DOI：10.11830/ISSN.1000-5013.202204028

采用区块链的物联网数据共享方案

傅文龙[1,2]，李国刚[1,2]，解童[1,2]

（1. 华侨大学 信息科学与工程学院，福建 厦门 361021；
2. 华侨大学 厦门市专用集成电路系统重点实验室，福建 厦门 361021）

摘要： 针对物联网(IoT)数据共享过程中存在的安全漏洞和隐私泄露风险，提出一种基于区块链的物联网数据共享方案.采用数据的不可篡改、分布式存储、隐私保护、可追溯及访问控制，将消息队列遥测传输(MQTT)作为通信协议和中间件，并为其提供身份认证和主题权限管理.结合国产加密算法实现密钥交换、数据摘要和加密传输，通过区块链记录设备的行为，在提高可信度的同时提供追溯的能力，采用智能合约对数据和主题进行共享和管理，实现链上链下数据协同保障数据的一致性.通过系统原型实现与测试，结果表明：该方案能够确保物联网设备之间共享数据时的安全性和隐私性，满足物联网应用性能需求，具有可行性.

关键词： 区块链；物联网；智能合约；数据共享；消息队列遥测传输

中图分类号： TP 311.13；TP 319　　**文献标志码：** A　　**文章编号：** 1000-5013(2023)02-0257-07

Data Sharing Scheme for Internet of Things Using Blockchain

FU Wenlong[1,2], LI Guogang[1,2], XIE Tong[1,2]

(1. College of Information Science and Engineering, Huaqiao University, Xiamen 361021, China;
2. Xiamen City Key Laboratory of Application Specific Integrated Circuit System, Xiamen 361021, China)

Abstract: Aiming at the security vulnerabilities and privacy leakage risks in the process of internet of things (IoT) data sharing, a data sharing scheme for IoT based on blockchain is proposed. The blockchain is used to realize data tamper-proof, distributed storage, privacy protection, traceability and access control. The message queue telemetry transport (MQTT) is used as a communication protocol and middleware, and provides identity authentication and topic permission management for it. The key exchange, data synopses and encrypted transmission are realized by combining the domestic encryption algorithm. The behavior of the device is recorded through the blockchain, and the traceability is provided while improving the credibility. The smart contract is used to share and manage the data and topics, and the on-chain and off-chain data coordination is achieved to ensure the consistency of the data. Through the system prototype implementation and testing, the results show that the scheme can ensure the security and privacy of data sharing between IoT devices, and meet the performance requirements of IoT applications, which is feasible.

Keywords: blockchain; internet of things (IoT); smart contract; data sharing; message queuing telemetry transport

物联网(internet of things,IoT)将数以亿计的设备连接到互联网，使生活、生产更加智能、便利、高效和自动化，被广泛应用于各个领域[1].随着海量的物联网节点的接入及多源异构数据的爆炸式增长，物联网设备之间通过数据交换获取更丰富的信息，以便做出更加合理的决策，从而提高任务效率[2].同

收稿日期： 2022-04-26

通信作者： 李国刚(1973-)，男，副教授，博士，主要从事嵌入式系统设计、信息安全研究与实现、区块链、物联网应用的研究.E-mail:lgg@hqu.edu.cn.

基金项目： 国家自然科学基金资助项目(61370007)

时,物联网应用的指数级增长导致大量安全漏洞的出现,且大规模物联网系统数据在传输、处理和存储过程中的泄露会严重影响个人隐私,造成严重后果[3].物联网系统通常没有中央管理系统,缺乏记录物联网设备行为的良好基础设施,因此很难为设备生成信任评级及行为追溯[4].区块链作为一种分布式存储技术,可以为物联网中安全、隐私、可追溯性、可靠性和互操作性相关的问题提供解决方案[5].

