计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190200298

基于链上链下相结合的日志安全存储与检索

吕建富[1]　赖英旭[1,2]　刘　静[1]
1 北京工业大学信息学部　北京 100124
2 信息保障技术重点实验室　北京 100072
(jianfu1993@163.com)

摘　要　信息系统中存在着大量的安全设备日志,这些安全设备日志对系统监控、查询、安全审计和故障诊断等都十分重要,因此对其进行安全存储与处理具有重要意义。文中提出了一种基于链上链下相结合的日志安全存储与检索模型,该模型结合区块链与分布式存储技术,实现了去中心化、去信任、数据难以篡改的安全设备日志存储,并对外向安全管理员提供密文检索接口,同时可以利用区块链技术实现数据的完整性校验。安全性分析论证了该模型能够保证安全设备日志的安全可靠存储,同时性能分析证明了该模型具有良好的检索效率。

关键词:安全设备日志;区块链;安全存储;密文检索;完整性校验
中图法分类号　TP309

Log Security Storage and Retrieval Based on Combination of On-chain and Off-chain

LV Jian-fu[1],LAI Ying-xu[1,2] and LIU Jing[1]
1 Faculty of Information Technology,Beijing University of Technology,Beijing 100124,China
2 Science and Technology on Information Assurance Laboratory,Beijing 100072,China

Abstract　There are a large number of security device logs in the information system. These security device logs are very important for system monitoring,query,security auditing and fault diagnosis. Therefore,it is important to securely store and process the security device logs in the information system. This paper proposed a log security storage and retrieval model based on the combination of on-chain and off-chain. This model combines blockchain and distributed storage technology,achieves security log storage which is decentralized,detrusted, and hard to tamper with data,and provides a ciphertext retrieval interface to security administrators externally. At the same time, it can use blockchain technology to realize data integrity check. The security analysis demonstrates that the model can ensure the secure and reliable storage of security device logs,and the performance analysis proves that the model has good retrieval efficiency.

Keywords　Security device log,Blockchain,Secure storage,Ciphertext retrieval,Integrity check

1　引言

随着计算机网络的普及,企业配置了越来越多的网络安全设备[1]。安全设备在系统运行中产生了大量的运行日志,如防火墙日志、入侵检测系统日志、漏洞扫描系统日志等,这些安全设备日志对系统监控、查询、安全审计和故障诊断等都是十分重要的。因此,安全设备日志往往成为了攻击对象,攻击者有针对性地修改、删除和伪造日志中的相关记录,隐藏其攻击行为;另外,信息系统内部的安全设备日志种类繁多、日志数据量巨大且较分散,数据存储和检索困难,导致大量的日志数据无法被充分利用,安全管理员很难快速从日志中得到有效信息。因此,保证安全设备日志的安全可靠存储,对于系统的检测和故障诊断等非常重要。

目前,针对日志数据的保护,文献[2]设计了一种安全审计日志协议,并通过使用防篡改硬件来增强协议的安全性;Wang 等[3]提出了一种基于安全芯片的审计日志保护机制;Jason[4]提出了将 MACs 技术与公钥密码相结合,以实现公开验证,从而保证日志的安全可靠存储;Yavuz[5]提出了一种适用于分布式存储系统的基于公钥的日志前向安全性机制。这些研究从多个方面为日志的安全存储提供了保障,但是无法更好地避免日志被恶意篡改的问题,并且过于复杂的日志保护策略在一定程度上削弱了日志数据的潜在信息价值。

区块链技术的出现给日志数据的安全可靠存储提供了一条可行的技术路径。区块链具有去中心化、去信任、信息难以

到稿日期:2019-02-15　返修日期:2019-07-08　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:青海省自然科学基金资助项目(2017-ZJ-912);信息保障技术重点实验室基金(614211204031117)
This work was supported by Qinghai Provincial Natural Science Foundation (2017-ZJ-912) and Foundation of Science and Technology on Information Assurance Laboratory (614211204031117).
通信作者:赖英旭(laiyingxu@bjut.edu.cn)

