计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2020,29(7):233−238 [doi: 10.15888/j.cnki.csa.007486]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于区块链技术的查询索引认证方法①

张少帅[1], 胡志勇[2], 张倩倩[3]

[1](太原科技大学 计算机科学与技术学院, 太原 030024)
[2](太原鹏跃电子科技有限公司, 太原 030032)
[3](西北农林科技大学 理学院, 杨凌 712100)
通讯作者: 张少帅, E-mail: melo2010k@163.com

摘　要: 为了实时快捷地在视频流上生成模式索引, 提出了基于区块链的索引认证方案, 用于面向事件的实时监控视频查询. 通过边缘节点和雾节点之间的加密安全信道来保护索引数据, 以提升智能监控系统的安全性. 首先, 通过在嵌入式边缘设备上执行检测和跟踪任务, 面向事件的监控服务通过处理输入帧来提取特征信息; 然后, 实时索引服务为每帧生成唯一性索引, 以防止对图像的恶意修改; 最后, 将帧索引输入区块链网络, 并通过基于去中心化智能合约的认证机制进行验证. 实验结果证明了本文方案的可行性和有效性. 其总开销非常低, 适用于实时监控视频查询的应用.

关键词: 区块链; 索引认证; 监控视频查询; 去中心化; 特征信息

引用格式: 张少帅,胡志勇,张倩倩.基于区块链技术的查询索引认证方法.计算机系统应用,2020,29(7):233–238. http://www.c-s-a.org.cn/1003-3254/7486.html

Query Index Authentication Method Based on Blockchain Technology

ZHANG Shao-Shuai[1], HU Zhi-Yong[2], ZHANG Qian-Qian[3]

[1](School of Computer Science and Technology, Taiyuan University of Science and Technology, Taiyuan 030024, China)
[2](Taiyuan Pengyue Electronic Science and Technology Co. Ltd., Taiyuan 030032, China)
[3](College of Science, Northwest A & F University, Yangling 712100, China)

Abstract: In order to generate pattern index on video stream in real time and quickly, an index authentication scheme based on Blockchain is proposed for event oriented real-time monitoring video query. By encrypting the secure channel between edge node and fog node, index data can be protected to improve the security of intelligent monitoring system. Firstly, by performing detection and tracking tasks on embedded edge devices, event oriented monitoring service extracts feature information by processing input frames. Then, real-time index service generates a unique index for each frame to prevent malicious modification of the image. Finally, the frame index is input into the Blockchain network and verified through the authentication mechanism based on decentralized smart contract Card. The experimental results show the feasibility and effectiveness of this scheme. The total cost is very low, which is suitable for the application of real-time monitoring video query.

Key words: Blockchain; index authentication; monitoring video query; decentralized; feature information

智能监控是智能城市概念中的核心主题之一, 具有广阔的应用前景, 包括相关区域的访问控制[1]、身份和行为识别[2]、人群流量统计和拥塞分析[3]、异常行为检测[4], 以及使用多个相机的交互式监控[5]. 这些领域的研究对智能城市的推动具有重大意义. 很多研究都集中在某个点上的研究, 很少从大数据角度出发.

① 基金项目: 西北农林科技大学博士科研启动基金 (Z1090219032)
Foundation item: Scientific Research Start-Up Fund for Doctorate of Northwest A & F University (Z1090219032)
收稿时间: 2019-12-05; 修改时间: 2020-01-03; 采用时间: 2020-01-07; csa 在线出版时间: 2020-07-03

由于大数据任务的计算要求非常繁重, 很多智能监控应用依赖于集中式云计算框架, 此类框架具有强大算力, 高度灵活性和优秀的可扩展性. 然而, 必须将大量原始的帧数据传输到云数据中心, 这就不可避免地产生不确定的延迟, 并给通信网络带来额外的工作负载. 此外, 从数以千计的视频帧中即时识别出感兴趣目标或放大可疑行为, 是非常有挑战性的任务[6]. 与依赖云数据中心进行批处理相比, 以实时、现场的方式在视频流上生成模式索引更有利于系统部署[7].