目前,已有许多学者通过研究测试证明区块链技术能够使物联网系统具有更高的安全级别及更好的隐私保护能力,其中,包括构建区块链用作物联网设备身份认证和访问控制管理,结合聚合签名、密文策略属性基加密和同态加密等技术,以及与云存储相结合的混合架构来实现物联网安全共享数据[6-11].文献[12-13]的方案保障了数据的安全共享,但缺乏可靠的物联网设备及用户行为存证,并且授权信息得不到监管和记录,忽略了设备的共享效率.

综合上述讨论,本文提出一种采用区块链的物联网数据共享方案,将消息队列遥测传输(MQTT)作为物联网设备之间的通信协议和系统中间件,利用区块链和智能合约实现物联网设备的身份认证、访问控制、密钥管理及行为记录,采用链上链下协同[14]的方式共享数据.

1 系统架构

将MQTT协议作为设备之间的传输协议,实现物联网设备之间无需直接连接或同时在线就可交换数据,使用超级账本(hyperledger)搭建联盟链为数据存储和共享提供安全保障,通过智能合约实现区块链的应用接口,将系统中非敏感数据和敏感数据分别存储在关系型数据库管理系统(MySQL)和星际文件系统(IPFS)数据库中.设备之间通过发布和订阅的方式实时共享较小的数据,文档、图片、音频、视频等较大的敏感数据则通过数据库共享.文中方案的系统架构,如图1所示,主要包括区块链平台、智能合约、应用模块、设备、MQTT服务器及数据库.

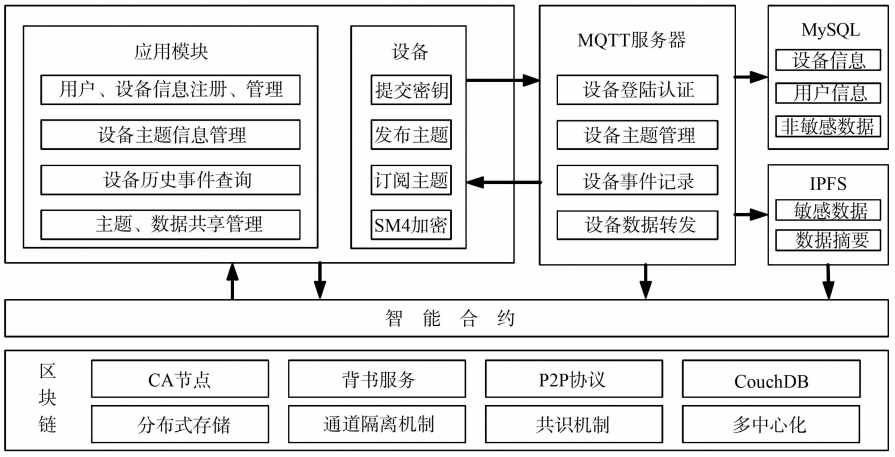

图1 文中方案的系统架构

Fig. 1 System architecture of proposed scheme

区块链是由多个组织共同参与维护的联盟链实现数据的多中心化分布式存储.由于MQTT协议运行于传输控制协议(TCP)之上,以明文方式传输,且缺少一些安全措施[15],为此,文中方案通过结合区块链技术为MQTT服务器添加了身份认证和访问控制,保障数据的安全传输和数据隐私,MQTT服务器负责物联网设备之间的数据转发及主题管理,会对设备的登录、退出、异常离线、发布主题、订阅主题及退订主题等操作执行智能合约上链记录,将设备信息、用户信息和在线状态等非敏感数据写入MySQL数据库中,将设备发布的加密后的敏感数据写入IPFS数据库中,并提取数据摘要和数据地址等信息上链存储.

应用模块主要包括用户和设备的注册管理、设备主题信息管理、设备历史事件查询和主题数据共享管理等功能.物联网设备中预设客户端身份标识号(ID)、用户签名和区块链服务器公钥,设备根据分组密码算法SM4生成通信密钥并使用服务器公钥加密,通过向MQTT服务器登录请求时提交密钥,将敏感数据经过SM4加密后由MQTT服务器进行转发.

