DoTI：面向数据业务的TEE融合技术研究

马承彦[1]，卢笛[2]，马鑫迪[1]，习宁[1]，王锦锦[3]，马建峰[1]
（1.西安电子科技大学网络与信息安全学院，陕西 西安 710071；
2.西安电子科技大学计算机科学与技术学院，陕西 西安 710071；
3.伯明翰大学计算机科学学院，英国 伯明翰 B15 2TT）

摘　要：协同平台面临系统和数据安全的挑战，可信执行环境（TEE）通过硬件隔离技术实现基于明文的机密计算，确保代码和数据的机密性与完整性。然而，异构的TEE技术使得同一份代码或程序无法直接在不同TEE架构中直接运行并相互提供可信的数据操作接口，导致跨TEE场景下任务协同执行的安全问题。为了解决上述问题，提出一种基于数据操纵语言的TEE融合技术DoTI，从数据处理的业务层解决跨TEE的数据安全交互问题，并结合基于属性加密的密码学方法保持多TEE协同的隔离性。实验结果表明，在DoTI环境下迁移至TEE的数据库性能约为原始数据库的119.15%，且网络通信能力优于现有方案，能够满足协同平台数据共享的可用性和安全性要求。

关键词：协同平台；可信执行环境；数据操纵语言；基于属性的加密
中图分类号：TP309
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025002

DoTI: research on data-oriented TEE integration technology

MA Chengyan[1], LU Di[2], MA Xindi[1], XI Ning[1], WANG Jinjin[3], MA Jianfeng[1]
1. School of Cyber Engineering, Xidian University, Xi'an 710071, China
2. School of Computer Science and Technology, Xidian University, Xi'an 710071, China
3. School of Computer Science, University of Birmingham, Birmingham B15 2TT, UK

Abstract: Collaborative platforms face the challenges of system and data security. Trusted execution environment(TEE) implements plaintext-based confidential computing through hardware isolation technology, ensuring the confidentiality and integrity of code and data. However, heterogeneous TEE technologies lead to security issues in data interoperability across TEE. To address the aforementioned issues, a TEE integration technology based on data manipulation language was proposed, combined with the cryptography method of attribute-based encryption to maintain the isolation of TEE. The experimental results show that the performance of the database migrated to TEE in DoTI is about 119.15% of the original database, and the network communication performance is better than existing solutions, which can meet the availability and security of data sharing in the collaborative platform.

Keywords: collaborative platform, trusted execution environment, data manipulation language, attribute-based encryption

收稿日期：2024–05–13；**修回日期：**2024–11–07
通信作者：卢笛，dlu@xidian.edu.cn
基金项目：国家重点研发计划基金资助项目（No.2023YFE0111100）；国家自然科学基金资助项目（No.62232013, No.62220106004, No.92167203, No.92267204, No.62402364）；陕西省重点研发计划基金资助项目（No.2023-ZDLGY-52）
Foundation Items: The National Key Research and Development Program of China (No.2023YFE0111100), The National Natural Science Foundation of China (No.62232013, No.62220106004, No.92167203, No.92267204, No.62402364), The Key Research and Development Program of Shaanxi Province (No.2023-ZDLGY-52)

0　引言

跨设备的数据共享已成为云服务、物联网、集群系统等协同平台中的关键功能。为应对协同平台[1]中的系统和数据安全问题，机密计算逐渐成为确保这些平台的敏感代码和数据安全运行的重要手段。其中，基于硬件隔离技术的可信执行环境（TEE, trusted execution environment）[2-3]实现基于明文的机密计算，确保计算过程中代码和数据的机密性和完整性。与基于密码学的机密计算方法[4-5]不同，TEE通过提供一个硬件级的执行环境，将敏感代码和数据与外部威胁隔离，从而支持基于明文的代码执行和数据处理，避免复杂密码学算法对系统可用性和实时性的影响，同时实现对复杂数据处理逻辑的支持。然而，协同平台中的大量异构设备导致异构TEE并存，且不同设备采用不同的TEE技术，如Intel SGX[6]、ARM TrustZone[7]、AMD SEV[8]等。不同TEE技术具有不同的开发套件、编程接口和运行环境，使得同一可信应用（TA, trusted application）在不同设备上执行前需要进行源码修改、重新编译和平台适配，这为TA在不同TEE平台上的迁移和运行带来了巨大挑战。由于缺乏统一的远程证明协议，各TEE的可信机制仅信任本地TA的执行结果。因此，如何打破异构TEE之间的壁垒，建立逻辑统一的TEE环境，实现TA在异构TEE之间的无缝迁移及跨设备的数据安全互操作，成为构建安全协同平台的关键挑战之一。

当前，关于如何统一异构TEE的研究主要包括设计跨平台TEE中间件和构建可信程序开发生态环境两方面。其中，跨平台TEE中间件通过屏蔽底层硬件架构的差异，抽象化异构TEE的服务接口，为TA搭建可调用多种TEE资源的虚拟执行环境，使不同开发架构的TA能够直接在虚拟机中运行。Jia等[9]提出HyperEnclave，利用虚拟化技术实现跨平台的可信执行环境，打破了不同平台之间的TEE开发壁垒，并为现有SGX Enclave程序提供了转换中间件，使原有程序在不改动或少量修改后可以在HyperEnclave中运行。Galanou[10]设想通过基于容器状态为用户提供虚拟TEE的远程证明。Han等[11]基于ARM Hypervisor组件搭建MyTEE，兼容OP-TEE安全操作系统，并基于可信平台模块（TPM, trusted platform module）提供远程证明服务。在可信程序开发生态构建方面，通过集成化异构TEE的开发环境，使得同一份代码能够直接部署至不同TEE运行。基于此，开源社区OpenEuler开发了机密计算框架secGear[12]，利用代码辅助生成工具，使开发者可以忽略平台差异，由一套代码通过编译器生成可在不同TEE架构上直接运行的TA。Scopelliti等[13]为异构TEE提供Rust和C语言编译器，以保证分布式系统中数据处理的真实性和完整性。Karanjai等[14]利用区块链技术为异构的TEE设备提供远程证明服务，并为计算任务有效分配TEE资源。然而，上述方法大多依赖于Intel、AMD等处理器的特殊硬件支持，并且需要复杂的系统或编译器设计，难以在嵌入式平台上直接应用。此外，由于嵌入式系统种类繁多、配置各异，构建涵盖所有平台类型的中间件或生态环境工作量大、成本高昂，难以满足通用性需求。

