掘数据泄露漏洞，对通信数据泄露进行有效地感知；文献［3］以网络节点属性、节点信息等为基础，分析数据泄露状况，计算网络节点数据泄露概率，确定数据泄露链路，获取具有可能性的数据泄露途径，实现网络通信数据泄露的快速检测，为防止通信数据泄露现象发生提供一定的依据。上述 3 种网络通信数据泄露检测系统均存在着各自的优势与劣势，虽然能够实现网络通信数据泄露的基本检测功能，但是依然存在着漏检率高、效率低下等问题，无法满足网络未来的发展需求。

针对上述问题，提出基于区块链技术的网络通信数据泄露自动检测系统设计研究，希望通过区块链技术的应用改善现有系统存在的问题，提升数据泄露检测整体性能，为信息网络后续的发展提供助力。

1　网络通信数据泄露自动检测系统硬件模块设计

1.1　基于区块链技术搭建网络通信数据存储结构

为了提升网络通信数据的安全性，方便于后续数据泄露的自动检测，此研究基于区块链技术搭建网络通信数据存储结构，为网络通信数据泄露问题描述奠定坚实的基础。基于区块链技术搭建网络通信数据存储结构可以提供更加安全和可信的数据存储方式。区块链指的是一种点对点网络的链式数据结构，也是一种数据存储新范式，具有追溯性强、不可篡改、公开透明等优势，能够最大限度地提升网络通信数据的可靠性[4]。区块链技术由密码学、共识算法等多种技术支撑，链上存储数据由所有节点进行维护，并且每个节点均保存一份完整的区块链数据，能有效避免单点故障造成的数据泄露现象[5]。区块链系统主要包含 5 个层次结构，具体如下所示：

1）网络层：网络层是支持区块链技术应用的关键所在。联合信息网络基本组网机制、数据传输机制等建立区块链节点之间的连接、传输路径，并且保障节点之间的对等关系，维持信息网络的正常通信。区块链网络节点拓扑结构为分布式结构，表现形式由数据传播机制决定；

2）数据层：数据层承担着网络通信数据存储的功能，主要由本地存储系统 I/O 进行控制。区块链实质上是一种底层数据结构，包括时间戳、随机数、公钥数据、私钥数据等，通过此种结构对网络通信数据进行存储，可以对通信数据安全进行基础保障，降低数据泄露检测工作量；

3）共识层：共识层是区块链系统的治理层级，控制网络节点对通信数据进行一致性处理、分析与管理。另外，共识层还参与区块链安全验证环节，为其提供激励机制与惩罚机制，即奖励安全存储的网络节点，惩罚数据泄露的网络节点；

4）合约层：合约层是区块链技术实现信任的基础与前提，将算法、机制、代码等嵌入至通信数据区块链中，在多种约束条件下，自动执行区块链智能合约；

5）应用层：应用层主要是对应用场景、应用案例等进行封装，并根据实际研究情况部署应用场景，能够为通信数据泄露检测提供一定的便利[6]。

依据上述区块链系统层次结构分析结果，对网络通信数据存储结构进行改变与完善，具体如图 1 所示。

如图 1 所示，区块是按照时间先后顺序构造的，每个区块均包含着通信数据集合的时间戳与哈希值，保证了区块链的防篡改功能，提升了通信数据的安全性。若某个区块内部存储的网络通信数据发生泄露现象，则该区块哈希值会发生相应的变化，这是数据泄露检测的主要依据之一[7]。