2　物联网数据共享方案

2.1　网络结构

用户通过应用程序实现对智能合约的调用及对数据库的访问，物联网设备与 MQTT 服务器通信完成发布和订阅主题，MQTT 服务器利用智能合约执行服务器相关合约方法和数据上传，并将数据写入数据库. 系统网络结构，如图 2 所示. 应用程序和 MQTT 服务器采用远程过程调用(gRPC)协议与区块链节点通信，提交调用请求时需要认证由证书授权中心(CA)颁发的 X.509 数字证书的合法性和访问权限才能执行相应的合约方法，使用传输层安全性协议(TLS)来确保 gRPC 通信时传输层的安全性，设备与 MQTT 服务器进行通信时会对设备身份进行验证，同时开启 TLS 保障通信安全和数据完整性.

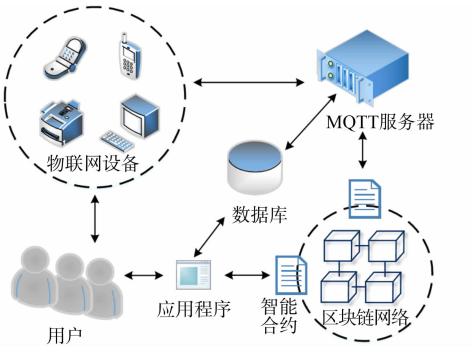

图 2　系统网络结构

Fig. 2　System network structure

2.2　智能合约

智能合约与账本一起构成了超级账本区块链系统的核心，在超级账本 Fabric 中智能合约又被称为链码(chaincode)，它是部署到 Fabric 中通道上实现业务逻辑的软件，能够执行读取、更改键值对及其他状态数据库操作的指令规则[16].

文中方案使用智能合约实现系统中物联网设备的注册和主题权限管理，MQTT 服务器的登录认证、设备行为记录、权限管理及数据的查询等功能，其智能合约函数，如表 1 所示.

表 1　智能合约函数

Tab. 1　Smart contract functions

函数名称	输入参数	功能描述
ConnectAuth	clientID, username, sign	客户端登录验证
ExchangeKey	username, sign, EnKey	上传客户端的通信密钥
ClientSubscribeAuth	clientID, topicName	客户端订阅主题权限验证
ClientSubscribe	clientID, subEvent, topic	上链客户端订阅记录
ClientConnect	clientID, conEvent, host	上链客户端连接记录
RegisterUserKey	username, random	创建 SM2 密钥对存储公钥
GetDisposableTopicHashToken	clientID, topic, time, target	获取订阅权限的一次性口令
GetDisposableDataHashToken	client, dataID	获取链下数据的一次性口令
AddPubTopicsForClient	clientID, topicMsgJson	为客户端添加发布主题信息
AddSubTopicsForClient	clientID, token	为客户端添加订阅主题权限
GetDataInformation	token	获取数据的通信密钥和摘要
UploadDataHash	clientID, SM3Key, DataID	上传客户端发布数据摘要

由于 Fabric 无法对智能合约中方法的执行进行权限管理，所以，在执行涉及物联网设备相关操作的函数时，为验证用户对设备操作的合法性，智能合约会对比用户所使用的 X.509 数字证书信息是否与该设备在区块链中存储的用户信息一致，MQTT 服务器在执行合约时则需要相应的管理员证书.

物联网设备信息在区块链中主要包括客户端标识、所属用户的名称、设备描述、订阅主题信息及发布主题信息. 其中，用户名称与用户在区块链组织中的名称一致并且与用户的 SM2 公钥为一对键值存储，设备发布主题和订阅主题中包含设备所发布和订阅的所有主题的信息. 发布主题信息包含主题公开标识、数据类型、数据说明及服务质量(QoS)，设备订阅主题信息以主题名称与订阅主题数据结构一一对应的集合存储. 订阅主题数据结构包括主题发布方的客户端标识和用户名、用于共享主题的一次性口令、主题订阅起始时间和截止时间，以及相应主题的发布信息.