然而，协同平台设备间交互的本质是数据的流动，而这些数据流动大多可以通过数据操纵语言（DML, data manipulation language）的驱动来实现。例如，关系型数据库系统中的SQL[15]就是一种DML，通过预定义的指令实现数据的本地或跨设备操作。目前，DML已被广泛应用于车联网[16]、工业互联网[17]、数字金融[18]、无人机集群[19]等领域。由于DML采用某种统一的语法规则，具有平台无关性，且能够实现对数据的增、删、查和改等基本操作，因此能够满足大部分业务对数据操作的需求。基于DML的上述特性，本文从数据业务的角度出发，采用DML将统一异构TEE的问题转化为数据业务层TA间DML的互操作问题。同时，利用平台无关的DML安全交互，消除由TEE异构性导致的TA难以迁移和安全互操作的问题，避免了从操作系统、编译器等复杂系统层面来解决跨TEE可信应用迁移的问题（即构建逻辑上统一TEE的问题）。此外，基于属性的加密（ABE, attribute-based encryption）[20]技术确保逻辑统一后的TEE仍具备强隔离性，本文主要贡献如下。

1) 从数据业务层面出发，构建基于DML面向数据业务的异构TEE安全融合（DoTI, data-oriented TEE integration）架构，实现TA在异构TEE间的无缝迁移和安全互操作。

2) 针对异构TEE缺乏统一可信证明技术的问题，提出一种基于ABE的群组密钥协商协议。通过以TEE可信根为加密属性，实现不同设备间的

身份认证，并构建可信域。数据的跨设备访问和共享操作仅限于可信域内，确保了DoTI的高度隔离性。

3) 基于上述研究内容，本文以当前主流DML-SQL为例，在由Raspberry Pi 3B、Hikey等异构设备组成的集群平台上，采用OP-TEE和内建于TEE的安全数据库系统实现了原型系统。

1 预备知识

1.1 TEE可信根

TEE可信根[21-22]是指在TEE中建立的基础安全性组件，通过提供硬件级别的安全保障，保护应用程序和数据免受恶意软件、物理攻击和侧信道攻击等威胁。可信根通常由硬件制造商或安全芯片生产厂商直接提供，并经过严格的验证和认证，以确保其安全性和可靠性，其主要功能包含以下4个方面。

1) 提供根密钥和身份认证服务：可信根为系统提供唯一的标识信息，该信息由硬件厂商固化在设备中，可作为根密钥使用，也可用于设备身份的识别。

2) 安全启动和认证：确保TEE启动过程的完整性和安全性，以防止其他干扰。

3) 安全存储和密钥管理：提供安全的存储空间，用于存储敏感数据和密钥，确保只有经过授权的应用程序能够访问这些数据。

4) 可信执行环境的管理：负责管理TEE中运行的可信程序，包括验证程序的完整性，确保其不会对系统安全构成威胁。通过基于硬件的安全保护，TEE可以直接处理明文数据，从而有效保障计算方案的通用性和性能。

1.2 DML

DML是一种用于数据库操作的编程语言，提供了数据增、删、查和改等基本功能。以面向RDBMS的SQL语言为例，其核心命令包括CREATE、INSERT、UPDATE和DELETE。通过JDBC（java database connectivity）统一的数据驱动接口，开发者可以使用标准SQL语法与不同的RDBMS进行交互，使跨数据库操作更加灵活和便捷。

针对非关系型数据库，一些研究者构建了异构分布式数据库管理系统HD-DBMS[23]，并设计了多库操作语言SMSQL[24]。通过屏蔽底层异构数据库的执行细节，SMSQL能够在不同架构的数据库之间实现便捷的数据查询与传递。

1.3 Hash函数

定义1 Hash函数[25]。Hash函数是一种将任意长度的消息映射为某一固定长度消息的函数，其输出称为数据消息的摘要。一个Hash函数$h:X\to Y$需要满足以下3个安全性要求。

1) 单向性：对于任意给定的$y\in Y$，寻找使$h(x)=y$成立的$x\in X$在计算上是困难的。

2) 弱抗碰撞性：已知$x\in X$，寻找$x'\in X$使$x\neq x'$且$h(x)=h(x')$在计算上是困难的。

3) 强抗碰撞性：寻找2个不同的$x\in X$与$x'\in X$使$h(x)=h(x')$在计算上是困难的。

通过计算数据使用Hash函数的摘要值，可以验证数据的完整性。

1.4 双线性映射

定义2 双线性映射[20]。假设G_1、G_2、G_T是3个阶为素数p的循环群，双线性映射e: $G_1\times G_2\to G_T$满足以下3个性质。

1) 双线性：对于$\forall g_1\in G_1, g_2\in G_2$，且$a,b\in Z_p^*$，有$e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$。

2) 非退化性：$e(g_1,g_2)\neq 1$。

3) 高效计算：对于$\forall g_1\in G_1, g_2\in G_2$，$e(g_1,g_2)$均可以高效计算。

若$G_1\neq G_2$，称映射e为非对称双线性映射；若$G_1=G_2$，称映射e为对称双线性映射。

1.5 基于属性的加密算法

基于属性的加密算法是一种实现访问控制的加密技术，数据所有者可以根据接收者的属性对数据进行加密，使得只有属性符合要求的用户能够成功解密密文[20]。为了使基于属性的加密支持更灵活的访问控制策略，Bethencourt等[26]提出基于密文策略的属性加密（CP-ABE, ciphertext-policy ABE）。CP-ABE将访问策略嵌入密文中，每个用户拥有自身的属性密钥，只有当用户属性符合密文中嵌入的访问策略时，才能解密密文。CP-ABE主要包含以下4个算法。

1) Setup：只接受隐式安全参数作为输入，生成公共参数PK和主密钥MK。

2) KeyGen(MK, S)：使用主密钥MK和属性集合S生成属性密钥SK。

3) Encrypt(PK, msg, A): 加密算法利用公共参数

PK、访问策略A对明文msg进行加密，生成密文CT。访问策略A规定数据接收者的属性，例如，访问策略$A=\{a_1 \vee (a_2 \wedge a_3)\}$表示能够解密密文的用户需满足拥有属性$a_1$或同时拥有属性$a_2$和$a_3$。

