文章编号:1671-4598(2025)09-0127-08 DOI:10.16526/j.cnki.11-4762/tp.2025.09.015 中图分类号:TP309 文献标识码:A

基于密文属性的物联网环境私有数据访问控制系统设计

黄雄平
(广东科学技术职业学院 教务部,广东 珠海 519090)

摘要:物联网环境中的设备和用户数量可能非常庞大且不断变化,系统需要能够适应这种动态性,并支持快速扩展;为此,设计一种基于密文属性的物联网私有数据访问控制系统;该系统由包括客户端模块、服务器模块和密钥生成模块组成;客户端模块主要负责数据的接收、加密、密钥管理和解密;服务器模块通过属性基加密算法生成部分密钥组件;通过将访问权限与密文属性绑定,系统可以实现更精细的访问控制,确保只有符合特定属性的用户或设备才能访问数据;利用重加密得出数据主密钥,将数据密钥储存到数据管理库中;密钥生成模块负责维护密钥组件和数据属性集,保证用户取消或新增访问时,及时更新数据属性列表,使得系统能够快速适应新的用户和设备,支持系统的扩展;最后由解密服务器对密钥解密输出明文,实现对物联网环境下私有数据的访问控制;系统测试结果表明,系统能在 30 ms 时间内完成物联网私有数据的加密和储存,加密强度可达 95%,加密后的物联网数据频率直方图波动非常小,访问成功率非常高,确保物联网系统安全稳定的运行。

关键词:物联网;数据访问;控制系统;数据加密;属性基加密;密钥生成

Design of Private Data Access Control System for IoT Environment Based on Cryptography Attributes

HUANG Xiongping
(Department of Academic Affairs, Guangdong Polytechnic of Science and Technology, Zhuhai 519090, China)

Abstract: Devices and users may be very large and constantly changing in the environments of Internet of Things (IoT). In order to adapt to this dynamism and support rapid expansion, an IoT private data access control system based on ciphertext attributes is designed, which consists of a client module, a server module, and a key generation module. The client module is mainly responsible for data reception, encryption, key management, and decryption; The server module generates partial key components through the attribute based encryption algorithm. By binding access permissions to ciphertext attributes, the system can achieve more accurate access control, ensuring that only users or devices that meet specific attributes can access data. A data master key is obtained through re encryption, and the data key is stored in the data management repository; The key generation module is responsible for maintaining key components and data attribute sets, ensuring that the data attribute list is updated in a timely manner when users cancel or add access, enabling the system to quickly adapt to new users and devices and support its expansion. Finally, the decryption server decrypts the key and outputs plaintext, achieving access control to private data in the environments of IoT. Experimental results show that the system can encrypt and store private data of Internet of Things within 30 ms, with an encryption strength of up to 95%. The encrypted data of IoT have a very little fluctuation in frequency histogram, with a very high access success rate, ensuring the safe and stable operation of IoT.

Keywords: IoT; data access; control system; data encryption; attribute based encryption; key generation

0 引言

智能家居、智慧城市、工业自动化等领域的快速发展下,大量的设备和传感器被连接到网络中,产生了海量的数据。这些数据往往包含了用户的隐私信息、企业的商业秘密以及国家的敏感数据,因此,对物联网环境

收稿日期:2024-07-30; **修回日期**:2024-09-12。
作者简介:黄雄平(1985-),男,硕士研究生,助理研究员。
引用格式:黄雄平.基于密文属性的物联网环境私有数据访问控制系统设计[J].计算机测量与控制,2025,33(9):127-134.

私有数据访问控制至关重要[1]。但是，物联网具有设备多样性、大规模分布、资源受限、环境不可控、数据敏感性、实时性和动态性等特征。这些特征使得物联网环境中的数据安全和隐私保护面临更大的挑战，需要通过严格的访问控制来确保只有授权的实体才能访问敏感数据，防止数据泄露和未授权使用，从而保护个人隐私、商业秘密和国家安全。同时，随着全球对数据保护法规的日益严格，如欧盟的通用数据保护条例（GDPR）和中国的网络安全法，物联网环境下的数据访问控制系统还需要符合这些法律法规的要求，确保数据的合法合规使用。在这样的背景下，设计一个有效的私有数据访问控制系统变得尤为重要。这个系统需要确保只有授权的用户或设备才能访问特定的数据，同时还要保证数据的完整性和可用性[2]。此外，随着数据量的激增和数据类型的多样化，传统的访问控制方法已经难以满足物联网环境下的安全需求。因此，构建一个既安全又高效的访问控制系统，成为了物联网领域研究的热点问题。