物联网设备通过向 MQTT 服务器发送 clientID, username 和 password 3 个字段进行登录认证和密钥交换，其中，clientID 为设备在区块链中合法注册的客户端标识，username 为设备所属的用户名称，password 为用户私钥对客户端标识签名后得到的密文，服务器调用登录认证的合约方法，智能合约以 username 为键查询区块链账本获取对应用户的公钥，使用用户公钥验证 password 是否为私钥对 clien-

tID 签名后的结果,从而验证设备的合法性. 当服务器判断字段 clientID 满足〈用户名〉/〈通信密钥类型〉/〈客户端 ID〉对应的数据类型时,则执行对称密钥上传,这时设备上传的 username 为使用服务器公钥对通信密钥加密后的密文,智能合约先通过 clientID 字段中的用户名、客户端 ID 及 password 字段中的密文执行登录认证方法,确定设备的合法性后,使用服务器私钥解密 username,获取对称密钥并将其与 clientID 字段中的通信密钥类型上链存储,对于对称密钥的获取,需要验证合法用户的证书或得到相应资源的授权权限.

物联网设备在请求订阅主题时,MQTT 服务器会执行订阅主题权限验证,检查设备是否已获取该主题的订阅权限,用户可以通过添加订阅主题的方法为设备添加公开或非公开的主题,其中,执行方法的参数 token 为发布方提供的一次性共享口令.

2.3 系统流程

2.3.1 *用户、设备注册* 准备阶段中的设备注册流程,如图 3 所示. 应用程序发送随机数来注册用于管理物联网设备的用户身份,智能合约生成 SM2 非对称密钥对并返回私钥,以用户名为键存储公钥并与用户的区块链证书绑定,完成后用户便可以注册设备并预设设备 ID、用户私钥签名设备 ID 及服务器公钥. 设备通过向 MQTT 服务器发送包含预设的登录凭证及经过服务器公钥加密后的通信密钥,由 MQTT 服务器调用密钥上传的合约方法,以此实现在区块链中存储设备的通信密钥.

2.3.2 *设备访问控制* 物联网设备在登录 MQTT 服务器时,需要提交设备 ID、所属用户名及对设备 ID 的签名,服务器执行智能合约中的相关方法验证设备的合法性. 当验证成功后,智能合约会上链记录设备登录时间和互联网协议(IP)地址等信息,设备与服务器建立连接之后便可以发布和订阅,其中,发布的主题数据由服务器转发给其他设备并存储到数据库中,订阅主题时服务器同样通过智能合约审核订阅权限并上链记录. 设备访问控制流程,如图 4 所示.

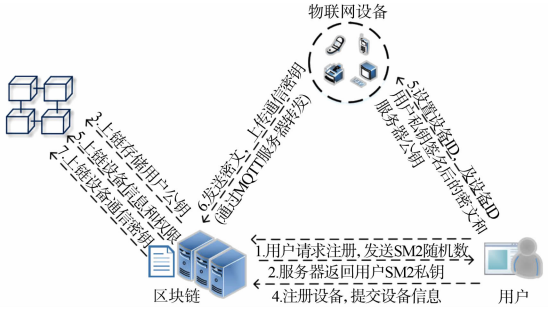

图 3 设备注册流程

Fig. 3 Equipment registration process

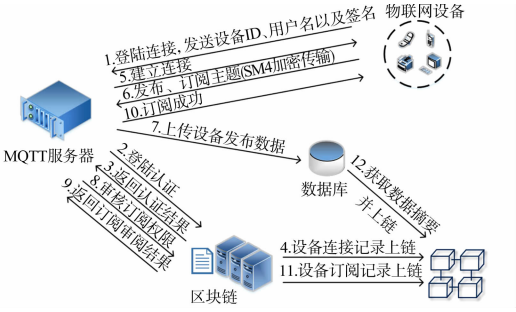

图 4 设备访问控制流程

Fig. 4 Equipment access control process

2.3.3 *主题、链下数据共享* 系统共享的数据资源主要包括 MQTT 的主题及数据库中存储的加密数据. 主题共享流程图,如图 5 所示. 用户 A 通过程序为物联网设备添加发布主题信息并获取用于订阅主题的一次性口令,用户 B 通过一次性口令为其设备添加订阅主题,当设备订阅主题时由智能合约决策设备的订阅权限同时上链记录,再由 MQTT 服务器转发数据.