4) Decrypt(CT, SK)：当生成密钥时的属性集合S满足密文CT中嵌入的访问策略A时，则用户可成功解密密文。

CP-ABE通过基于属性条件定义访问控制规则，并根据用户的变化更新属性，从而实现动态的访问权限管理。将CP-ABE用于群组密钥管理，可以确保群组成员之间的安全通信。不同的属性被分配给不同的用户，使得只有满足特定属性条件的用户才能解密群组密文或获取群组密钥。

2　系统模型

本文从数据业务层面出发，利用DML提出一种基于数据驱动的异构TEE融合架构DoTI，如图1所示。该架构中每台主机包含运行在非可信执行环境（REE, rich execution environment）中的应用程序以及运行在TEE内的数据库系统。

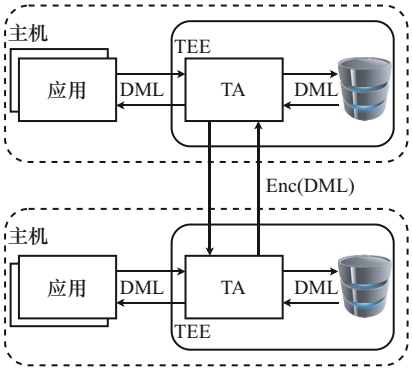


图1　基于数据驱动的异构TEE融合架构DoTI

在DoTI架构中，应用程序对数据的采集、处理、传输和存储等操作均通过DML命令序列传递至TEE内完成。异构设备间则通过TEE内TA生成的加密DML实现机密数据的传输，从而实现跨设备的数据访问。由于TA仅负责处理不同业务的DML脚本，且DML作为一种解释型语言无须在执行前进行编译，因此，该场景下的跨TEE数据操作实质上被转化为跨TEE的DML操作，规避了操作系统及TEE异构性带来的问题。

此外，由于所有明文数据的处理均在设备的TEE中进行，而传输和存储操作仅涉及密文数据，这一架构确保了跨设备数据全生命周期的安全性。

3　系统实现

3.1　单设备TEE架构

如图2所示，在数据采集和处理阶段，位于TEE内的嵌入式数据库引擎、AI算法等数据处理模块可以通过共享内存从REE侧读取密文数据，并在TEE中解密后直接进行明文数据操作。目前，已有一些研究探索了内嵌于TEE的安全数据库，例如，基于Intel SGX的CryptSQLite[27]和基于ARM TrustZone的BiTDB[28]等。这些数据库通过在可信环境中提供明文检索服务，代替非可信环境下基于密码学的机密计算方案[29]，显著提高了加密数据库的业务覆盖范围和执行效率。

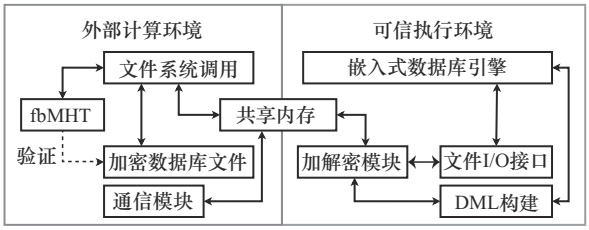


图2　单设备TEE及加密数据库架构

当TEE需要与外部设备交互数据时，DML生成器会根据业务需求构建SELECT查询命令或INSERT、UPDATE等数据修改命令，并通过加解密模块对其加密后，以密文形式传输至其他设备的TEE中。由于明文数据处理全部在TEE内完成，而TEE外的数据均以密文形式存在，无论数据位于REE还是TEE，其机密性和完整性均能得到有效保障。

设备中处理完毕的数据通过TEE加密后，以列级加密或页级加密的形式存储在系统资源丰富但安全性较低的REE中。为确保数据的完整性，构建基于文件的默克尔哈希树（fbMHT, file-based Merkle Hash tree）[29]。该树形结构由数据库文件的基本单元——页，通过两两合并哈希自底向上生成，并与数据库文件一起以密文形式存储在REE侧文件系统。当数据库引擎执行查询操作时，相关页的哈希值在TEE内重新进行计算，并与fbMHT中存储的值进行校验，以确保查询结果未被篡改。对于更新操作，系统首先验证被更新页的完整性，确定未被篡改后，重新计算这些页面的哈希值，并完成对哈希树的更新。

3.2　基于属性加密的可信域构建

在确保终端设备数据安全的前提下，通过融合TEE可以为协同平台构建逻辑上统一的机密计算环境。通过将TEE作为系统可信根，完成设备身份认证和群组密钥协商，并构建可信域，可以将非法设备排除在群组外，确保融合后TEE的隔离性。传统的一对一远程证明方案在协同平台内处理大量并发认证请求（如蜂群无人机、战场信息汇聚等场景）时，可能由于拥塞概率增大使得认证时延增加，服务质量显著下降。借助CP-ABE算法实现TEE间的高效交互验证，可以为整个协同平台快速建立逻辑上统一的可信根和可信执行环境[30]。

本节以协同平台中终端设备与地面、空中数据中心构成的云系统TEE互认证为例，说明本文方案对融合后TEE隔离性的保护作用。图3展示了TEE融合的过程，在初始化阶段，终端设备在可控的网络环境下接收地面数据中心分配的认证材料，以提高设备在后续集群作业中的认证效率[31]。在协同作业期间，终端设备处于非安全无线网络环境时，可基于自身TEE的可信根和认证材料，借助空中数据中心接收群组会话密钥。最终，所有具备群组会话密钥的设备构成一个可信域，实现安全的跨设备数据访问。

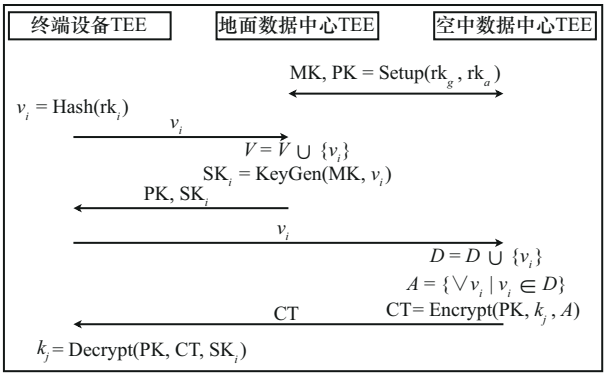


图3　TEE融合的过程

在初始化阶段，由地面数据中心和空中数据中心联合构成的认证云系统为管域内的终端设备分配可信认证材料，具体步骤如下。

1) 地面数据中心和空中数据中心基于各自的TEE根密钥rk_g和rk_a，共同协商生成主密钥MK和公共参数PK

$$\mathrm{MK,PK} = \mathrm{Setup}\left(\mathrm{rk}_g,\mathrm{rk}_a\right) \tag{1}$$