篡改等特点，能有效保证数据的完整性，同时能通过数据加密来保证数据的机密性。基于此，本文提出一种基于区块链的日志安全存储与检索方案，该方案采用链上链下相结合的方式来实现日志的安全可靠存储与检索，将日志摘要、数据索引等重要信息交由区块链管理，保证了重要信息的安全可靠性；同时将真实的日志数据加密存储于链下分布式数据库中。基于链上链下相结合的存储管理方式既能减轻区块链上数据存储和高频访问的压力，又能实现大量日志数据的加密存储；同时，该方案对外提供密文检索接口。针对安全设备日志检索的特殊性，将时间戳作为主关键词检索，能很好地改善检索效率，实现日志数据的高效检索。

2 相关技术背景

2.1 区块链技术

(1)区块链概念。区块链技术起源于 2008 年 Nakamoto 在密码学邮件组发表的奠基性论文“Bitcoin：A peer-to-peer Electronic Cash System”[6]。狭义来讲，区块链是一种按照时间顺序将数据区块以链条的方式组合而成的链式数据结构，如图 1 所示。广义来讲，区块链技术是利用加密链式区块结构来验证与存储数据，并利用分布式节点共识算法来生成和更新数据的一种全新的分布式基础架构与计算范式[7]。

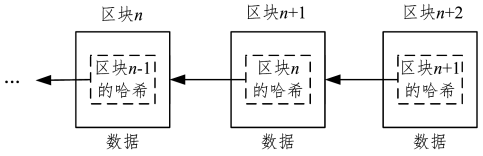

图 1 区块链数据结构

Fig. 1 Blockchain data structure

(2)区块链网络架构。区块链系统的网络架构分为公有链、联盟链、私有链 3 种[8]，不同网络架构之间的区别如表 1 所列。

表 1 区块链的网络架构

Table 1 Network structure of blockchain

架构类型	中心化程度	参与者	信任机制	记账者	典型案例
公有链	去中心化	任何人	工作量证明	所有参与者	比特币，以太坊
联盟链	多中心化	特定成员	共识机制	协商决定	清算
私有链	中心化	特定成员	自行背书	自定	R3 联盟

(3)区块链共识算法。共识算法是区块链技术的核心要素，也是近年来分布式系统的研究热点[9]。本文拟采用联盟链构建用于管理日志数据的区块链系统，其中使用较多的共识算法为实用拜占庭容错(Practical Byzantine Fault Tolerance，PBFT)算法[10]。该算法是一种状态机副本复制算法，所有的副本均在一个视图轮换的过程中操作，通过视图编号以及节点数集合来确定主节点。本文采用了 PBFT 作为日志联盟链的共识算法，共识过程在具体的存储过程中介绍。

(4)区块链应用。2013 年 12 月，Buterin[11]提出了以太坊(Ethereum)区块链平台，该平台首次将智能合约(Smart Contract)融入到区块链中。2015 年 12 月，Linux 基金会发起了 Hyperledger 开源区块链项目[12]。2016 年 4 月，R3 公司发布了面向金融机构定制设计的分布式账本平台 Corda[13]。2016 年 2 月，BigchainDB 公司发布了可扩展的区块链数据库 BigchainDB[14-15]。文献[16-17]在比特币的基础上，提出了基于数据可追溯性证明的去中心化数据存储模式[18]，提高了数据的安全性。文献[19]给出了区块链应用在物联网中的挑战和解决方法，并给出了应用场景。BlockStack[20]在传统 DNS 的基础上加入了区块链的特性，提出了一种安全的命名空间存储系统，通过虚拟链[21]来查询和修改区块链中的数据。文献[22]提出了一种基于区块链的数据验证方法，从而保证从第三方获取的数据确实是原始上传的数据。文献[23]提出了一个基于区块链的数据完整性服务框架。文献[24-25]针对医疗数据的隐私性和安全性问题，提出了基于区块链的医疗数据共享模型。