数据共享流程,如图 6 所示. MQTT 服务器将设备发布的数据写入数据库,按条数打包成数据块并

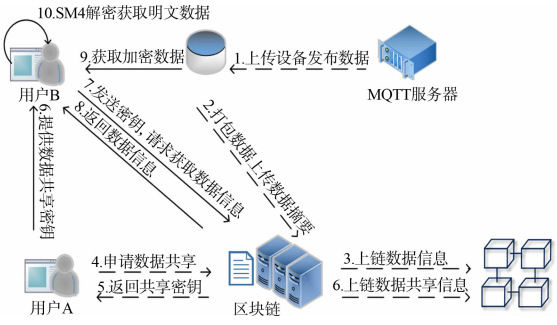

图 5 主题共享流程

Fig. 5 Subject sharing process

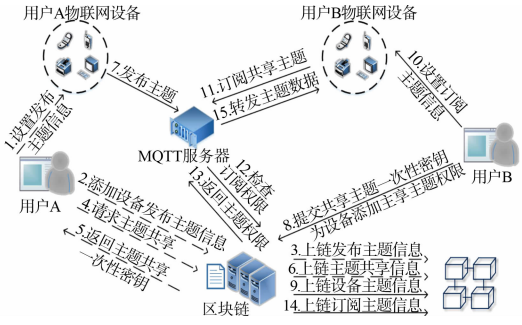

图 6 数据共享流程

Fig. 6 Data sharing process

提取 SM3 杂凑字串，与数据地址、时间范围等信息一起上传至区块链，以杂凑字串为键存储数据信息及通信密钥. 用户 A 向用户 B 提供包含数据摘要和通信密钥等信息的一次性数据共享口令来授权数据的访问权限，用户 B 便可通过数据地址获取加密数据，使用数据摘要验证数据完整性，再通过对称密钥解密获取明文数据.

3　安全性分析和性能测试

3.1　物联网数据共享方案对比

文献[10]所提方案利用密文属性策略基加密对数据进行加密后，同时存储在云平台和区块链中，用户从云平台获取加密数据解密后，对比区块链中的数据，保障其一致性. 文献[12]将物联网数据统一格式后存储在区块链帐本中，采用通道隔离的方式建立多账本和身份认证，实现数据访问管理. 区块链网络中的各个节点通常会备份所有账本数据，如果将物联网系统产生的所有数据都存储在区块链中，不仅会给各个节点带来严重的内存压力，查询数据所带来的时间开销也不利于数据的共享，为了提升共享效率、保护数据隐私及消除节点存储压力，采用链上链下协同存储，数据经过对称加密算法加密后，存储在 IPFS 中，数据摘要和加密数据存储地址等信息存储在区块链中，建立链上与链下数据的链接，同时保障数据的一致性. 文献[11]提出的方案中，由边缘服务器加密物联网数据后提交至云服务器中，同时在区块链中存储数据摘要，用户通过向云服务器提交访问请求获取解密后的数据. 文献[13]将 MQTT 代理作为中间件，处理物联网设备发送的请求，执行相应的合约方法，同时，将物联网设备发送的加密数据存储在分布式数据库中，通过区块链中存储的访问控制列表实现数据共享.