为此，文献［3］提出一种基于区块链和密文属性加密设计访问控制系统，通过门限密钥共享技术对用户数据密钥进行分割，引入密文策略属性加密算法，实现了用户私钥的计算并确保了私钥的唯一性，有效保护数据访问的安全性。文献［4］结合物联网区块链的去中心化和不可修改的特性，构建一种能够对物联网数据进行细粒度访问控制，并确保其隐私保护的智能合约访问系统，在提高了访问控制的可靠性的同时，能够满足大规模的访问需求。上述系统能够在某种程度上保障物联网数据的安全性，但存在访问控制系统复杂、易受攻击等问题。文献［5］介绍了一种动态访问控制策略，该策略以安全属性为核心，对设备和用户的网络访问权限进行动态管理。该方法考虑了与设备配置和操作相关的安全属性，通过实时监控和评估设备及用户的安全档案，动态调整访问限制，从而实现对设备配置和操作的灵活调整。文献［6］提出了一种集成本体和网格计算系统的医疗领域数据访问控制模型，该模型采用了三层安全访问控制架构。该模型通过基于截止期限优先级的调度算法，根据用户优先级（低、中、高）来调度作业，并采用基于角色的策略来识别和阻止未经授权的访问。在多用户访问的云平台数据库中，为了确保访问安全，需要频繁插入规则，而传统方法在处理多规则集插入时存在较大的时间开销。

针对上述问题，设计了基于密文属性的物联网环境私有数据访问控制系统。该系统在保障物联网数据安全性的同时，提升物联网私有数据访问控制系统的效率。主要创新点如下。

1）属性基加密算法的应用：系统采用属性基加密算法来生成部分密钥组件，这种算法能够根据数据的属性来控制访问权限，提高了数据访问的安全性和灵活性。

2）重加密技术的使用：通过重加密技术得出数据主密钥，并将数据密钥存储到数据管理库中，这种方法增强了密钥管理的效率和安全性。

3）动态密钥和属性管理：密钥生成模块负责维护密钥组件和数据属性集，能够及时更新数据属性列表以响应用户访问权限的变化，如取消或新增访问，确保系统的动态适应性。

4）解密服务器的独立性：解密服务器独立于其他模块，负责对密钥进行解密并输出明文，这种设计分离了解密操作，减少了其他模块的负担，同时提高了系统的安全性和可维护性。

5）模块化设计：系统采用模块化设计，包括客户端模块、服务器模块和密钥生成模块，每个模块各司其职，提高了系统的可扩展性和维护性。

1 物联网环境私有数据访问控制系统设计

物联网系统通常由大量分布式、异构的设备组成，这些设备可能具有不同的计算能力、存储容量和安全特性，因此物联网（IoT）环境的私有数据访问控制比普通网络环境更具难度。此外，物联网设备往往部署在开放或不可控的环境中，容易受到物理攻击和网络攻击。物联网数据的产生、传输和处理过程涉及多个层面和环节，包括传感器、网关、云平台等，这增加了数据在传输过程中被截取或篡改的风险。同时，物联网设备的资源受限特性限制了其执行复杂加密和认证算法的能力，这进一步增加了确保数据安全和隐私的难度。私有数据访问控制系统可以确保只有经过授权的用户和设备才能访问特定的数据，从而防止数据泄露和未授权访问。这对于保护用户隐私具有重要意义。设计基于密文属性的物联网私有数据访问控制系统，通过先进的加密技术和模块化架构，确保在物联网环境中传输和存储的私有数据能够得到有效的保护，防止未授权访问和数据泄露。这种系统设计采用了属性基加密算法，能够根据数据的属性来精确控制访问权限，从而在保障数据安全的同时，也提供了灵活的访问控制策略。为了实现职责分离和提高系统的可维护性、可扩展性，将系统设计分为客户端模块、服务器模块和密钥生成模块。客户端模块负责数据的接收、加密、密钥管理和解密，直接与用户交互，确保数据在传输过程中的安全；服务器模块负责生成部分密钥组件、重加密和数据密钥的存储，是数据处理和存储的核心；密钥生成模块则专注于维护密钥组件和数据属性集，确保密钥和访问权限的动态更新。这种模块化设计使得系统各部分能够独立运作，便于管理和