其中，MK和PK分别为

$$\mathrm{MK} = \{ g^x \} \tag{2}$$

$$\mathrm{PK} = \left\{ e(g,g)^x \right\} \tag{3}$$

2) 终端设备在协同行动前，通过地面机密信道，向地面数据中心提交由自身TEE根密钥rk_i利用Hash函数生成的唯一编号v_i

$$v_i = \mathrm{Hash}\left(\mathrm{rk}_i\right) \tag{4}$$

3) 地面数据中心收到终端设备传输的v_i后，将其添加至认证云的设备集合V中。随后，生成随机数s，并使用CP-ABE密钥生成算法KeyGen生成SK_i。地面数据中心通过地面机密信道将SK_i和PK反馈至终端设备

$$\mathrm{SK}_i = \mathrm{KeyGen}\left(\mathrm{MK},v_i\right) = g^{v_i x + s} \tag{5}$$

在任务执行阶段，假定所有终端设备均已完成初始化。终端设备定期向临近的空中数据中心或地面数据中心汇报自身的身份信息v_i，那么一个数据中心管域内的所有终端设备将构成一个设备群D。数据中心生成一个随机串k_n，并通过连续运用Hash函数生成剩余的密钥值，最终构成群组会话密钥串为

$$\mathrm{key} = \{ \cup k_j | k_j = \mathrm{Hash}\left(k_{j+1}\right), j = n-1, n-2, \cdots, 0 \} \tag{6}$$

最后，利用CP-ABE算法通过无线信道将密钥安全地分发给管域成员，具体步骤如下。

1) 数据中心收集一个时间段内终端设备报送的身份信息v_i，并通过设备集合V校验v_i的合法性。如果$v_i \in V$，则将其添加至数据中心管辖的设备群D。

2) 当设备群D中的成员发生变动或到达群组密钥更新时间时，数据中心按照从k_0到k_n的顺序选择群组会话密钥，并利用CP-ABE算法对密钥进行加密，生成密文消息CT为

$$\mathrm{CT} = \mathrm{Encrypt}\left(\mathrm{PK},k_j,A\right) = \left\{ C_i = k_j e(g,g)^{(v_i x + s)r}, L = g^r, A \right\} \tag{7}$$

其中，参数A为密文消息CT的访问控制策略，表示为$A = \left\{ \vee v_i | v_i \in D \right\}$。

3) 数据中心向管域内的终端设备广播密文消息CT，终端设备收到CT后，通过访问策略A验证

其是否为合法群成员。若验证通过，则解密消息CT；否则，等待下一轮密钥广播。验证过程为

$$k_j = \mathrm{Decrypt}\left(\mathrm{PK},\mathrm{CT},\mathrm{SK}_i\right) = \frac{C_i}{e\left(\mathrm{SK}_i,L\right)} = \frac{k_j e\left(g,g\right)^{\left(v_i x+s\right)r}}{e\left(g^{v_i x+s},g^r\right)} = \frac{k_j e\left(g,g\right)^{\left(v_i x+s\right)r}}{e\left(g,g\right)^{\left(v_i x+s\right)r}} = k_j \tag{8}$$

4) 终端设备解密得到新的群组密钥k_j后，根据原群组密钥k'验证k_j的正确性，即判断式(9)是否满足条件

$$k' = \mathrm{Hash}\left(\mathrm{Hash}\left(\cdots\mathrm{Hash}\left(k_j\right)\right)\right) \tag{9}$$

若新的群组会话密钥k_j能通过有限次Hash函数推导出原群组密钥k'，则表明k_j已被正确接收。

如图4所示，当终端设备协商完成群组会话密钥后，拥有会话密钥的设备将构成一个可信域。可信域内的终端设备可通过TEE内的数据处理模块，实现跨设备访问加密数据库文件中的信息，或将本地加密数据提交至数据中心。对于被撤销权限的终端设备，由于无法获得更新的群组会话密钥，因此无法通过TEE访问其他设备的加密数据。通过TEE融合，不仅有效提升了终端设备间共享数据的效率，同时也保障了可信域内数据的安全性。

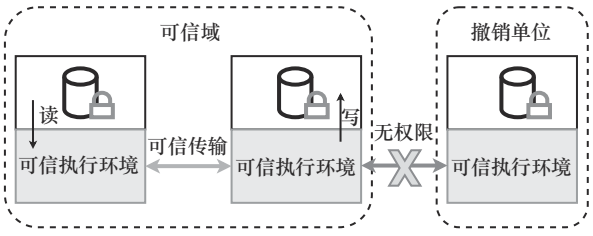


图4　融合TEE隔离性示意

3.3　基于数据驱动的TEE融合技术

在缺乏DoTI技术支持的情况下，单设备的TEE通常不信任来自外部传递的数据，且异构TEE之间缺乏统一的远程可信证明体系，无法有效保证异构TEE间数据访问的安全性。因此，利用TEE的可信根作为CP-ABE算法的加密属性，可以高效实现TEE设备的远程证明。而不具备已验证可信根的设备，则没有权限访问DoTI环境内的数据，从而在实现TEE融合的同时，仍能够保持其与外界的隔离性。

在数据跨TEE传输、处理和存储阶段，TEE内程序的执行方式均通过DML序列实现。由于DML不需要预先编译，即可直接在具备TEE内建数据库的终端设备上运行，因此在一个可信域内，不同的数据处理或任务执行需求都能够安全地在异构TEE内直接运行。

本文基于内建于TEE的安全数据库系统，并以基于属性加密构建的可信域为安全保障，设计了数据驱动的TEE融合技术DoTI。如图5所示，结合第4.2节的场景，在地面数据中心与空中数据中心构成的云系统和设备终端实现TEE融合后，本节以跨异构TEE设备的数据访问为例，详细说明DoTI对数据全生命周期的保护。