2.2 安全设备日志数据

安全设备日志是指产生于 IT 架构中各个硬件设备、网络设备运行过程中的多源异构数据。由于日志数据对于信息系统的安全、稳定、可靠运行具有重要的作用，因此对其进行合理的收集和应用是信息系统安全稳定运行的重要保障。

随着现代计算机系统规模和复杂性的不断增加，安全设备产生的日志数量不断增多，其中包含了信息系统活动相关的重要信息。安全设备日志数据具有海量、多样、异构等特点，如何有效地收集与处理安全设备日志数据成为了网络运维管理人员的研究课题。对安全设备日志数据的研究主要分为两个方面：1)数据主要来源于防火墙、入侵检测系统、漏洞扫描系统等安全设备，具有数据量大、类型复杂、速度快等特点，如何对其进行高效的收集管理是安全设备日志数据中的一大问题；2)安全设备日志数据具有很高的利用价值，通过对安全设备日志数据进行分析，能够对系统监控、查询、安全审计和故障诊断起到至关重要的作用。

3 基于区块链技术的日志安全存储与检索

应用安全设备日志数据的前提是对日志数据进行高效收集、安全存储以及管理。本文通过分布式存储技术对日志数据进行收集与存储，但在分布式存储过程中，用户通常无法控制正在使用的数据存储服务器，这意味着存在破坏数据机密性、数据完整性和数据可用性的风险。区块链技术作为一种全新的技术框架，与传统的数据管理技术相比，它非常适用于保障重要数据的机密性、一致性、完整性。利用区块链技术存储数据，从根本上防止了恶意的入侵者以及内部人员的非法访问。对此，本文根据链上链下相结合的思想提出了基于区块链的日志安全存储与检索方案。

3.1 日志数据的存储架构

本文设计了一种基于区块链的日志安全存储模型，实现了去中心化、安全不可篡改的日志数据存储。在该模型的基础上，通过结合 PBFT 共识算法，可实现对日志数据的采集、存储、利用等，保证了日志数据的安全可靠存储。该模型采用链上链下相结合的方式实现对日志数据的安全存储，将日志数据文件加密存储在分布式数据库系统(Distributed Database System，DDBS)中，解决了数据集中存储在服务器上的

问题，同时也减轻了区块链上的数据存储和高频访问的压力。

日志安全存储模型如图 2 所示，其主要包括以下实体：

(1)分布式数据库系统。安全设备日志最终将存储在 DDBS 中，为了保证数据的机密性，通过加密算法对数据进行加密存储。

(2)数据区块。为了保证日志数据的内容可信、不被篡改，本文模型将日志数据摘要、日志元数据存储在区块体交易记录中，以保证安全管理员对日志数据进行数据完整性校验。在区块中，每一条数据记录包含 3 个元组：公钥、日志数据摘要和元数据。

(3)共识算法。为了保证日志数据的安全高效存储，本文使用 PBFT 共识算法，有效地实现了日志数据的去中心化存储。在数据记录节点中通过工作量证明(Proof of Work，PoW)选出主节点，其他节点为从节点，然后通过 PBFT 共识算法进行区块的广播验证存储工作，从而有效减少系统资源的浪费。

(4)安全管理员。通过该模型对安全设备日志数据进行存储还须对安全管理员提供密文检索接口，同时可以利用区块链中存储的数据摘要进行数据完整性校验。

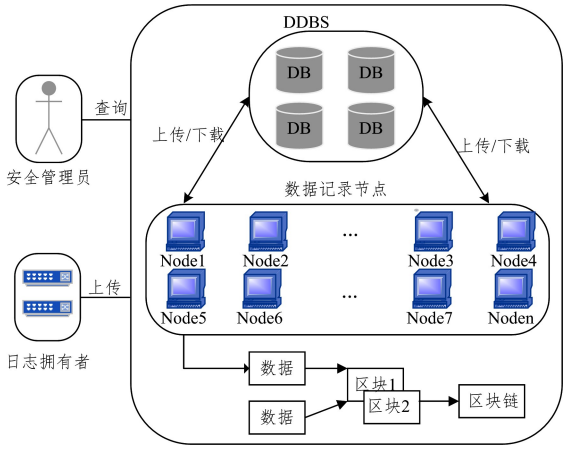

图 2 基于区块链的日志安全存储模型

Fig. 2 Block-based log security storage model

3.2 日志数据的预处理

为了实现日志的安全存储以及密文检索，日志拥有者应对日志文档进行预处理。

(1)根据日志文档生成日志元数据。将时间戳、IP 地址、Port 端口号、Protocol 协议等信息从日志文档中提取出来作为关键词，得到关键词集合 $K=(K_1,K_2,\cdots,K_n)$，将其作为日志文档元数据。