上述过程完成了网络通信数据存储结构的搭建，为通信数据泄露检测提供一定的便利。

1.2　网络通信数据流检测装置

依据上述网络通信数据泄露问题描述结果，根据设计系统硬件需求，设计网络通信数据流检测装置，为设计系

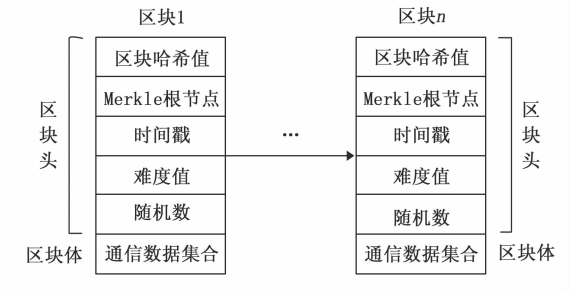

图 1 网络通信数据存储结构示意图

统稳定运行提供一定的硬件支撑。网络通信数据流检测装置主要承担着数据流异常检测的任务，是数据泄露检测的关键设备之一。已有系统数据流检测装置在应用过程中，由于运行错误容易产生检测效率低、精度差等现象[8]。通过深入分析可知，上述问题主要是因为数据流检测装置电路无调理功能，故此研究为数据流检测装置设计三相电调理电路，其具体如图 2 所示。

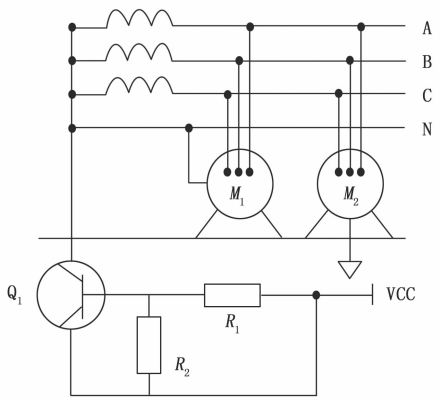

图 2 三相电调理电路示意图

图 2 中，A、B、C 指的是三相电的 3 个相位线路，即 A 相、B 相和 C 相线。N 指中性线。中性线是连接电源和负载之间的导线，提供电流回路的返回路径。中性线在三相电系统中起到平衡和稳定电压的作用，它能够将不平衡的电流分配到各个相位上，以保持系统的稳定运行。此外，中性线还承担着提供节点对地的连接以及接地保护的功能。VCC 指电源供电电压，Q1 指晶体管，用于放大信号、开关电路、调节电流和电压等，R_1、R_2 分别为调节电阻。

如图 2 所示，三相电调理电路的设计可以对信息网络通信数据流异常进行实时感知，从而准确察觉数据泄露现象，为设计系统功能实现提供良好的助力。三相电调理电路可以最大限度地提升数据流检测装置的安全性，并且可以提升设计系统硬件的可操作性，完成网络通信数据流异常的精准检测[9]。

1.3 污点分析器

污点分析器是一种用于分析数据流中存在的安全漏洞和敏感信息的工具。它可以检测到潜在的数据污点，如密码、个人身份信息、银行账户等，并根据预先设置的规则和策略对其进行分析和处理。它可以帮助确保网络通信的安全性和保密性，防止敏感信息的泄露。污点分析器与数据流检测装置并不是直接连接的，其中间需要添加一个开关。当数据流检测装置输出结果为数据流正常，开关处于关闭状态；当数据流检测装置输出结果为数据流异常，开关处于开启状态。已有系统污点分析设备由于数据通路自身缺陷，导致污点源判定结果存在着一定的偏差，会对数据泄露检测造成不利影响，无法满足信息网络技术的后续发展需求[10]。因此，设计系统采用单总线结构创建新的污点分析设备数据通路，具体如图 3 所示。

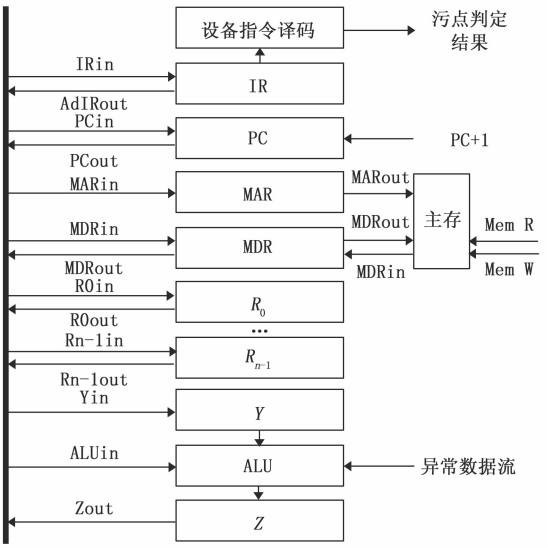

图 3 污点分析设备数据通路设计图

如图 3 所示，数据通路指的是污点分析器中每个部件之间的传送路径，是污点分析器正常运作的关键。需要注意的是，在设计系统运行之前，需对污点分析器中的数据通路进行测试，以此来保障数据通路的顺畅，提升污点分析与判定的整体效率。