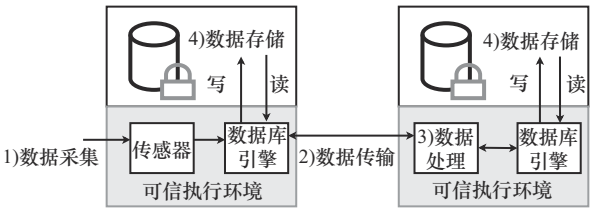


图5　DoTI中数据生命周期示意

算法1描述了空中数据中心和地面数据中心如何定期与管域内的终端设备通过CP-ABE协商群组会话密钥的流程，收到有效群组会话密钥的设备被视为加入数据中心管辖的可信域。在协同作业期间，可信域内的设备可向数据中心提交环境感知数据。数据中心在汇聚并分析所有终端设备的数据后，可向终端设备下达新的数据采集任务。终端设备也可以直接向目标设备请求数据，以完善自身的感知数据集，从而实现更高效的协同作业。

算法1　可信域构建算法

输入　本轮收集的终端设备报送身份信息集合M，合法设备集合V，上一轮可信域内设备集合D'，公共参数PK，群组会话密钥k

输出　群组会话密钥消息CT

$D \leftarrow \varnothing$

1) for each v_i in M
2)　if $v_i \in V$ then
3)　　$D \leftarrow D \cup \{v_i\}$
4)　end if
5) end for

6) if $D \neq D'$或到达会话密钥更新时间则then

7)　$A = \left\{ \vee v_i | v_i \in D \right\}$/*构造访问策略$A$*/

$$\mathrm{CT} \leftarrow \mathrm{Encrypt}\left(\mathrm{PK}, k_j, A\right)$$

8) end if

1) 数据采集

数据采集设备通过将传感器、输入键盘等外部设备连接至主机的TEE部分，由TEE环境中的安全设备驱动[32]控制外部设备，从而避免非可信系统中攻击者对数据源的干扰及对原始数据的篡改。采集到的数据以明文形式在TEE中进行处理和计算，处理结果则通过TEE中的加密数据库加密后传输至非可信环境进行存储或等待传输。

2) 数据传输

数据中心通过SELECT指令向终端设备发起数据请求，终端设备将本地数据库的查询结果用会话密钥加密后发送至空中数据中心或地面数据中心。传输的数据均为密文DML形式，可直接通过TEE的安全设备驱动无线传输至其他设备的TEE中，有效避免了攻击者窃听数据的可能性。同时，为确保加密DML的完整性，附加了根据式(8)计算得到的消息认证码MAC

$$\mathrm{MAC} = \mathrm{Hash}\left(\mathrm{DML}, k, v_i\right) \tag{10}$$

3) 数据处理

如图6所示，数据中心在收到加密数据包后，会在TEE内使用群组会话密钥解密数据，并重新计算消息认证码MAC'。随后，将MAC'与原始消息中附带的MAC进行对比。若两者相同，则数据包被认为完整且未被篡改，可进行下一步处理；否则，直接丢弃该条DML。

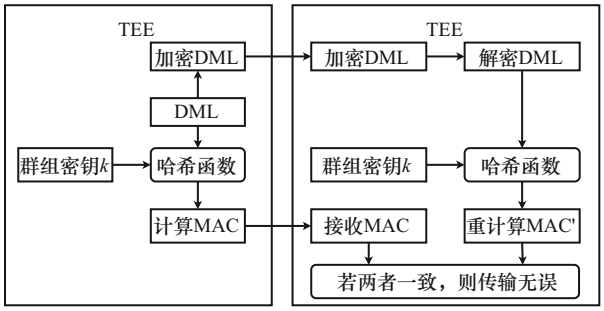


图6　DoTI中DML完整性校验协议

数据中心在TEE内以明文形式汇聚，并处理其管辖可信域内所有设备上报的DML，完成数据格式校验、数据去重等操作。由于TEE与外部计算环境之间具有严格的硬件级隔离，在TEE内处理明文数据不仅能够确保数据的机密性和完整性，还能显著提升数据处理效率。

4) 数据存储

数据中心根据数据处理结果生成INSET、UPDATE、DELETE等DML命令，并将这些命令发送至相关单位以更新设备存储信息；或者直接通过DML将数据以页级或列级的加密粒度存储在云数据库文件中，以备后续使用。

在上述阶段，所有安全数据操作均可通过即时生成的DML实现，从而有效避免因适应异构TEE的需求而对现有程序进行优化或再设计，或开发部署新的TA程序。

4　性能与安全性分析

4.1　性能分析

1) 实验环境

本文实验平台由Raspberry Pi 3B、Hikey、Hikey 960等嵌入式开发板混合组成。虽然这些嵌入式系统搭载的可信执行环境均为ARM TrustZone，且安全操作系统统一采用OP-TEE[33]，但由于系统配置和开发套件不同，在一种平台上编译生成的TA无法直接移植到其他系统的TEE中运行。为克服这一问题，本文实验基于SQLite[34]在所有嵌入式开发板上实现了内建于TEE的加密数据库。同时，跨TEE的数据处理和交互行为则通过TA生成满足业务逻辑的DML实现，并将其传递至目标TEE数据库执行。因此，在本文实验中，任意TEE内的TA能够通过DML直接访问其他异构TEE设备中的数据，与调用自身资源类似。

2) 数据库性能分析

本节以无人机集群协同作业场景为例，构建实验数据库。在该场景中，数据库存储了2个表，分别是记录自身飞行信息的数据表gps和保存全局无人机状态的数据表uav。其中，gps包含16个字段，如无人机编号Id、时间戳timestamp、经度Lat、纬度Lng、海拔高度Alt、速度Spd等；uav保存无人机编号Id和相应设备的位置等信息。为了验证TEE内数据库引擎在处理无人机位置状态查询和更新等协同任务时的性能，本文设计了如表1所示的语句。

表1　面向无人机集群任务的数据库查询语句

语句编号	查询语句
Q*X*[*n*]	SELECT * FROM gps LIMIT *n*
CQ1	SELECT Id, COUNT(*) FROM gps WHERE Alt > 628.81 GROUP BY Id ORDER BY COUNT(*) ASC
CQ2	SELECT * FROM gps WHERE Alt > 628.81 GROUP BY Spd DESC
CQ3	SELECT uav.Id, gps.Lat, gps.Lng, gps.Alt FROM uav INNER JOIN gps ON uav.gpsid = gps.Id WHERE Alt > 1 586.8
CQ4	SELECT uav.Id, gps.Lat, gps.Lng, gps.Alt FROM uav LEFT JOIN gps ON uav.gpsid = gps.Id WHERE Alt > 1 586.8
CQ5	SELECT * FROM gps WHERE Id IN (SELECT Id FROM gps WHERE Spd > 8.999)
INSERT	INSERT INTO gps (*c*1...*c*16) VALUES (*v*1...*v*16)