上述方案都实现通过区块链保障链下数据的共享安全，但无法满足部分物联网场景下设备实时共享数据的需求，因此，利用 MQTT 协议实时转发加密后的物联网数据，并且为保障数据的访问安全，设备和用户需要通过身份认证才能连接 MQTT 服务器和执行智能合约，通过合约实现访问控制及主题权限管理. 与其他方案相比，文中方案在架构设计上避免使用区块链直接存储或作为平台交换物联网数据，而是采用区块链来保护设备之间通过 MQTT 服务器交换数据过程中的安全性和隐私性，以此来保障物联网数据的共享效率，提供细粒化的数据访问控制，与此同时，将设备行为、数据共享记录及授权凭证上链存储以便追溯. 不同物联网数据共享方案的对比，如表 2 所示.

表 2　不同物联网数据共享方案的对比

Tab. 2　Comparison of different IoT data sharing schemes

方案	区块链平台	数据存储	数据访问	数据加密	授权方式	设备行为追溯
文献[10]	以太坊	链下、链上	访问控制	密文策略属性基加密	访问策略	无
文献[11]	Fabric	链上链下协同	访问控制	完全同态加密	访问策略	无
文献[12]	Fabric	链上	身份认证	非对称加密	通道隔离	无
文献[13]	以太坊	链上链下协同	身份认证＋访问控制	对称加密	访问策略	无
文中方案	Fabric	链上链下协同	身份认证＋访问控制	对称加密	一次性口令	支持

3.2　安全性分析

在安全方面，将国密算法 SM2，SM3 和 SM4 分别用作对称加密、哈希函数和非对称加密，数据使用对称加密算法加密，非对称加密用于设备身份认证及安全地交换对称密钥，链下数据提取哈希值存储在区块链中，以保证数据的一致性和完整性. 执行智能合约需要验证区块链中的合法身份，MQTT 协议和 gRPC 协议传输过程开启 TLS 提供保密性和数据完整性. 文中系统的安全特性具体如下.

3.2.1　防篡改　采用 Fabric 搭建多方共同维护的许可链，节点需通过验证登记证书和通信证书接入，大大降低了恶意节点入侵的风险，使用 Raft 崩溃容错共识算法实现分布式账本的一致性，允许故障节点数量在不多于正常节点的情况下工作. 通过节点共识、分布式账本等技术保证链上数据的不可篡改性，采用链上链下协同的存储方法，加密文件存储在链下，少量的文件信息存储在链上，链下数据通过链上数据进行检索；通信过程中，通过哈希检测保障数据完整性和一致性.

3.2.2　机密性　物联网设备通过非对称密钥将用于安全通信的对称密钥加密后上传至区块链中，只有使用服务器的私钥才能解密获得设备的对称密钥，设备之间通过对称密钥进行通信，数据库中存储的数

据也是经过对称密钥加密后的密文.在共享主题和加密文件时,用户需要通过授权的一次性口令获取主题订阅权限、数据地址及对称密钥,执行该操作需要区块链中的合法证书.

3.2.3 *身份验证* 用户在执行注册、查询及其他区块链操作时,通过 gRPC 协议与区块链节点通信并验证区块链用户证书.物联网设备在连接 MQTT 服务器之前,需要用户进行注册并在设备中预设登录凭证,设备通过向服务器提供签名密文验证设备连接的合法性.

3.2.4 *权限管理* 通过对物联网设备订阅主题的权限控制,避免越权访问、发布恶意内容和订阅主题捕获数据等攻击;对用户执行物联网设备信息修改、增加主题和共享数据等操作,合约会检验其是否为相关设备所属的合法用户;用户只能通过数据所属方提供的一次性共享密钥来添加主题的订阅权限和获取链下存储的数据.

3.2.5 *行为追溯* 物联网设备连接服务器、交换密钥和订阅主题等操作的信息均会存储在区块链中,数据共享和获取行为也将在区块链中永久留痕,区块链中的所有节点都将存储行为记录,使记录难以被篡改,从而提供可靠的行为追溯.