目前, 雾计算和边缘计算能够将计算任务迁移至网络边缘, 有望解决云架构运行的智能监控系统的难题. 通过提高网络摄像机和智能移动设备的智能化程度, 允许利用网络边缘处的去中心化节点执行更多作业. 由此使得智能监控系统满足对延迟敏感的关键任务的要求[8]. 分布式边缘设备/雾设备对原始视频流进行本地处理, 并通过提取、识别和标记有用特征, 使视频具有可索引性. 特征描述和索引数据被传输到高层节点, 以完成高级分析任务. 然而, 远程数据传输也会产生数据安全和隐私方面的问题, 可能会遭受恶意攻击, 例如拒绝服务 (DoS) 攻击、虚假视频注入攻击、跟踪轨迹修改、私人视频流窃听等.

由于智能监控系统被部署在分布式网络环境, 其中包含大量具有高度异质性和动态性的 IoT 设备, 这就要求分布式 IoT 网络采用扩展性强、灵活性高的轻量级安全机制. 此外, 这些智能设备分散在不可信网络环境的近场边缘网络中. 在此类设备上以集权的方式实施安全机制是不合适的, 会造成性能瓶颈或单点故障问题. 因此, 智能监控系统需要新的去中心化框架, 针对无信任应用网络环境提供安全方案. 而区块链技术满足这些要求, 支持去中心化和匿名维护等[9]. 本文的创新之处是提出了基于区块链的索引认证方案, 用于面向事件的实时监控视频查询, 以提升智能监控系统的安全性. 主要工作总结如下: 1) 提出了用于智能监控系统的实时索引认证方案的完整框架, 其中包括面向事件的监控视频查询, 实时索引, 以及基于区块链的认证; 2) 在局部私有区块链网络上实施并部署了基于智能合约的概念证明原型.

1 IoT 中的区块链和智能合约

区块链由 Nakamoto 在 2008 年提出[10], 是比特币的技术基础. 区块链是一种公共账本, 其提供了可验证、仅可附加的链式交易数据结构. 区块链支持分布式存储和更新数据, 本质上是去中心化架构, 不再依赖集中式管理. 由“矿工”对交易进行核实并记录在包含时间戳的区块中, 每个区块包含加密散列标识, 并按时间顺序链接到之前的区块上. 区块链使用共识机制, 在大量被称为“矿工”的分布式节点上强制执行该机制, 以维护记录在区块上的数据的不可篡改性. 得益于对网络中矿工采用的不信任证明机制, 用户可以信任存储在世界各地不同的分布式节点上的公共账本系统, 这些账本由“矿工-会计师”来维护, 无需与交易对方或第三方中介建立并保持信任. 因此, 为确保不信任环境 (例如 IoT 网络) 中所有参与方之间的分布式交易的安全, 区块链是较为理想的去中心化架构.

区块链技术具有很多优秀特性, 因此研究人员尝试利用该技术解决 IoT 网络中的安全问题, 例如访问控制[9]. 区块链已经在货币和支付的去中心化上获得了成功, 例如比特币. 设计支持各种灵活的事务类型的可编程合约成为了一种趋势, 从而将区块链的应用扩展到加密货币之外的领域. 智能合约允许用户通过区块链网络达成多方共识, 而无需依赖于第三方来保持信任关系. 通过利用密码和安全机制, 智能合约将协议与用户接口相结合, 实现计算机网络上关系的规范和安全.

智能合约包括预定义指令和数据的集合, 这些指令和数据作为 Merkle 哈希树保存在区块链的特定地址上, Merkle 哈系树采用自下而上的二叉树数据结构而构建. 智能合约通过应用程序二进制接口 (ABI) 与用户交互, 以提供预定义的商业逻辑或合约协议. 用于 IoT 系统的基于智能合约的安全机制已经成为一个研究热点, 例如数据保护和访问控制. 本文希望结合区块链和智能合约, 为分布式智能监控系统的索引认证提供可行的解决方案.