图7对比了TEE内数据库与运行在外部操作系统的原始数据库执行语句Q*X*[*n*]的时间，Q*X*[*n*]表示该语句查询了*n*条数据。实验结果表明，在执行一些简单查询语句时，TEE内数据库的性能是原始数据库的81.33%~135.68%。由于TEE内数据库性能的主要损耗集中在对外部文件的读写操作，而TEE的内存管理机制比外部操作系统更高效，因此在执行简单查询语句时，TEE内数据库表现出更优的性能。

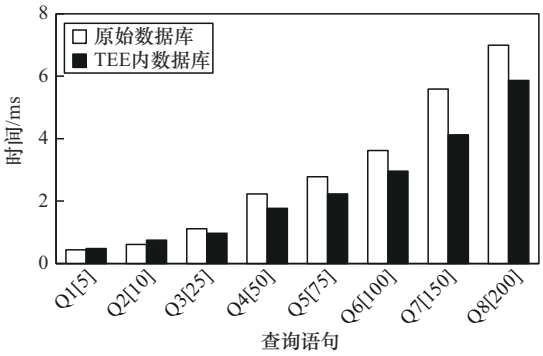


图7　TEE内数据库与运行在外部操作系统的原始数据库执行Q*X*[*n*]语句的时间

图8展示了TEE内数据库与运行在外部操作系统的原始数据库执行包含WHERE、GROUP BY、JOIN等谓词的复杂查询语句的时间。实验结果表明，在此类查询中，TEE内数据库的性能约为原始数据库的49.34%。

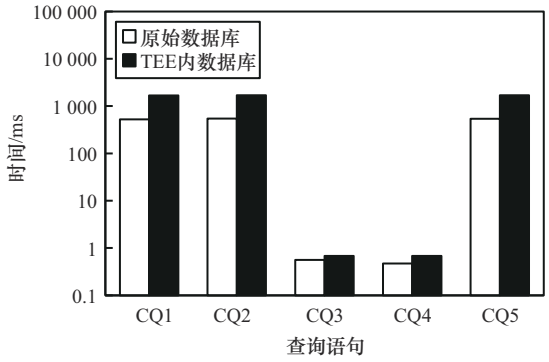


图8　TEE内数据库与运行在外部操作系统的原始数据库执行CQ*X*语句的时间

图9展示了在对gps数据表执行数据插入操作时，不同密钥长度对TEE内数据库与运行在外部操作系统的原始数据库执行INSERT语句的时间。实验结果表明，与简单查询实验相似，在数据插入场景中，TEE内数据库的性能达到原始数据库的226.78%。

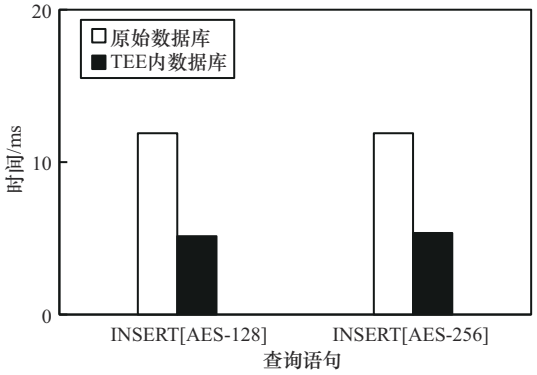


图9　TEE内数据库与运行在外部操作系统的原始数据库执行INSERT语句的时间

上述实验结果表明，迁移至TEE的数据库性能约为原始数据库的119.15%，展现出了较强的可用性，能够有效满足集群协同作业场景的需求。

4.2　安全性分析

1) 抗重放攻击

假设攻击者截获了节点申请加入可信域的数据包，并冒充该节点再次向中心节点提交入域申请。尽管攻击者可以从中心节点获取群组密钥的广播消息，并满足解密策略，但由于解密密钥SK_i在初始化阶段已通过机密信道预先存储于设备的TEE中，攻击者仍无法解密消息和获取群组密钥。

2) 抗中间人攻击

假设攻击者截获数据中心广播的群组密钥消息，并随机生成一串新密钥，用公共参数PK加密

后发送给其他节点。由于群组密钥由中心节点通过连续哈希函数生成，新密钥无法通过完整性校验，从而有效抵御了中间人对数据包的篡改。

3) 数据机密性和完整性

协同平台的数据及其处理过程的机密性和完整性由平台内各设备的TEE保证。单设备内明文数据的处理均在TEE内完成，数据在TEE内以页级或列级加密后安全存储在REE中。在TEE融合阶段，通过群组密钥的分发和更新，确保了可信域的隔离性。TEE间的数据交互通过加密的DML完成，保证了数据传输的机密性。假设攻击者获取了一台正在作业的终端设备，由于可信根和群组密钥均安全地存储于TEE中，攻击者无法解密任何REE数据。同时，任何对加密数据库文件的篡改或破坏都可以被fbMHT检测到。同时，即使攻击者试图伪造DML以窃取TEE中的数据，由于不具有群组密钥，因此也无法构造合法的消息认证码，本文方案有效保障了数据的机密性和完整性。

综上所述，本文方案的安全性主要由TEE提供保障。虽然存在一些针对TEE的侧信道攻击，但由于TEE的复杂性和代码量远低于通用操作系统，随着TEE技术的不断成熟和完善，这些攻击成功的可能性将逐渐降低。

4.3　对比分析

现有TEE融合方案在设计原理、技术侧重点和实现硬件平台等方面均存在差异，因此难以在性能方面进行直接比较。如表2所示，本文从部署灵活性、代码可迁移性、是否提供可信远程证明以及硬件平台兼容性等功能角度对比了DoTI与相关方案的能力属性。

由于HyperEnclave[9]、MyTEE[11]和secGear[12]等方案需要对设备的硬件虚拟层或代码编译器进行改造，才能在异构设备上部署和运行特定功能的TA。而本文方案仅需将数据库引擎移植至TEE内，即可通过DML在异构TEE间实现数据业务，因此本文方案的部署更加便捷。

同时，HyperEnclave与MyTEE的开发仍限定于特定的编程方式，即需要借助SGX SDK或MyTEE API，这使得开发代码难以迁移到新平台。而secGear采用的代码辅助生成工具以及本文方案使用的DML具有平台无关性，因此无须考虑代码移植问题。