升级，同时也增强了系统的安全性和稳定性。如图 1 所示。

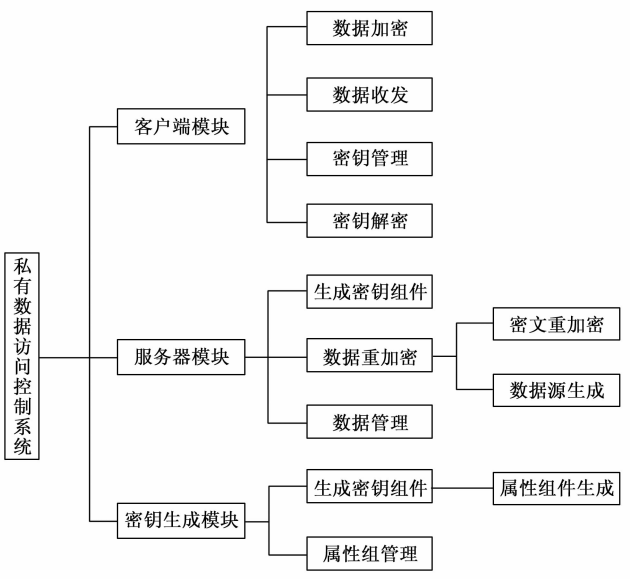

图 1　访问系统结构图

客户端模块是整个系统的用户界面。该模块集成了数据加密、数据收发、密钥管理以及密钥解密四大核心功能。在数据加密环节，客户端模块使用先进的加密算法对用户的数据文件进行加密处理，确保数据在传输前的机密性。数据收发功能则负责与服务器模块进行通信，安全地传输加密后的数据。密钥管理部分确保了加密密钥的安全存储和分发，防止密钥泄露。最后，在接收到加密数据后，客户端模块的密钥解密功能能够使用相应的密钥将数据解密，恢复为原始明文，供用户使用。

服务器模块是系统的核心处理单元，它由生成密钥组件、数据重加密和数据管理三大功能组成。服务器模块负责对从客户端上传的加密数据进行高效管理，确保数据的安全存储和访问控制。在数据重加密过程中，服务器模块利用先进的加密技术对数据进行再次加密，增强数据的安全性[7]。同时，服务器模块还负责生成部分密钥组件，这些组件是密钥生成模块能够顺利生成完整密钥的关键。通过这些功能，服务器模块为整个系统的安全性和稳定性提供了坚实的基础。

密钥生成模块是系统的安全保障中心，它由生成密钥组件和数据属性组管理两大功能构成。该模块的主要任务是确保每个数据项都能生成与其属性相对应的密钥，以及相关的组件参数。在数据重加密和密钥生成的过程中，数据属性扮演着至关重要的角色。因此，密钥生成模块在保证密钥组件正确生成的同时，还必须对属性组中的数据进行细致的管理，确保数据的访问控制策略能够根据属性动态调整，从而实现对物联网环境下私有数据访问的精细化控制。