2 实时索引认证

受智能合约和区块链技术的启发, 本文提出了用于面向事件的监控视频查询系统的实时索引认证方案, 从而在不可信的边缘网络环境中提供去中心化的视频流安全机制. 图 1 给出了提出的系统框架, 演示场景包括两个独立的基于 IoT 的视频监控域, 且两者之间没有预先建立信任关系. 通过智能摄像机执行目标检测和跟踪任务, 在网络边缘处处理监控视频流以提取低等级特征信息, 其后传输到雾设备以进行数据聚合并

作进一步分析. 在每个域中, 雾设备不但强制实施预定义的安全策略以管理域相关的设备和服务, 而且作为中介与公共区块链和云进行交互, 以支持面向事件的监控视频序列的索引认证. 本文框架的主要组件包括面向事件的监控视频序列、实时索引和安全数据传输, 以及基于区块链的认证.

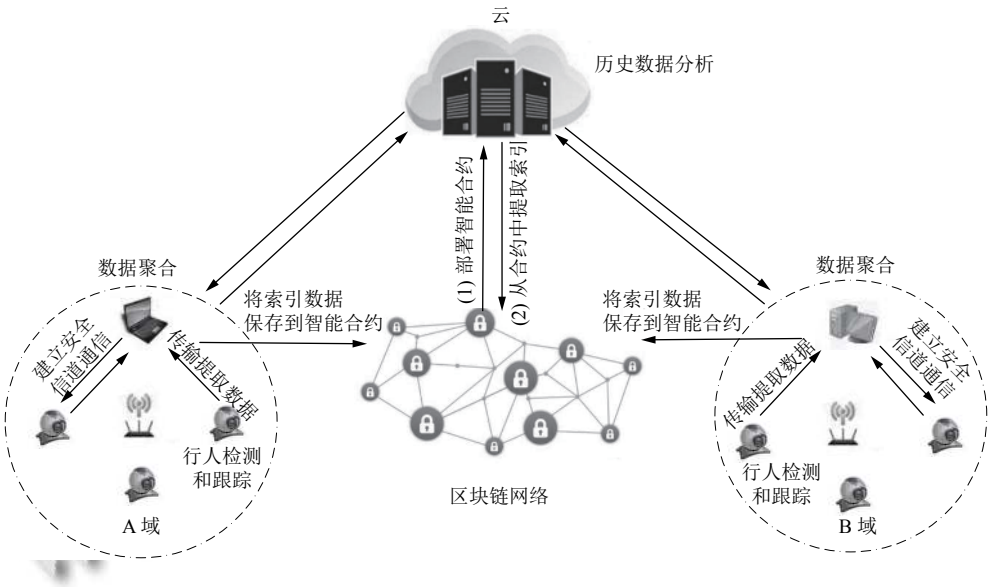

图 1 本文方案的框架结构

2.1 智能监控系统和安全数据传输

即时处理视频, 有助于更好地理解实时发生的事件. 监控摄像机捕捉视频, 并近实时地传输至边缘雾设备. 边缘设备与相机通过局域网 (LAN) 连接, 位于现场. 其将每个帧作为自动化异常检测机制的起始点.

在接收到视频帧后, 边缘设备负责提取低级特征以进行异常行为检测. 为支持异常行为检测或预测, 监控系统需要准确识别目标. 否则会造成异常漏检或高误警率. 实践中, 对于边缘设备来说, 运行人类、目标、车辆 (POV) 检测算法的负担较重, 因此在初始检测后可使用更轻量的跟踪器进行目标跟踪, 并在之后较长时间内执行检测. 人类目标的外观和场景照明条件存在差异, 因此该跟踪器应利用感兴趣目标进行在线训练. 快速可靠的跟踪器, 如核相关滤波器 (KCF)[11] 可利用在线跟踪确保实时的跟踪.

第 2 步是提取检测到的目标的特征. 特征可能包括速度、方向和其他一些描述指标, 例如目标可能拥有的特定姿态. 通过目标头部、肩膀、上臂和下臂的检测, 及其可能产生的角度来定义姿态. CNN 能够对人体部位进行分类, 将被检测到的人物的当前位置及其他特征将被保存为单独对象.

边缘节点将剩余步骤外包至雾节点或云数据中心, 例如特征情境化, 将特征分类为正常或异常实例, 以及保存信息以供未来参考等. 提取出特征后, 节点之间的信息传输就要求安全措施来确保信息的保密和完整.