除此之外，污点分析器核心芯片引脚较多，若是不对其合理配置，极容易降低污点分析器的性能，进而影响数据泄露检测的精度与效率[11]。为了提升污点分析器应用效果，对其核心芯片引脚进行定义，具体如表 1 所示。

依据表 1 所示的核心芯片引脚定义结果对污点分析器进行配置与调试，保障污点分析器性能最优化，为数据泄露检测提供硬件支撑[12]。

上述过程完成了网络通信数据流检测装置与污点分析器的设计与说明，为系统设计与软件开发提供一定的助力。

2 网络通信数据泄露自动检测系统软件功能设计

2.1 基于污点分析法描述网络通信数据泄露问题

网络通信数据泄露现象主要发生在两个阶段，分别为通信数据存储阶段与通信数据传输阶段。其中，通信数据存储阶段只需要对网络通信数据区块哈希值进行获取与分

表 1　污点分析器核心芯片引脚定义表

引脚号	引脚名	定义
1	USS	开关系统电源
2	UCC	电源
3	UEE	对比调整电压
4	RS	0－输入指令 1－输入数据
5	R/W	0－写入指令或者数据 1－读取指令或者数据
6	E	使能信号
7	DB0	数据总线 Line0
8	DB1	数据总线 Line1
9	DB2	数据总线 Line2
10	DB3	数据总线 Line3
11	DB4	数据总线 Line4
12	DB5	数据总线 Line5
13	DB6	数据总线 Line6
14	DB7	数据总线 Line7
15	A	电源正极
16	K	电源负极

析，即可判定通信数据存储阶段是否存在泄露现象。而通信数据传输阶段由于通信用户、路径较复杂，使得数据泄露检测也更加困难[13]。

此研究将网络通信数据传输阶段数据泄露问题描述为污染传播的过程。数据泄露的污点分析方法是一种用于确定数据泄露源、识别潜在泄露点以及追踪数据泄露传播路径的技术。在网络通信数据泄露问题描述之前，对污点源、泄漏点、污染变量及其污染流等定义进行明确，方便后续研究的说明与继续[14]。其中，污点源指可能包含敏感信息或已经被污染的数据源。该源可能是用户输入、数据库、文件系统等。泄露点指敏感信息从系统中泄露的地点或方式。泄露点可以是网络通信、存储介质、数据传输等。污染变量是指在安全性受到破坏的情况下，可能被恶意代码或攻击者控制的变量。这些变量可能包含敏感信息或与安全相关的数据。污染流指从污点源传播到其他变量或系统中的数据流。当污染源传递给其他变量时，数据流也被认为是污染的。依据上述定义情况，以污染变量关系图来描述网络通信数据泄露过程，本质上是一个有向连通图，表达式为：

$$\xi = (V, E) \tag{1}$$

式中，ξ 为污染变量关系图（有向连通图），V 为有向连通图的顶点，代表一个污点源、泄漏点或者污染变量，E 为有向连通图的边，代表有向边两个端点的污染传播关系。

采用圆圈（O）表示污点源，圆圈（A、B、C、D）表示污染变量，圆圈（E）表示泄露点。污点源依次传播到污染变量 A、B、C、D，最终传播到泄露点，对其进行连接即可以获得污染变量关系图，具体如图 4 所示。