(2)构建倒排索引：根据日志文档元数据构建密文关键词集合 $EK=(EK_1,EK_2,\cdots,EK_m)$。对于每一个密文关键词 EK_i，提取包含该关键词的日志文档 F_i 作为一个元组插入索引链表中。倒排索引如图 3 所示。

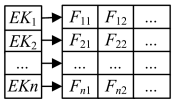

图 3 倒排索引的结构图

Fig. 3 Structure graph of inverted index

链上存储中，数据索引由区块链管理以保证索引的安全性。本文对区块链头结构做了字段扩展，用于存储日志文档预处理之后的倒排索引，如图 4 所示。

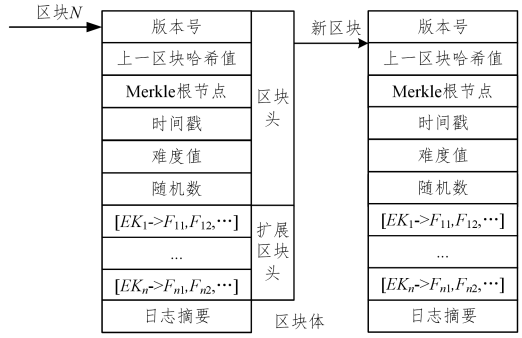

图 4 扩展的区块链结构

Fig. 4 Extended blockchain structure

3.3 日志数据的安全存储

本文基于区块链技术实现了日志数据的采集以及安全存储，表 2 列出了所用符号及含义。

表 2 符号及其含义

Table 2 Symbols and corresponding meaning

符号	含义
N_i	第 i 个日志拥有者
R_j	第 j 个数据记录节点
PK_i,SK_i	实体 i 的公钥、私钥
$Timestamp$	时间戳
$E_{PK_i}(m)$	用实体 i 的公钥加密 m
$Sign_{SK_i}(m)$	用实体 i 的私钥对 m 签名
$Hash(m)$	用实体 i 的私钥对 m 签名
$MetaData$	元数据
$x \parallel y$	元素 x 连接元素 y
$Record$	消息记录

日志数据的具体采集存储过程如下：

(1)日志拥有者以自己的公钥作为标识，向本地数据记录节点提交上传请求。具体表示为：

$$N_i \rightarrow R_j: Request=(Req \parallel PK_{N_i}) \tag{1}$$

(2)本地数据记录节点对日志拥有者的公钥进行验证，确认其具有上传数据的权限。

(3)日志拥有者利用自己的私钥对数据摘要进行数字签名，并用自己的公钥对数据进行加密。该过程具体描述为：

$$N_i \rightarrow R_j: Sign=Sign_{SK_{N_i}}(Hash(m)) \tag{2}$$

$$Record=E_{PK_{N_i}}(Data \parallel timestamp \parallel Sign) \tag{3}$$

(4)本地数据记录节点收集上传数据：数据记录节点对上传 $Record$ 进行验证，如果数据安全有效，则将日志数据加密存储到分布式数据库，同时将日志元数据提交给数据记录节点。

(5)数据记录节点工作量证明：每隔 10 min，数据记录节点 R_j 把这段时间内所有暂存的数据整合成数据集合(表示为 $Data\_Set=\{MetaData \parallel timestamp\}$)。通过 PoW 的方式来确定某个时间段内的数据记录管理权限。

(6)数据记录节点间的区块共识过程：将最快计算出工作量证明的数据记录节点作为共识过程的主节点(设为 R_j，标记为 Leader)，其余数据记录节点作为从节点。本文采用 PBFT 共识算法进行区块共识。