边缘节点与雾节点的数据传输, 在以 AES 和 RSA 算法加密的安全通信信道上进行. 使用两种加密算法的优点在于, 提供了较短的密钥建立时间, 且能够更好地抵御网络嗅探攻击. 使攻击者无法拦截密钥的方式建立共享密钥加密. 使用雾节点的公钥对共享密钥进行加密, 并使用该加密数据向雾节点发送共享密钥, 以建立安全的共享密钥信道. 交换共享密钥的散列值, 以验证该密钥是否已经被建立. 这对信道效率的影响非常小, 因此可以建立双层加密信道. 图 2 给出了安全信道的建立过程, 其中包括以下步骤:

1) 边缘节点向雾节点发起握手消息;

2) 雾节点响应并回复公钥证书;

3) 边缘节点使用雾节点的公钥, 并发送加密后的共享密钥;

4) 雾节点使用其私钥, 对接收到的共享密钥进行解密. 其后, 雾节点将其计算出的共享密钥的散列值发送至边缘节点;

5) 边缘节点验证共享密钥散列值, 并发送确认消息. 由此, 建立安全信道并开始数据传输;

6) 一旦完成数据传输, 即终止连接, 并丢弃共享密钥 (未来不再使用). 有必要时, 利用新的共享密钥建立新的连接.

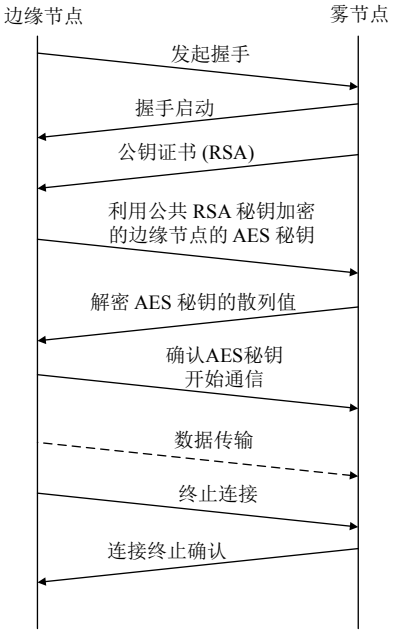

图 2 节点之间的双重加密通信

2.2 实时索引和面向事件的视频查询

在进一步的数据处理中可能不会使用边缘设备, 因为目标检测和跟踪已经消耗了大部分资源. 将每个视频帧中提取出的特征加密并发送至雾节点, 雾节点对特征解密并进行情境化, 将特征放入时空背景中. 举例来说, 在工作时间内一个人在大学办公区的大厅走到上行走是正常的, 但同样的行为发生在深夜的话则是可疑的. 除了在分类中使用以外, 在数据存储前进行情境化, 是搜索感兴趣的活动或事件的关键, 例如捕捉到某人出现在案发时间内的视频片段中.

因此, 将相机的地理位置、视频帧的时间或序列、帧内目标总数量及其姿态, 以键值 (Key-Value) 的方式记录为矩阵. 在每个给定帧中, 每个目标都有一组键, 且每个可调用的键都有一个指定数值. 这些信息将存储在雾节点上, 未来可根据键进行搜索. 实践中, 这些键成为索引数据, 用于快速搜索感兴趣信息. 类似地, 大数据存储管理系统利用相同方法并行搜索关键词数值, 使搜索速度更快[12].

一般可以使用索引表完成视频查询, 当搜索视频流中特定事件或活动时, 该特征非常有用. 实践中常见做法是慢慢观看录像, 找到事件发生的相关时刻, 通常会耗费大量的时间. 利用特征索引表, 能够通过查询字符串变量而非实际观看之前的视频文件, 有效节约查询视频的搜索时间. 一旦在雾节点中保存情境化数据, 则根据时间、位置或其他相关属性, 使用关键词将目标视频片段编入索引. 该方法可提供强大的搜索功能. 举例来说, 在时间和摄像机 ID 为已知的情况下, 场景中的目标速度可作为查询来使用.

2.3 基于区块链的认证机制

在雾层, 将边缘设备提取出的特征信息与背景数据相合并. 雾层与云端共享信息以执行高级任务. 本文提出了基于区块链的索引认证策略, 以支持去中心化、可扩展和安全的数据共享服务. 关键组件和操作如下:

1) 注册: 在区块链系统中, 每个实体必须创建至少一个主账户以加入网络, 该账户由密钥对定义. 从其自身的公钥中推导出每个账户的地址. 在图 1 的场景中, 利用唯一性账户地址作为虚拟身份标识 (VID), 在云服务器上实施身份验证和管理功能, VID 存储在由云维护的全局档案数据库中. 每个雾节点可向云端发送注册请求. 一旦与雾节点相关的身份信息通过验证, 利用其地址为每个注册实体建立档案, 用于将散列索引表数据传输到智能合约时的身份验证过程.