如图 4 所示，在一个污染变量关系图（有向连通图）中，污点源顶点数量有且仅有一个，并且不含自回路。依

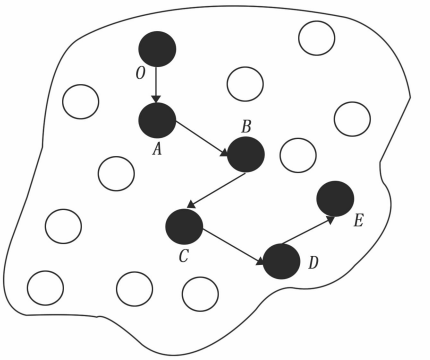

图 4　污染变量关系示例图（有向连通示例图）

据已有文献成果研究可知，网络通信数据泄露检测主要是污染变量发现与污染流追踪的过程，其需要定义若干规则，为最终研究目标的实现提供依据[15]。

污染变量关系图形成污染传播规则如表 2 所示。

表 2　污染传播规则表

规则类别	规则代码	规则内容
污染源规则	R1	规则关系为［$X.*$，W］，表示为赋值语句，左值为污染变量 $X.*$，右值为污点源方法集合
污染变量传播规则	R2	若赋值语句右值为污染变量，则赋值语句左值变量会被污染
	R3	若赋值语句右值为调用的污染封装方法（内部包含污染变量），则赋值语句左值变量会被内部变量污染
	R4	若赋值语句右值为方法调用表达式，则赋值语句左值变为污染变量
	R5	当形参的声明语句成立，则形参被污染变量 $X.*$ 污染
	R6	若存在方法调用语句满足谓词 $Return(M,X,i)$，则方法实参被形参污染
	R7	与 R6 相同
别名规则	R8	若赋值语句右值为污染变量，则赋值语句左值为右值的别名
	R9	若赋值语句左值为污染变量，则赋值语句右值为左值的别名
方法规则	R10	若赋值语句是方法的返回语句，其返回值就是污染变量
	R11	若赋值语句是形参声明语句，则形参被污染
	R12	当存在方法调用语句，方法中某个实参就是污染变量
	R13	与 R12 相同
泄露规则	R14	当存在一个属于泄漏点集合的调用语句，则某个特定参数 $Y.*$ 为污染变量，规则关系为 $<Y.*, L>$
	R15	与 R15 相同
隐式规则	R16	若污染变量被用于条件语句，认定该污染变量为隐式泄露
清除规则	R17	当赋值语句中污染变量被阈值为空值、字面量、非污染变量时，污染变量采取清除操作
	R18	与 R17 相同
	R19	与 R17 相同

上述过程完成了网络通信数据泄露问题的描述，为后续系统硬件装置或者设备的设计提供支撑。

2.2 潜在污染流获取与验证

常规情况下，一条污染流对应着一条反映其污染过程的污染变量序列[16]。在污染变量关系图中，某个污点源 W_i 到泄漏点 L_j 的路径并不是只有一条，这些路径被称为潜在污染流，对其进行获取与验证，可以为最终数据泄露检测提供一定的便利，降低数据泄露检测的运算量，提升数据泄露检测的整体效率。

此研究将潜在污染流转换成为公式（1）所示的有向连通图，数学形式表达如下：

$$f_i=[(W_i,X_1),(X_1,X_2),\cdots,(X_n,L_j)] \tag{2}$$

式中，f_i 为污染变量关系图第 i 条潜在污染流，X_i 为第 i 个污染变量，(W_i,X_1) 为 X_1 被污点源 W_i 污染，(X_{i-1},X_i) 为 X_i 被 X_{i-1} 污染，(X_n,L_j) 为 X_n 被泄漏点 L_j 泄露。

为了提升设计系统的效率，从污染传播规则（表 2）角度出发构建污染变量关系图（有向连通图）。但是，效率提升代价就是缺失精度，致使污染变量关系图中包含着不确定的污染变量，表明某些潜在污染流是虚假的，若是直接对其进行应用，会造成数据泄露检测错误事件发生，进而威胁信息网络的稳定运行。由此可见，在潜在污染流获取之后必须对其进行验证，以此来保障潜在污染流的正确性[17]。

此研究应用 FastDroid 工具提取污染变量关系图中的全部潜在污染流，记为集合 $F=\{f_1,f_2,\cdots,f_i,\cdots,f_n\}$，其验证过程主要分为 3 个阶段，具体如下所示：