3.3 性能测试

为了验证文中方案的可行性,使用 Fabric 2.2 和 Golang 语言实现方案原型,将 1 台 2 核、4 GB 内存、80 GB 固态硬盘(SSD),Ubuntu Server 18.04.1 LTS 64 bit 操作系统的腾讯云应用服务器作为服务端;将 1 台 Windows 10 操作系统的笔记本电脑作为客户端.测试环境中,区块链是由 2 个组织组成的联盟链,通过 Docker 部署 4 个 Peer 节点及 1 个 Order 节点,将 CouchDB 作为存储方式.

性能测试主要研究系统处理不同事件的时延和吞吐量(TXN(事件数)·s^{-1}),物联网设备之间共享数据的效率主要取决于 MQTT 服务器的性能,测试中所采用的 MQTT 服务器通过发布订阅进行数据交换的饱和吞吐量达到 70 000 TXN·s^{-1},MQTT 服务器查询区块链数据的饱和吞吐量为 2 700 TXN·s^{-1},文献[12]和文献[13]的方案分别以 Fabric 和以太坊作为数据的共享平台,其吞吐量分别为 60,0.54 TXN·s^{-1}.

系统中的时间开销主要用于设备身份认证和密钥交换,对 MQTT 登录认证进行测试,其登录认证时延,如图 7 所示.图 7 中:N 为并发数;t 为登陆请求响应时延.在 20 个并发请求下,时延为 277 ms,饱和吞吐量可以达到 420 TXN·s^{-1}.

密钥交换涉及区块链账本的查询、修改及 SM2 验签和私钥解密,是方案中最耗时的合约方法.交换密钥时延,如图 8 所示.在 20 个并发数下,时延为 480 ms,饱和吞吐量为 100 TXN·s^{-1}.

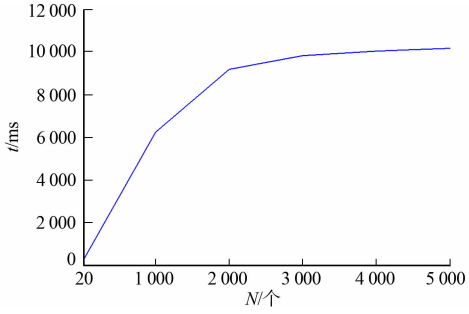

图 7 登录认证时延

Fig. 7 Login authentication delay

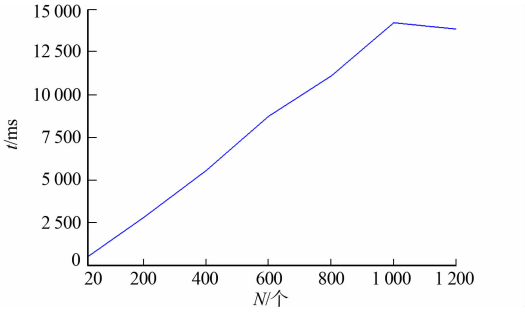

图 8 交换密钥时延

Fig. 8 Exchange key delay

4 结束语

针对物联网数据共享过程中存在的安全漏洞、隐私泄露风险及共享灵活性不足等问题,提出一种采用区块链的物联网数据共享方案.利用链上链下协同的方式存储和共享数据,将 MQTT 作为物联网设备之间的通信协议和系统中间件,实现物联网设备交换数据时,无需互相连接或同时在线,只需要连接同一个利用智能合约进行身份认证的可信 MQTT 消息代理,从而保障数据共享过程的安全性.采用智能合约实现设备主题管理和链下数据共享,并记录设备的连接、离线及订阅等历史操作以便追溯,通过加密算法保障共享数据过程中的一致性和隐私性.在下一步研究中,将对物联网设备的访问控制和资源

管理的细粒化进行研究，在保证安全性和有效性的前提下，进一步提高数据的共享效率.

参考文献：

[1] ALAM N，VATS P，KASHYAP N. Internet of Things：A literature review[C]// Recent Developments in Control，Automation and Power Engineering. Noida：IEEE Press，2017：192-197. DOI：10.1109/RDCAPE.2017.83582 65.