在跨TEE数据交互方面，MyTEE提供了基于TPM的远程证明协议。HyperEnclave和secGear基于TEE提供的可信远程证明能力，设计了一对一的远程证明协议，从而确保跨TEE数据交互的安全性。本文方案则通过CP-ABE实现群组会话密钥的分发，并构建可信域，从而保障跨TEE数据的安全交互。

同时，本节利用图10所示的网络拓扑结构，将DoTI与基于TEE的远程证明（TEE-RA）[9]及基于TPM的远程证明（TPM-RA）[11]等一对一的远程证明协议进行比较，进一步说明了DoTI方案在网络通信性能方面的优势。

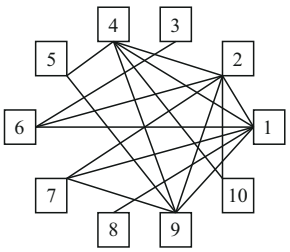


图10　协同平台网络拓扑结构

如图11所示，实验统计了以节点1为源节点，分别向其余N个节点发送一次数据请求并处理N个节点返回数据所需的时间，其中$N = 1, 2, 3, \cdots, 9$。实验结果表明，在基于RA的异构TEE融合方案中，由于2台设备间每次远程证明交互都需要对双方设备进行软硬件完整性度量，以保证设备的可信性，因此节点1处理数据所需的时间随着通信设备数量的增加逐渐增长。而TPM-RA方案由于受限于TPM的运算性能，时间增幅显著高于TEE-RA方

表2　　**DoTI与相关方案的能力属性比较**

方案	部署灵活性	代码可迁移性	提供可信远程证明	支持x86平台	支持ARM平台
HyperEnclave[9]	×	×	√	√	×
MyTEE[11]	×	×	√	×	√
secGear[12]	×	√	√	√	√
DoTI	√	√	√	√	√

案。相比之下，DoTI利用可信根作为属性，并通过CP-ABE完成群组密钥分发后，即可通过加密的DML实现跨TEE的数据安全交互，无须再执行一对一的远程证明协议。随着与节点1交互的设备数量增加，本文方案仍能保持良好的网络通信性能。

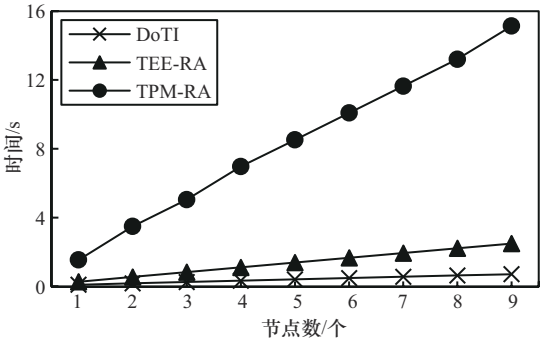


图11　节点1与其余N个节点执行一次数据交互的时间

实验结果表明，在可信域建立后，大量跨设备的DML传输与执行不会对协同平台的网络造成较大开销，从而保证了平台的可用性。在方案通用性方面，仅有secGear和本文方案同时支持通用计算平台和嵌入式系统。因此，本文方案在上述功能上具有显著优势。

5　结束语

TEE通过硬件隔离技术有效保障设备系统和数据的机密性与完整性。然而，如何保证异构TEE间数据互操作的安全性，已成为协同平台稳定运行的关键问题。本文基于DML实现DoTI技术，并采用基于属性加密的群组密钥分发协议构建可信域，从而确保TEE融合后的隔离性。实验分析表明，更高效的群组密钥协商协议有助于进一步提升DoTI方案的整体性能。

参考文献：

[1] 李松. 基于消息互联的无人机平台协同导航方法[J]. 科技导报, 2022, 40(17): 113-119.
LI S. A collaborative navigation method of UAV platform based on message interconnection[J]. Science & Technology Review, 2022, 40(17): 113-119.

[2] EKBERG J E, KOSTIAINEN K, ASOKAN N. Trusted execution environments on mobile devices[C]//Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security-CCS'13. New York: ACM Press, 2013: 1497-1498.

[3] JAUERNIG P, SADEGHI A R, STAPF E. Trusted execution environments: properties, applications, and challenges[J]. IEEE Security & Privacy, 2020, 18(2): 56-60.

[4] ZHAO C, ZHAO S N, ZHAO M H, et al. Secure multi-party computation: theory, practice and applications[J]. Information Sciences, 2019, 476: 357-372.

[5] WEI K, LI J, DING M, et al. Federated learning with differential privacy: algorithms and performance analysis[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 3454-3469.

[6] ZHENG W, WU Y, WU X X, et al. A survey of Intel SGX and its applications[J]. Frontiers of Computer Science, 2020, 15(3): 153808.

[7] LI W H, XIA Y B, CHEN H B. Research on ARM TrustZone[J]. GetMobile: Mobile Computing and Communications, 2019, 22(3): 17-22.

[8] MOFRAD S, ZHANG F W, LU S Y, et al. A comparison study of intel SGX and AMD memory encryption technology[C]//Proceedings of the 7th International Workshop on Hardware and Architectural Support for Security and Privacy. New York: ACM Press, 2018: 1-8.

[9] JIA Y K, LIU S, WANG W H, et al. HyperEnclave: an open and cross-platform trusted execution environment[C]//2022 USENIX Annual Technical Conference (USENIX ATC'22). Berkeley: USENIX Association, 2022: 437-454.

[10] GALANOU A. Tailoring and verification of the trust boundaries in a heterogeneous TEE landscape[C]//Proceedings of the 2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S). Piscataway: IEEE Press, 2023: 173-175.

[11] HAN S, JANG J. MyTEE: own the trusted execution environment on embedded devices[C]//Proceedings 2023 Network and Distributed System Security Symposium. Reston: Internet Society, 2023: 1-15.

[12] 刘忻, 王家寅, 杨浩睿, 等. 一种基于区块链和secGear框架的车联网认证协议[J]. 信息网络安全, 2022, 22(1): 27-36.
LIU X, WANG J Y, YANG H R, et al. An Internet of vehicles authentication protocol based on blockchain and secGear framework[J]. Netinfo Security, 2022, 22(1): 27-36.