阶段一：构建控制流图

应用完整函数调用污染变量关系图，结合数据泄露完整过程（潜在污染流）构建控制流图，为潜在污染流 f_i 验证提供依据；

阶段二：建立潜在污染流的期望路径

应用 FastDroid 工具对潜在污染流期望路径进行建立并标记，具体过程如下所示：

1）通过污染变量关系图构造算法对潜在污染流期望路径 ζ 进行初始化处理，设置其初始值为 null；

2）启动 for 循环，对潜在污染流中所有污染变量进行遍历，生成相应的标记语句；

3）findStatement 方法反馈污染传播关系语句，将语句中存在的污染变量添加至潜在污染流期望路径 ζ 中；

4）若 3）中污染传播关系语句是基于别名规则生成的，需要在语句前添加标记←；

5）若 3）中污染传播关系语句中污染变量存在于谓词中，需要在语句后添加标记→；

6）循环迭代进行 1）～5），直至遍历全部潜在污染流以及全部污染变量为止，输出标记后的潜在污染流期望路径 ζ[18]。

阶段三：搜索实现期望路径的可执行路径

以阶段输出的潜在污染流期望路径 ζ 为基础，联合污染过程间控制流图，将上述两者作为搜索算法的输入，其输出为布尔值。布尔值是潜在污染流真实或者虚假验证的主要依据，具体潜在污染流验证规则如下式所示：

$$\begin{cases}\eta(f_i)\geqslant\alpha^{\Delta} & f_i\text{ 真实}\\ \eta(f_i)<\alpha^{\Delta} & f_i\text{ 虚假}\end{cases} \tag{3}$$

式中，$\eta(f_i)$ 为可执行路径搜索算法输出的潜在污染流 f_i 对应布尔值；α^{Δ} 为潜在污染流真实或者虚假判定阈值，需要根据网络通信数据实际情况进行具体的设置[19]。

依据上述 3 个阶段即可完成潜在污染流的验证，将验证结果为虚假的潜在污染流进行删除处理，将验证结果为真实的潜在污染流进行保留处理，获得最终的潜在污染流集合为 $F'=\{f'_1,f'_2,\cdots,f'_i,\cdots,f'_m\}$，其中 m 为最终潜在污染流的总数量。

上述过程完成了潜在污染流的获取与验证，为后续网络通信数据泄露自动检测的实现做好充足的准备。

2.3 网络通信数据泄露自动检测实现

以上述潜在污染流获取结果 $F'=\{f'_1,f'_2,\cdots,f'_i,\cdots,f'_m\}$ 为依据，结合设计系统硬件检测数据，制定网络通信数据泄露自动检测程序，执行制定程序即可实现数据泄露的检测，为信息网络与用户数据安全提供有效的保障。

网络通信数据泄露自动检测程序分为两个子程序，主要针对的是通信数据存储阶段与通信数据传输阶段，具体如下所示：

子程序一：通信数据存储阶段数据泄露检测程序

网络通信数据区块哈希值计算公式为：

$$H_i=\frac{F'\times\beta_0\times H_{i-1}+\mathrm{str}[K_i]}{\chi^{*}+1} \tag{4}$$

式中，H_i 与 H_{i-1} 为第 i 个与第 $i-1$ 个网络通信数据区块对应的哈希值；β_0 为随机常数，取值范围为 $[0,10]$；$\mathrm{str}[K_i]$ 为数据区块 K_i 的转换函数；χ^{*} 为哈希值辅助计算因子。

以公式（4）计算结果为依据，制定通信数据存储阶段数据泄露检测规则，具体如下式所示：

$$\begin{cases}H_i\geqslant\tilde{\vartheta} & \text{存在数据泄露现象}\\ H_i<\tilde{\vartheta} & \text{不存在数据泄露现象}\end{cases} \tag{5}$$

式中，$\tilde{\vartheta}$ 为通信数据存储阶段数据泄露检测阈值，需要根据区块链技术存储的通信数据实际情况进行具体的设置。

子程序二：通信数据传输阶段数据泄露检测程序

应用设计的网络通信数据流检测装置获取信息网络的数据流，记为 $Z=\{z_1,z_2,\cdots,z_t,\cdots,z_N\}$，根据数据流的变化情况判定其是否正常，判定规则如下式所示：

$$\begin{cases}\gamma_t=\dfrac{z_t-z_{t-1}}{z_{t-1}}\times\upsilon^0\\ \begin{cases}\gamma_t>\hat{\delta} & \text{数据流异常}\\ \gamma_t\leqslant\hat{\delta} & \text{数据流正常}\end{cases}\end{cases} \tag{6}$$