2) 智能合约部署: 智能合约负责管理散列索引表数据. 由索引认证策略持有方在区块链网络上开发并部署智能合约. 本文框架中, 由云充当数据持持有方和策略制定方, 能够部署封装了索引认证策略的智能合约. 在成功将智能合约部署到区块链网络后, 智能合约对整个网络是透明的. “透明”指的是区块链中所有节点均能够访问记录在链数据中的事务和智能合约. 通过区块链网络提供的密码和安全机制, 保护智能合约中所有协议和关系在无信任网络环境中免受第三方的恶意干涉. 每个节点可通过引用本地同步的链数据访问所有事务和智能合约最近状态, 并通过地址与公共远程过程调用 (RPC) 接口与智能合约进行交互.

3) 散列索引记录的生成: 为将散列索引记录成功保存到区块链, 雾节点首先向云端发送访问请求, 以获得执行智能合约的散列索引记录生成 ABI 的许可. 给定在档案数据库中建立的注册实体信息, 则策略制定模块通过强制执行预定义授权策略来评估请求. 若授予了访问请求, 云将启动一个事务, 以更新智能合约中的授权实体列表. 在事务通过核准并被记录在新区块

中之后, 云通知雾节点智能合约地址和 ABI, 以记录散列索引数据. 每当授权雾节点设备上有可用的散列索引记录时, 雾节点仅需与授权 ABI 交互即可在区块链上更新散列索引数据.

4) 索引认证: 索引认证过程由作为视频查询服务用户的授权实体执行, 本文研究中该授权实体为云节点. 若云操作人员希望对存储在雾节点上的视频查询数据进行验证, 其仅需检查定期同步的本地链数据中的合约的当前状态, 以得到散列键值索引记录. 云操作人员可以通过对计算出的记录索引表散列值和区块链中散列索引记录进行比较, 检验接收到的视频查询数据.

3 实验与分析

本文在现实物理网络环境中实施原型系统, 以验证提出系统的可行性. Solidity 是用于智能合约开发的一种面向合约的高级语言, 将区块链支持的索引认证机制转换为智能合约, 并部署在私有以太坊[13]区块链网络上. 利用 Python 将散列索引验证函数作为基于 Flask 框架的 Web 服务应用程序来实施.

3.1 测试平台设置

边缘设备为两块华硕卡片电脑主板, 其配置了 1.8 GHz 32 位四核 ARM Cortex-A17 CPU, 2 GB 的 LPDDR3 双通道内存, 操作系统为基于 Linux 内核的 TinkerOS. 在笔记本电脑上实施雾层, 其中配置了 2.3 GHz Intel Core i7 (8 核) 处理器, 16 GB 内存, 操作系统为 Ubuntu 16.04. 私有以太坊网络包括分布于四台桌面电脑的 4 名矿工, 桌面电脑配置为 3 GHz Intel Core TM (双核) 处理器和 4 GB 内存, 采用 Ubuntu 16.04 操作系统. 每名矿工使用两个 CPU 核心进行挖矿作业, 以维持私有区块链网络. 雾节点和矿工之间的数据传输通过加密信道进行. 在信道两端均使用基于 Python的套接字编程语言.

3.2 性能评价

一旦视频被传入边缘设备, 则利用轻量级 CNN 进行实时行人目标检测[14]. 对行人进行识别, 跟踪算法利用检测框来跟踪感兴趣目标, 直至目标离开视频帧. 跟踪器逐帧运行, 检测则每秒仅执行两次. 根据视频帧中行人的移动, 从感兴趣目标提取出特征. 本文研究中考虑了多个特征, 包括行人相对速度 (基于 1 s 内像素移动来计算) 和方向, 如图 3 所示. 将特征写入一个文件并发送至雾节点. 该文件中, 每行展示了时间戳、帧序列号、摄像机 ID、行人 ID, 图 4 展示了行人特征.