Step1 如图 5 所示，Leader 将收集到的日志数据整合成一个新的数据区块，附上主节点的数字签名和新数据区块的哈希值以备审查验证。Leader 向各个从节点广播新生成的数据区块以待验证。

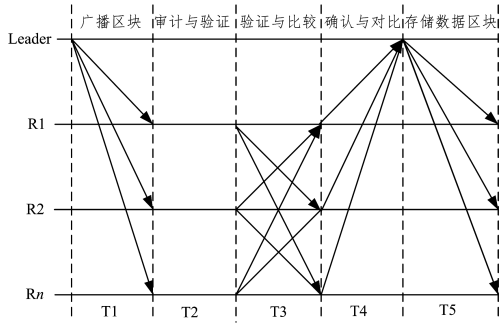

图 5 日志联盟链的共识过程

Fig. 5 Consensus process of log alliance chain

Step2 从节点接收到来自主节点的日志区块后，通过验证主节点发送来的区块哈希值和数字签名等信息来确认区块的合法性和正确性，并将验证结果(Result)附上各自的数字签名广播给其他从节点，保证节点间的相互监督和共同查验。

Step3 各从节点接收并汇总其他节点的审查结果，同时与自身的审查结果进行比对，然后向主节点发送一个响应结果(Reply)，这个响应结果包含从节点自身的审查结果和收到的所有审查结果以及对比结果。

Step4 主节点汇总各从节点的审计回复。若全部数据记录节点都认可当前数据区块的合法性和正确性，则将该区块链接到联盟链中。

Step5 若有部分数据记录节点不认可当前的审计结果，主节点将分析和查验这些节点的审计结果。主节点可重新发送该数据区块给这些节点进行二次审计，若仍有节点不认可，则采用少数服从多数的原则。同时，主节点将判断这些数据记录节点是否有恶意行为，及时对恶意节点进行处理，从而保证系统的安全运行。

3.4 密文检索及数据完整性验证

为了保证数据的机密性，安全设备日志数据在分布式数据库中以密文的形式存储。为了分析日志信息，本文采用可搜索加密技术来实现安全设备日志的密文检索。在加密存储数据的同时，将日志数据摘要以及倒排索引保存在区块链中，一方面便于密文日志的快速检索，另一方面可以对检索到的数据进行数据完整性验证，以保证检索到的数据没有被篡改过。图 6 给出了密文检索以及数据完整性验证过程。

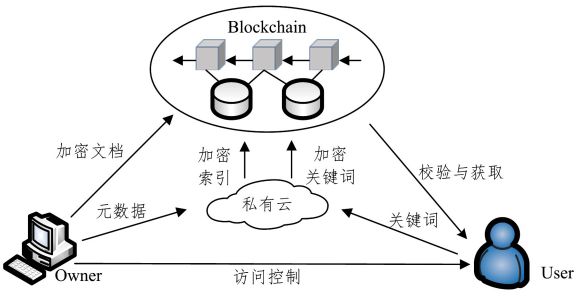

图 6 检索以及数据完整性验证过程

Fig. 6 Search and data integrity verification process

(1)*User*→私有云：用户输入查询关键词组合(起始时间＋截止时间＋IP 或时间＋Port 等)，私有云获取用户输入的关键词组合。系统首先根据用户输入的时间段进行链上检索，检索所需时间段内的日志信息；然后根据区块链时间戳锁定所需时间段的日志所在的区块；最后私有云将次关键词(IP 或 Port)加密提交给分布式数据库。

链式检索过程的伪代码描述如下：

```
Procedure query(time1,time2,kw,buffer)
1. begin
2.   while(previousHash!=NULL)
3.       if(previousHash.timestamp>time1 and previousHash.time-
         stamp<time2)
4.           if(kw in previousHash.select)
5.               buffer.add(previousHash.data)
6.           end if
7.       end if
8.       previousHash=previousHash.next
9.   end while
10. return buffer
11. end
```