式中，γ_t 为时刻 t 数据流变化率，z_t 与 z_{t-1} 为当前时刻与前一时刻的数据流，υ^0 为数据流变化率计算标准参量，$\hat{\delta}$ 为数据流状态判定阈值。

在异常数据流中依据污点源独有特征对污点源进行寻找，以确定污点源为基础，对其污染流进行探寻与提取，表达式为：

$$\psi_i = [(Y_1, Y_2), (Y_2, Y_3), \cdots, (Y_{n-1}, Y_n)] \tag{7}$$

式中，ψ_i 为异常数据中的污染流，Y_1 为污点源，Y_n 为泄露点，$Y_2, \cdots, Y_{n-1}$ 为污染变量。

衡量式（7）输出结果与潜在污染流之间的相似度，表达式为：

$$\theta(\psi_i, f'_j) = \frac{\mathrm{cov}(\psi_i, f'_j)}{\sigma(\psi_i) \cdot \sigma(f'_j)} \tag{8}$$

式中，$\theta(\psi_i, f'_j)$ 为异常数据中污染流 ψ_i 与潜在污染流 f'_j 的相似度，$\mathrm{cov}(\psi_i, f'_j)$ 为异常数据中污染流与潜在污染流的协方差数值，$\sigma(\psi_i)$ 与 $\sigma(f'_j)$ 为异常数据中污染流与潜在污染流的方差数值。

以公式（8）计算结果为基础，判定异常数据中的污染流是否为真实污染流，其判定规则为：当 $\theta(\psi_i, f'_j)$ 大于或者等于阈值 $\theta^{\odot}$ 时，认定异常数据中的污染流为真实污染流；当 $\theta(\psi_i, f'_j)$ 小于阈值 $\theta^{\odot}$ 时，认定异常数据中的污染流为虚假污染流[20]。

综上所述，在区块链技术的支撑下，实现了网络通信数据泄露自动检测系统的设计与运行，为网络数据的安全提供更有效的系统帮助。

3　实验与结果分析

设置文献［1］提出的基于智能电网内部数据流分析的内存泄露检测方法、文献［2］提出的 Kinect 传感器的网络通信数据泄露自主感知系统设计与文献［3］提出的基于 HTTP 协议的 Ad hoc 网络信息泄露点快速检测方法作为对比方法，联合设计系统共同进行网络通信数据泄露自动检测对比实验，以此来验证设计系统的应用效果。

3.1　实验准备阶段

准备阶段是实验能否顺利进行的关键所在。设计系统涉及多个参数，尤其是数据流变化率计算标准参量 υ^0，其决定着数据流异常检测的精准度，进而影响着数据泄露检测结果的准确性。因此，在实验进行之前需要对参数 υ^0 最佳取值进行确定。

通过测试获得参数 υ^0 与数据流异常检测精准度之间的关系如图 5 所示。

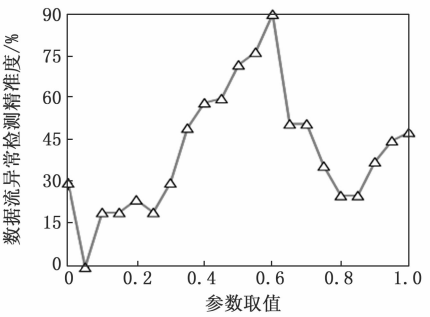

图 5　参数 υ^0 与数据流异常检测精准度关系图

如图 5 所示，当参数 υ^0 取值为 0.6 时，数据流异常检测精准度达到最大值 90%。因此，确定参数 υ^0 最佳取值为 0.6。

3.2　区块链网络配置

区块链网络是区块链技术应用的基础与前提。因此，在实验进行之前，需要对区块链网络进行科学地配置，具体配置情况如表 3 所示。

表 3　区块链网络配置表

配置排序	配置内容	配置数量
1	服务器 System x3650 M5	4 台
2	运行组织	11 个
3	维护对等节点组织数量	10 个
4	维护排序服务节点组织数量	1 个
5	通道副本	1 个