[13] SCOPELLITI G, POUYANRAD S, NOORMAN J, et al. End-to-end security for distributed event-driven enclave applications on heterogeneous TEEs[J]. ACM Transactions on Privacy and Security, 2023, 26 (3): 1-46.

[14] KARANJAI R, COLLIER R, GAO Z M, et al. Decentralized translator of trust: supporting heterogeneous TEE for critical infrastructure protection[C]//Proceedings of the 5th ACM International Symposium on Blockchain and Secure Critical Infrastructure. New York: ACM Press, 2023: 85-94.

[15] MELTON J, SIMON A R. SQL: 1999: understanding relational language components[M]. San Francisco: Morgan Kaufmann Publishers Incorporated., 2001.

[16] 刘瑶秋, 赵苗苗. 数据驱动的公交路线智能识别系统开发[J]. 客车技术与研究, 2024, 46(5): 22-26.
LIU Y Q, ZHAO M M. Development of a data-driven intelligent recognition system for bus routes[J]. Bus & Coach Technology and Research, 2024, 46(5): 22-26.

[17] 程敏敏, 朱灿, 何栓, 等. 基于工业互联网平台的核电运行数据服务研究[J]. 网络安全与数据治理, 2024, 43(8): 49-55.
CHENG M M, ZHU C, HE S, et al. Research on nuclear power operation data service based on industrial Internet platform[J]. Cyber Security and Data Governance, 2024, 43(8): 49-55.

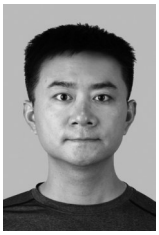
[18] 侯鹏, 李智鑫, 张飞, 等. 金融数据安全治理智能化技术与实践[J]. 网络与信息安全学报, 2023, 9(3): 174-187.
HOU P, LI Z X, ZHANG F, et al. Technology and practice of intelligent governance for financial data security[J]. Chinese Journal of Network and Information Security, 2023, 9(3): 174-187.

[19] 龙笑. 无人机货运大数据实时传输及管理技术研究[D]. 南京: 南京

航空航天大学, 2019.
LONG X. Research on real-time transmission and management technology of UAV freight big data[D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2019.
[20] QIAO Z, LIANG S W, DAVIS S, et al. Survey of attribute based encryption[C]//Proceedings of the 15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). Piscataway: IEEE Press, 2014: 1-6.
[21] AHMAD Z, FRANCIS L, AHMED T, et al. Enhancing the security of mobile applications by using TEE and (U)SIM[C]//Proceedings of the 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing. Piscataway: IEEE Press, 2013: 575-582.
[22] ZHAO S J, ZHANG Q Y, HU G Y, et al. Providing root of trust for ARM TrustZone using on-chip SRAM[C]//Proceedings of the 4th International Workshop on Trustworthy Embedded Devices. New York: ACM Press, 2014: 25-36.
[23] CARDENAS A F. Heterogeneous distributed database management: The HD-DBMS[J]. Proceedings of the IEEE, 1987, 75(5): 588-600.
[24] 施化吉, 田挺, 江丽英, 等. 基于多库操作语言的异构数据库集成框架研究[J]. 计算机工程与设计, 2008, 29(17): 4484-4487, 4549.
SHI H J, TIAN T, JIANG L Y, et al. Study on integration framework of heterogeneous databases based on multidatabase language[J]. Computer Engineering and Design, 2008, 29(17): 4484-4487, 4549.
[25] 王祥宇. 外包数据安全检索关键技术研究[D]. 西安: 西安电子科技大学, 2022.
WANG X Y. Research on key technologies of secure retrieval of outsourcing data[D]. Xi'an: Xidian University, 2022.
[26] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP'07). Piscataway: IEEE Press, 2007: 321-334.
[27] WANG Y Z, SHEN Y L, SU C C, et al. CryptSQLite: SQLite with high data security[J]. IEEE Transactions on Computers, 2020, 69(5): 666-678.
[28] MA C Y, LU D, LYU C Y, et al. BiTDB: constructing a built-in TEE secure database for embedded systems[J]. IEEE Transactions on Knowledge and Data Engineering, 2024, 36(9): 4472-4485.
[29] LU D, SHI M Q, MA X D, et al. Smaug: a TEE-assisted secured SQLite for embedded systems[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(5): 3617-3635.
[30] 张国印, 付小晶, 马春光. 移动对等传感器网络的基于属性加密的组密钥管理协议[J]. 高技术通讯, 2013, 23(2): 109-115.
ZHANG G Y, FU X J, MA C G. A group key management protocol using attribute-based encryption for mobile peer-to-peer wireless sensor networks[J]. Chinese High Technology Letters, 2013, 23(2): 109-115.
[31] TIAN C, MA J F, LI T, et al. Provably and physically secure UAV-assisted authentication protocol for IoT devices in unattended settings[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 4448-4463.
[32] WEI N, SANI A A. SchrodinText: strong protection of sensitive textual content of mobile applications[C]//Proceedings of the IEEE Transactions on Mobile Computing. Piscataway: IEEE Press, 2022: 1402-1419.
[33] NEHAL A, AHLAWAT P. Securing IoT applications with OP-TEE from hardware level OS[C]//Proceedings of the 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA). Piscataway: IEEE Press, 2019: 1441-1444.
[34] BHOSALE S T, PATIL T, PATIL P. Sqlite: light database system[J]. International Journal of Computer Science and Mobile Computing, 2015, 4(4): 882-885.

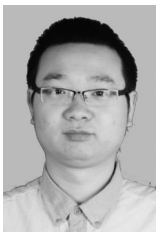
[作者简介]

马承彦（1994– ），男，江苏扬州人，西安电子科技大学博士生，主要研究方向为无人系统安全、数据库安全、嵌入式系统可信计算技术。



卢笛（1983– ），男，陕西安康人，博士，西安电子科技大学教授、硕士生导师，主要研究方向为可信计算技术、云计算、虚拟化技术及其安全。

马鑫迪（1989– ），男，山东淄博人，博士，西安电子科技大学副教授、博士生导师，主要研究方向为数据安全、隐私保护。



习宁（1986– ），男，陕西渭南人，博士，西安电子科技大学教授、博士生导师，主要研究方向为异构网络融合安全、服务组合安全、信息流安全。

王锦锦（1998– ），男，陕西西安人，伯明翰大学博士生，主要研究方向为软件定义网络、机密计算。

马建峰（1963– ），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为计算机安全、密码学、无线网络安全。