(2)*User*←私有云：根据区块中存储的索引信息获取相关日志数据密文，将检索到的日志数据密文返回给用户。用户解密从数据库检索到的日志数据密文，同时利用哈希函数计算日志数据的摘要。

(3)*User*↔*Blockchain*：在检索到相关日志数据的同时，可以在区块体交易记录中获得相关日志数据摘要，将该摘要与第(2)步计算的数据摘要进行比对，若一致，则检索到的日志数据没有被恶意篡改；否则数据是被恶意篡改过的。

4 安全性能分析

本节将从两个方面分析本文方案的安全性，并通过实验进行性能分析。

4.1 安全性分析

本文从区块链的安全性方面提出两个问题，并进行了分析证明。

问题 1 区块链在一定的容忍度下，是否是不可篡改和不可伪造的。

系统方案利用密码学算法来保证信息传递的真实性、可靠性、完整性。数据的发送方要对数据的哈希值进行签名。文中 $Hash(m)$ 表示数据 m 的哈希值，则 $Sign_{sk_i}(Hash(m))$ 表示节点 i 对数据 m 哈希值的数字签名。本文方案采用 PBFT 算法完成数据区块的共识过程，假设本文方案是由 n 个节点组成的共识系统，则该算法提供 $f=\frac{n-1}{3}$ 的容错能力，即系统的失效节点数不能超过全网节点的 1/3。其中，f 代表恶意节点个数，$n=|R_j|$ 为参与共识的节点数，R_j 为共识节点集合。

为了证明系统的安全性，本文假设系统网络正好将所有共识节点分为 3 个部分，即 $R_j=R_1\cup R_2\cup F$，且 $R_1\cap R_2=\varnothing$，$R_2\cap F=\varnothing$，$R_1\cap F=\varnothing$；同时，假设 R_1 和 R_2 均由诚实可信的节点组成，F 全部由恶意节点组成且已形成合谋，可以统一运

行。在共识过程中，节点广播的消息内容包含数字签名，因此恶意节点无法伪造节点。恶意节点若想破坏共识过程，只能试图改变系统的状态，使系统状态回退到前一状态，即使系统产生“分叉”，从而伪造一个区块链。

若恶意节点 F 想要使系统产生“分叉”，则恶意节点只需与可信节点 R_1 达成共识并发布新区块，且在不告知可信节点 R_2 的情况下与之完成第二次共识，撤销与 R_1 的共识。若须达成此过程，则须满足：$|R_1|+|F|\geqslant n-f$，且 $|R_2|+|F|\geqslant n-f$。系统最坏情况为恶意节点数量达到了系统所能容忍的最大值，即 $|F|=f$。因此不等式化简为：$|R_1|\geqslant n-2f$，且 $|R_2|\geqslant n-2f$。将上述不等式相加得 $|R_1|+|R_2|\geqslant 2n-4f$，化简得 $n\leqslant 3f$。已知 $f=\frac{(n-1)}{3}$，这与 $n\leqslant 3f$ 矛盾，因此该方案在共识算法的容错范围内无法分叉，则恶意节点无法进行恶意破坏。同时，系统方案中的网络节点都是日志联盟链内规定的节点，不会有外部任意节点加入此网络虚假广播恶意信息。

问题 2　日志数据摘要以及元数据能否正确保存在区块链中。

在区块链的形成过程中，采用 PBFT 共识算法进行区块共识，并对日志数据摘要以及元数据的记录进行监督。日志联盟链中的主节点由工作量证明过程产生，数据完整性和打包信息的公正性由区块链中的其他节点保证。同时，联盟链还被监管机构对主节点的工作进行监督，以保证数据操作记录能够完整地保存在区块中形成区块链。

综合以上 2 个问题和安全性分析，可以将区块链安全性与数据完整性的安全性有效结合，以保证整体模型的安全可靠。

4.2　系统性能分析

为了验证本文提出的基于区块链的日志安全存储与检索架构，基于 Java 语言开发存储检索日志的联盟链。将该链部署在 2 台物理机以及 4 台 VM(ubuntu16.04)虚拟机中，即包含 6 个节点的日志联盟链；同时链下分布式数据库采用 Hadoop 文件存储系统，在其中 1 台物理机上基于 Hadoop2.9.0 搭建了伪分布式集群环境。