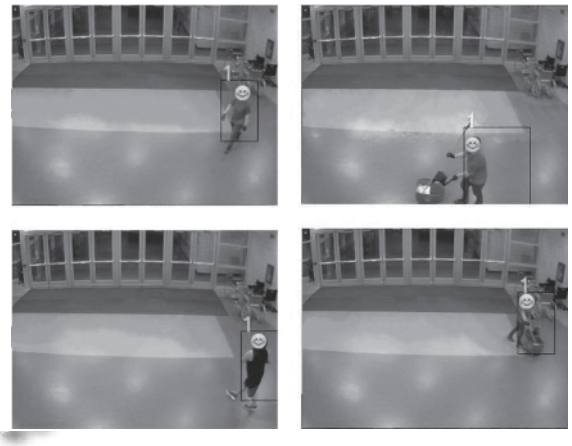

图 3 目标检测和跟踪的可视化

时间	相机 ID	序列号	目标数	中心	方向	方向
13. 0. 6	10	56	1	(189, 135)	东	1.303 840 481 04
13. 0. 6	10	57	1	(195, 136)	东	1.878 829 422 81
13. 0. 6	10	58	1	(204, 137)	东	2.751 363 298 44
13. 0. 6	10	59	1	(213, 136)	东	3.613 862 199 92
13. 0. 6	10	60	1	(220, 136)	东	3.687 817 782 92
13. 0. 7	10	61	1	(225, 146)	东	3.601 388 621 07
13. 0. 7	10	62	1	(232, 136)	东	3.7
13. 0. 7	10	63	1	(240, 135)	东	3.601 388 621 07
13. 0. 7	10	64	1	(249, 136)	东	3.601 388 621 07
13. 0. 7	10	65	1	(256, 136)	东	3.6
13. 0. 7	10	66	1	(261, 136)	东	3.6
13. 0. 7	10	67	1	(264, 135)	东	3.201 562 118 72
13. 0. 7	10	68	1	(272, 136)	东	3.2
13. 0. 7	10	69	1	(279, 137)	东	3.001 666 203 96
13. 0. 7	10	70	1	(284, 137)	东	2.801 785 145 22
13. 0. 8	10	71	1	(287, 136)	东	2.6
13. 0. 8	10	72	1	(290, 136)	东	2.601 922 366 35
13. 0. 8	10	73	1	(295, 136)	东	2.3
13. 0. 8	10	74	1	(300, 136)	东	2.102 379 604 16
13. 0. 8	10	75	1	(305, 137)	东	2.1
13. 0. 8	10	76	1	(307, 136)	东	2.0
13. 0. 8	10	77	1	(310, 136)	东	2.0
13. 0. 8	10	78	1	(312, 136)	东	1.7
13. 0. 8	10	79	1	(313, 138)	东	1.315 294 643 82
13. 0. 8	10	80	1	(315, 139)		1.019 803 902 72
13. 0. 8	10	81	1	(316, 140)		0.984 885 780 18

图 4 提取出的特征文件内容

1) 索引认证的计算开销: 在雾节点和边缘节点上执行索引认证测试, 以评估计算开销. 在测试过程中, 计算出 50 轮运行的平均延迟时长. 从图 5 的结果中可以发现, 查询索引令牌过程 (主要负责从智能合约中获取令牌数据) 在索引认证步骤中计算量最大. 由于雾节点的算力远超边缘节点, 在边缘节点上查询索引令牌的执行时间约为 53 ms, 在雾节点上的相同操作仅需 6 ms. 整个索引认证过程可分为两个步骤: 处理特征文件中的数据, 以及验证散列特征数据. 认证过程在边缘节点上的执行时间约为 2.3 ms (1.8 ms + 0.5 ms), 在雾节点上约为 0.3 ms (0.2 ms + 0.1 ms).