[2] MOHANTY J，MISHRA S，PATRA S，*et al*. IoT security，challenges，and solutions：A review[C]// Progress in Advanced Computing and Intelligent Engineering. [S. l.]：Springer，2021：493-504. DOI：10.1007/978-981-15-6353-9_46.

[3] SAXENA S，BHUSHAN B，AHAD M A. Blockchain based solutions to secure IoT：Background，integration trends and a way forward[J]. Journal of Network and Computer Applications，2021，181：103050. DOI：10.1016/j.jnca.2021.103050.

[4] WANG Qin，ZHU Xinqi，NI Yiyang，*et al*. Blockchain for the IoT and industrial IoT：A review[J]. Internet of Things，2020，10：100081. DOI：10.1016/j.iot.2019.100081.

[5] UMER M，IBRAR Y，KHALED S，*et al*. Blockchain for IoT-based smart cities：Recent advances，requirements，and future challenges[J]. Journal of Network and Computer Applications，2021，181：103007. DOI：10.1016/j.jnca.2021.103007.

[6] BANOUN N，DIARRA N. Authentication of mobile IoT devices using hyperledger fabric blockchain[C]// Eighth International Conference on Software Defined Systems. Gandia：IEEE Press，2021：1-6. DOI：10.1109/SDS54264.2021.9732141.

[7] HOU Mingyu，KANG Tianyu，GUO Li. A blockchain based architecture for IoT data sharing systems[C]// IEEE International Conference on Pervasive Computing and Communications Workshops. Austin：IEEE Press，2020：1-6. DOI：10.1109/PerComWorkshops48775.2020.9156107.

[8] SULTANA T，ALMOGREN A，AKBAR M，*et al*. Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices[J]. Applied Sciences，2020，10(2)：488. DOI：10.3390/app10020488.

[9] MANZOOR A，BRAEKEN A，KANHERE S S，*et al*. Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain[J]. Journal of Network and Computer Applications，2021，176：102917. DOI：10.1016/j.jnca.2020.102917.

[10] 杨业平，林德威，黄芳芳，等. 基于区块链的物联网安全数据共享系统[J]. 福州大学学报(自然科学版)，2021，49(6)：739-746. DOI：10.7631/issn.1000-2243.21326.

[11] SUN Shuang，DU Rong，CHEN Shudong. A secure and computable blockchain-based data sharing scheme in IoT system[J]. Information (Switzerland)，2021，12(2)：47. DOI：10.3390/info12020047.

[12] 于金刚，张弘，李姝，等. 基于区块链的物联网数据共享模型[J]. 小型微型计算机系统，2019，40(11)：2324-2329. DOI：10.3969/j.issn.1000-1220.2019.11.015.

[13] CARVALHO K，GRANJAL J. Security and privacy for mobile IoT applications using blockchain[J]. Sensors，2021，21(17)：5931. DOI：10.3390/s21175931.

[14] 梁秀波，吴俊涵，赵昱，等. 区块链数据安全管理和隐私保护技术研究综述[J]. 浙江大学学报(工学版)，2022，56(1)：1-15. DOI：10.3785/j.issn.1008-973X.2022.01.001.

[15] HINTAW A J，MANICKAM S，ABOALMAALY M F，*et al*. MQTT vulnerabilities，attack vectors and solutions in the internet of things (IoT)[J/OL]. IETE Journal of Research，2021：1-30. [2022-04-19]. https：// doi. org/10.1080/03772063.2021.1912651.

[16] ZOU Weiqin，LO D，KOCHHAR P S，*et al*. Smart contract development：Challenges and opportunities[J]. IEEE Transactions on Software Engineering，2019，47(10)：2084-2106. DOI：10.1109/TSE.2019.2942301.

（责任编辑： 黄晓楠　　**英文审校：** 吴逢铁）