为了验证所提方案在保证安全性的前提下不会过于损失检索效率，同时测试了将密文元数据存储在链下的检索时间。本文以 Snort 检测的告警日志为测试数据集进行检索，利用 Snort 系统在 24 h 产生的数据量进行测试实验，实验过程中累计采集到日志数据 200 000 条。实验中每个测试数据均为实验运行 10 次所取的平均值，图 7 对比了两种检索方案的检索时间。

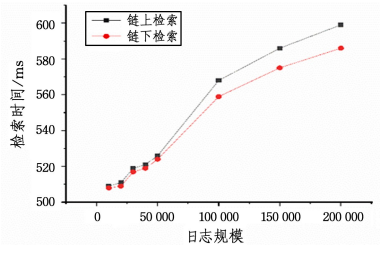

图 7　日志检索时间

Fig. 7　Log retrieval time

从图 7 可以看出，随着日志存储规模的增大，两种检索方案的检索时间也逐渐增长。在相同日志规模下，所提链上检索方案在提高安全性的基础上，较链下检索方案的检索效率损失不大；同时，随着日志规模的增大，区块链中构建的区块数量也逐渐增加，但检索时间没有过度延长，两种方案的增长幅度基本一致。本文所应用的密文检索算法是基于倒排索引的查询，链下检索方案的查找效率与索引本身有关。由图 7 可知，查找效率拟合成一个对数函数，链上检索方案的查找效率与形成的区块数量有关，时间复杂度为 $O(|W|*|N|)$，其中 $|W|$ 为关键词的数量，$|N|$ 是所形成的区块个数。针对安全设备日志检索的特殊性，将时间戳作为主关键词，能很好地改善检索效率。

综上所述，基于链上链下相结合的日志安全存储与检索模型采用区块链保证了安全设备日志数据的机密性以及完整性，并通过链上索引的方式对外提供密文检索接口。实验验证了所提方案在保证日志数据机密性以及完整性的同时，检索效率与链下检索方式基本持平。

结束语　本文设计了一种基于区块链的日志安全存储与检索模型。该模型所采用的链上链下相结合的安全存储方案既可以实现日志信息的海量存储，又可以保证日志信息的安全性，防止被恶意篡改。在保证日志信息安全海量存储的同时，通过利用 PBFT 算法，在不浪费计算资源的前提下保证了日志信息的一致性；另外，系统对外提供了密文检索接口，用户可以通过关键词查询相关的日志数据。该模型保证了安全设备日志数据的机密性、完整性以及可用性。本文在考虑数据安全性的情况下，损失了一定的密文检索效率，未来将考虑如何在保证更高安全性的前提下更好地提高密文检索的效率。

参 考 文 献

[1] KUMAR M, SINGH A K, KUMAR T V S. Secure Log Storage Using Blockchain and Cloud Infrastructure[C]// 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). Washington D C: IEEE, 2018: 1-4.

[2] CHONG C N, PENG Z, HARTEL P H. Secure audit logging with tamper-resistant hardware[C]// IFIP International Information Security Conference. Boston: Springer, 2003: 73-84.

[3] WANG G, WANG Z, SUN J, et al. An Audit Log Protection Mechanism Based on SecurityChip[C]// International Conference on Trusted Systems. Cham: Springer, 2015: 226-233.

[4] HOLT J E. Logcrypt: forward security and public verification for secure audit logs[C]// Proceedings of the 2006 Australasian Workshops on Grid Computing and E-research. New York: ACM, 2006, 167: 203-211.

[5] YAVUZ A A, NING P. Baf: An efficient publicly verifiable secure audit logging scheme for distributed systems[C]// 2009 Annual Computer Security Applications Conference. Washington D C: IEEE, 2009: 219-228.