所采用 System x3650 M5 服务器是 IBM 推出的一款企业级服务器型号。它支持双路 Intel Xeon E5-2600 v3/v4 系列处理器，最高支持 1.5 TB DDR4 内存，通过 24 个 DIMM 插槽进行扩展。依据表 3 所示的内容对区块链网络进行配置与调试，保障区块链网络的稳定运行，区块链技术相关性能的稳定发挥，为设计系统的有效应用做准备。

3.3　实验结果分析

以上述实验准备内容、区块链网络配置情况为依据，进行网络通信数据泄露自动检测对比实验。为了直观显示设计系统的应用性能，选取网络通信数据泄露检测结果与数据泄露检测时延为评价指标，具体实验结果的分析过程如下所示。

通过实验获得网络通信数据泄露检测结果如图 6 所示。

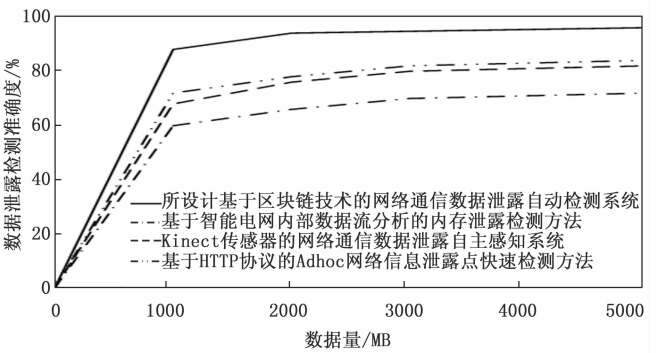

图 6　网络通信数据泄露检测结果示意图

如图 6 所示，所设计基于区块链技术的网络通信数据泄露自动检测系统应用后获得的网络通信数据泄露检测准

确性为 95%，基于智能电网内部数据流分析的内存泄露检测方法、Kinect 传感器的网络通信数据泄露自主感知系统、基于 HTTP 协议的 Ad hoc 网络信息泄露点快速检测方法获得的网络通信数据泄露检测准确性分别为 66%、80%、81%。实验结果表明设计系统网络通信数据泄露检测结果更加精确。

网络通信数据泄露检测效率是验证设计系统性能的关键指标，其主要由数据泄露检测时延来反映。常规情况下，数据泄露检测时延越短，表明网络通信数据泄露检测效率越高；数据泄露检测时延越长，表明网络通信数据泄露检测效率越低。通过实验获得数据泄露检测时延数据如表 4 所示。

表 4 数据泄露检测时延数据表 ms

实验组别	所设计基于区块链技术的网络通信数据泄露自动检测系统	基于智能电网内部数据流分析的内存泄露检测方法	Kinect 传感器的网络通信数据泄露自主感知系统	基于 HTTP 协议的 Ad hoc 网络信息泄露点快速检测方法
1	10.23	20.13	23.44	26.35
2	8.56	25.46	21.00	18.25
3	7.20	15.48	25.79	19.45
4	9.45	16.45	21.45	20.14
5	8.65	25.44	15.62	21.47
6	11.02	23.55	19.65	23.62
7	10.25	19.20	24.31	21.03
8	12.45	28.58	17.89	20.11
9	10.33	29.78	20.12	18.50
10	9.48	22.14	24.16	12.56

如表 4 所示，在不同实验组别背景下，应用所设计基于区块链技术的网络通信数据泄露自动检测系统获得的数据泄露检测时延范围为 7.20～12.45 ms，基于智能电网内部数据流分析的内存泄露检测方法获得的数据泄露检测时延范围为 15.48～29.78 ms，Kinect 传感器的网络通信数据泄露自主感知系统获得的数据泄露检测时延范围为 15.62～25.79 ms，基于 HTTP 协议的 Ad hoc 网络信息泄露点快速检测方法获得的数据泄露检测时延范围为 12.56～26.35 ms。通过数据对比可知，设计系统数据泄露检测时延远远低于 3 种对比方法，在第 3 组实验组别背景下，获得数据泄露检测时延最小值 7.20 ms，表明设计系统网络通信数据泄露检测效率更高。