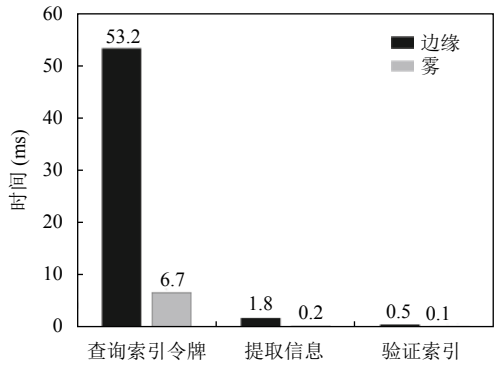

图 5 每个阶段的计算时间

2) 加密信道分析: 必须通过安全信道将文件从雾节点传输到挖矿 (边缘) 节点, 以避免被窃听. 例如中间人攻击、ARP 嗅探攻击等都可能会破坏保密性. 结果显示加入额外的加密层不会造成较多延迟, 数据传输速度相关抖动是网络流量造成的.

4 结束语

本文提出利用边缘-雾-云计算范式, 保护智能监控系统中节点之间交换的索引数据和特征数据. 在提出的分层架构中, 在边缘节点上提取视频帧的特征, 并通过安全信道传输至雾节点, 在雾节点上将特征情境化, 并保存到索引表内, 以提供面向事件的快速查询. 利用智能合约确保部署在边缘、雾和云层的节点之间通信的安全性, 智能合约利用索引表的散列值生成区块链网络中的下一个区块. 云可利用 Web 服务, 安全地获得节点上索引表和查询信息的访问权限. 实验结果表明, 提出的方法产生的开销非常低, 适用于面向事件的实时监控视频查询应用.

参考文献

1 曹利峰, 陈性元, 杜学绘, 等. 多级安全网络区域边界访问控制模型研究. 计算机工程与应用, 2011, 47(32): 118–122. [doi: 10.3778/j.issn.1002-8331.2011.32.035]

2 郭梓鑫, 衣杨, 李汉巨. 基于自适应特征融合的自然环境视频行为识别. 计算机学报, 2013, 36(11): 2330–2339.

3 徐洋, 孙建忠, 黄磊, 等. 基于 WiFi 定位的区域人群轨迹模型. 山东大学学报 (理学版), 2019, 54(5): 8–20.

4 余昊, 孙锬锋, 蒋兴浩. 基于光流块统计特征的视频异常行为检测算法. 上海交通大学学报, 2015, 49(8): 1199–1204.

5 Henriques JF, Caseiro R, Martins P, *et al*. High-speed tracking with kernelized correlation filters. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2015, 37(3): 583–596. [doi: 10.1109/TPAMI.2014.2345390]

6 杨超宇. 基于计算机视觉的目标检测跟踪及特征分类研究 [博士学位论文]. 北京: 中国矿业大学 (北京), 2017.

7 Aved AJ, Blasch EP. Multi-INT query language for DDDAS designs. Procedia Computer Science, 2015, 51: 2518–2532. [doi: 10.1016/j.procs.2015.05.360]

8 Chen N, Chen Y, Blasch E, *et al*. Enabling smart urban surveillance at the edge. Proceedings of 2017 IEEE International Conference on Smart Cloud. New York, NY, USA. 2017. 109–119.

9 Ouaddah A, Elkalam AA, Ouahman AA. FairAccess: A new blockchain-based access control framework for the Internet of Things. Security and Communication Networks, 2016, 9(18): 5943–5964. [doi: 10.1002/sec.1748]

10 喻辉, 张宗洋, 刘建伟. 比特币区块链扩容技术研究. 计算机研究与发展, 2017, 54(10): 2390–2403. [doi: 10.7544/issn1000-1239.2017.20170416]

11 张雷, 王延杰, 孙宏海, 等. 采用核相关滤波器的自适应尺度目标跟踪. 光学 精密工程, 2016, 24(2): 448–459.

12 Shafer J, Rixner S, Cox AL. The hadoop distributed filesystem: Balancing portability and performance. Proceedings of 2010 IEEE International Symposium on Performance Analysis of Systems & Software. White Plains, NY, USA. 2010. 122–133.

13 钱卫宁, 邵奇峰, 朱燕超, 等. 区块链与可信数据管理: 问题与方法. 软件学报, 2018, 29(1): 150–159. [doi: 10.13328/j.cnki.jos.005434]

14 李宗民, 邢敏敏, 刘玉杰, 等. 结合 Faster RCNN 和相似性度量的行人目标检测. 图学学报, 2018, 39(5): 901–908.