[6] NAKAMOTO S. Bitcoin: A peer-to-peer Electronic Cash System [OL]. https://bitcoin.org/bitcoin.pdf.

[7] YUAN Y, WANG F Y. Blockchain: The State of the Art and

Future Trends[J]. Acta AutomaticaSinica, 2016, 42(4): 481-494.

[8] SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: Architecture and Reasearch Progress[J]. Chinese Journal of Computer, 2018, 41(5): 969-988.

[9] MINGXIAOD, XIAOFENG M, ZHE Z, et al. Areview on consensus algorithm of blockchain[C]// 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC). Washington D C: IEEE, 2017: 2567-2572.

[10] CASTROM, LISKOV B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461.

[11] BUTERINV. A next-generation smart contract and decentralized application platform[R]. 2014.

[12] CACHINC. Architecture of the hyperledger blockchain fabric [C]// Workshop on Distributed Cryptocurrencies and Consensus Ledgers. 2016.

[13] BROWNR G. Introducing r3 cordatm: A distributed ledger designed for financial services[R]. R3: Corda, 2016.

[14] MCCONAGHYT, MARQUESR, MÜLLERA, et al. BigchainDB: A scalable blockchain database[R]. GmbH: BigchainDB, 2016.

[15] Bigchaindb White Paper. BigchainDB: Ascalableblockchain database[EB/OL]. (2017-01-11). https://www. bigchaindb. com/whitepaper/bigchaindb-whitepaper. pdf.

[16] ANDREW M, ARI J, ELAINE S, et al. Permacoin: Repurposing bitcoin work for data preservation [C]// Proceedings of IEEE Symposium on Security and Privacy. Washington D C: IEEE, 2014: 475-490.

[17] BINANDA S, SAMIRAN B, SUSHMITA R, et al. Retricoin: Bitcoinbased on compact proofs of retrievability[C]// Proceedings of the 17th International Conference on Distributed Computing and Networking. New York: ACM, 2016: 14: 1-10.

[18] RUJ S, RAHMAN M S, BASU A, et al. BlockStore: A Secure Decentralized Storage Framework on Blockchain[C]// 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA). Washington D C: IEEE, 2018: 1096-1103.

[19] ALI D, SALIL S, RAJA J. Blockchain in Internet of Things: Challenges and solutions[EB/OL]. (2015-11-12). httpsarxiv. org/ftp/arxiv/papers/1608/160-8. 05187. pdf.

[20] MUNEEB A, JUDE C, RYAN S, et al. Blockstack: A globalnaming and storage system secured by blockchains[C]// Proceedings of the 2016 USE-NIX Annual Technical Conference. Denver: USENIX Association, 2016: 181-194.

[21] JUDEN, MUNEEB A. Extending existing blockchains with virtualchain[EB/OL]. (2016-12-13). http://www. zurich. ibm. com/dccl/paper-s/nelson_dccl_slides. pdf.

[22] LIU Y, CHEN H, HU F. A blockchain-based verification for sharing data securely[C]// 2017 International Conference on Progress in Informatics and Computing (PIC). Washington D C: IEEE, 2017: 249-253.

[23] LIU B, YU X L, CHEN S, et al. Blockchain based data integrity service framework for IoT data[C]// 2017 IEEE International Conference on Web Services (ICWS). Washington D C: IEEE, 2017: 468-475.

[24] THEODOULI A, ARAKLIOTIS S, MOSCHOU K, et al. On the design of a Blockchain-based system to facilitate Healthcare Data Sharing[C]// 2018 17th IEEE International Conference On Trust, Security And Privacy in Computing and Communications. Washington D C: IEEE, 2018: 1374-1379.

[25] ALOMAR A, BHUIYAN M Z A, BASU A, et al. Privacy-friendly platform for healthcare data in cloud based on blockchain environment[J]. Future Generation Computer Systems, 2019, 95(6): 511-521.

LV Jian-fu, born in 1993, postgraduate. His main research interests include cyber security, and blockchain.

LAI Ying-xu, born in 1973, Ph. D, professor, Ph. D supervisor. Her main research interests include computer network and cyber security.