4 结束语

在网络通信数据急剧增加的背景下，其安全问题也愈加严重，尤其是通信数据泄露问题。数据泄露事件发生频率逐年递增，威胁着网络通信数据的安全性与完整性，也阻碍着网络后续的发展，故提出基于区块链技术的网络通信数据泄露自动检测系统设计研究。实验结果表明，设计系统应用后大幅度地提升了网络通信数据泄露检测的精度与效率，能够为网络通信数据安全提供更有效的保障。

参考文献：

[1] 陈 畅，刘福来. 基于智能电网内部数据流分析的内存泄露检测方法研究 [J]. 信息安全研究，2022，8 (1)：85－92.

[2] 邓志东，孙 宇，居 强，等. Kinect 传感器的网络通信数据泄露自主感知系统设计 [J]. 自动化技术与应用，2021，40 (9)：75－79.

[3] 成彦衡，黄 宇. 基于 HTTP 协议的 Ad hoc 网络信息泄露点快速检测 [J]. 电子设计工程，2023，31 (3)：85－89.

[4] 张凯亮，臧国全. 泄露概率情境下的个人数据隐私计量研究 [J]. 图书情报工作，2021，65 (9)：62－69.

[5] 张人上，邱久睿. 基于多层结构的移动终端数据防泄露系统设计 [J]. 火力与指挥控制，2021，46 (7)：66－68.

[6] 马金龙，张俊峰，张冬雯，等. 基于通信序列熵的复杂网络传输容量 [J]. 物理学报，2021，70 (7)：346－354.

[7] 朱丹红，程 烨. 基于局部差分隐私的物联网敏感数据泄露控制 [J]. 计算机仿真，2021，38 (2)：472－476.

[8] 朱 睿，傅友华. 基于多 IRS 辅助的 MIMO 网络安全通信 [J]. 南京邮电大学学报：自然科学版，2022，42 (5)：29－35.

[9] 潘旭东，张 谧，杨 珉. 基于神经元激活模式控制的深度学习训练数据泄露诱导 [J]. 计算机研究与发展，2022，59 (10)：2323－2337.

[10] 魏大威，李志尧，刘晶晶，等. 基于区块链技术的智慧图书馆数字资源管理研究 [J]. 中国图书馆学报，2022，48 (2)：4－12.

[11] 张雪媛，都平平，雷 镭. 基于区块链技术的科学实验数据协同管理研究 [J]. 情报杂志，2022，41 (8)：149－155.

[12] 龚胜佳，张琳琳，赵 楷，等. 基于区块链技术的虚假新闻检测方法 [J]. 计算机应用，2022，42 (11)：3458－3464.

[13] 赵 斌，姜 雪，周 洋. 基于区块链技术的在线电子商务信用信息共享方法 [J]. 情报科学，2023，41 (1)：158－165.

[14] 方 刚，王家辉. 基于区块链技术的协同创新知识共享研究 [J]. 科技进步与对策，2022，39 (24)：130－140.

[15] 冉玲琴，彭长根，许德权，等. 基于区块链技术架构的隐私泄露风险评估方法 [J]. 计算机工程，2023，49 (1)：146－153.

[16] 相富钟，赵庆海. 基于 LSTM 模型的光通信网络数据传输负载预测方法 [J]. 激光杂志，2023，44 (2)：154－158.

[17] 朱颖婷，杨立鹏，单杏花. 基于区块链技术的旅客联程运输数据共享和售票方案研究 [J]. 铁道运输与经济，2022，44 (4)：16－21.

[18] 杨 亮. 基于区块链技术的机器人数据加密传输控制系统设计 [J]. 计算机测量与控制，2021，29 (6)：119－122.

[19] 杨 迪，徐 涵，龙承念，等. 基于区块链技术的道路路边停车管理系统 [J]. 应用科学学报，2021，39 (1)：90－98.

[20] 朱 圳，刘立芳，齐小刚. 基于数据挖掘的通信网络故障分类研究 [J]. 智能系统学报，2022，17 (6)：1228－1234.