1.1　客户端模块

客户端模块负责对数据文件进行加密和解密：由服务器获取数据和组件参数，密钥生成模块接收后对数据进行加密和解密。客户端模块的流程图如图 2 所示。

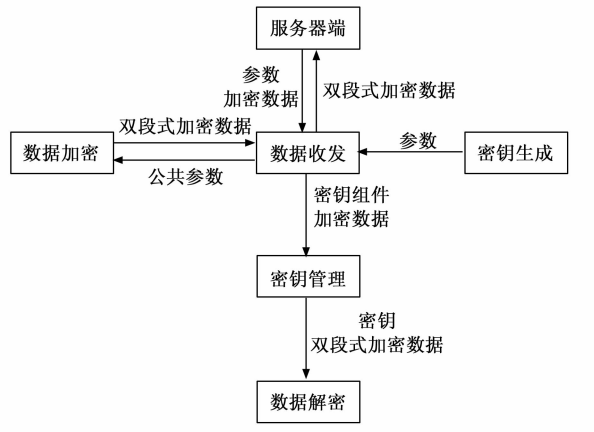

图 2　客户端模块流程图

1）数据加密：

在设计数据加密系统时，面临着一个挑战：传统的属性加密算法虽然提供了高度的安全性和灵活的访问控制，但其效率相对较低，难以满足对大型数据文件进行快速加密的需求。为了解决这一问题，采用了双段式数据加密策略。首先，使用一个专用密钥对原始数据文件进行加密。这种专用密钥通常基于高效的加密算法，能够迅速处理大量数据，确保加密过程的效率。接着，利用属性加密技术对专用密钥本身进行加密。属性加密技术能够根据数据的访问控制属性生成密钥，从而实现对密钥的精细控制[8]。通过这种双段式加密方法，得到了一个由两部分组成的加密文件：一部分是使用专用密钥加密的原始数据，另一部分是使用属性加密的专用密钥。这样的文件结构不仅保证了数据的安全性，还兼顾了加密效率。当需要解密数据时，系统首先对加密文件进行解密，以恢复出专用密钥。随后，使用这个专用密钥对原始数据文件进行解密，最终得到可读的明文数据。这种解密过程的顺序确保了只有在满足访问控制条件的情况下，用户才能成功解密并访问数据，从而在保证效率的同时，也实现了对数据访问的严格控制。

2）数据收发：

数据收发模块需要完成两个核心功能：对数据进行加密以及生成密钥组件。在用户端，该模块负责对数据进行加密处理，确保数据在上传到服务器端之前的机密性。加密后的数据文件随后被安全地传输到服务器，以便进行进一步的处理和存储。当客户端需要访问数据时，数据收发模块从服务器下载加密的数据文件，确保

数据的传输过程中不会被未授权的第三方截取或篡改。此外，为了保证数据解密的顺利进行，客户端还必须能够接收由服务器和密钥生成模块发出的数据密钥组件。这些密钥组件是解密过程中的关键要素，它们确保了只有拥有正确密钥的用户才能解密并访问数据。通过这些功能，数据收发模块不仅保障了数据在传输过程中的安全性，还为数据的加密和解密提供了必要的支持，确保了整个数据加密系统的稳定运行和高效性能。

3）密钥管理：

这个模块将由服务器和密钥生成模块发出的数据密钥部件结合在一起，形成一个完整的密钥。主要是作为数据的访问者形式[9]。并且，当系统用户权限有变化时，密钥管理也要随之更新。密钥管理的流程图如图 3 所示。

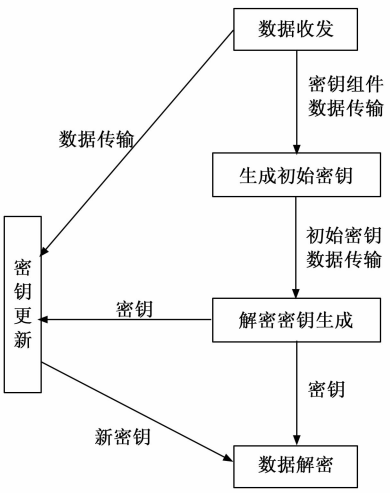

图 3 密钥管理模块流程图

4）数据解密：

数据解密过程是数据加密系统的核心环节，它涉及多个步骤，包括生成数据源解密属性组件、升级密钥、解密属性组件得到的密钥及密文。在这些步骤中，升级密钥和解密属性组件尤为关键，它们直接影响到解密操作的成功与否以及数据的安全性。生成数据源解密属性组件是解密过程的起点，它确保了解密操作能够根据数据的特定属性进行，从而实现精确的访问控制[10]。接着，升级密钥的步骤至关重要，它涉及到对现有密钥进行更新，以应对可能的安全威胁或满足新的访问控制需求。密钥的升级确保了即使面对不断变化的安全环境，数据仍然能够得到有效的保护。

解密属性组件得到的密钥及密文是解密过程的最终阶段。在这一步骤中，系统使用从解密属性组件中提取的密钥来解密加密的数据，恢复出原始的明文信息。这一过程的成功依赖于前面步骤中生成的正确密钥和属性组件，确保了数据解密的准确性和安全性。

1.2 服务器模块

服务器接收由客户端发出的密文后[11]，通过密钥生成模块获取得到属性组结构信息进行重加密，把通过重加密的数据文件输送到数据管理模块储存或分散数据。当用户权限变化时，密文则需要随之重新加密，进而实现访问控制。并且服务器模块还负责将部分密钥产生组件和参数传递给客户端模块。服务器模块的流程图如图 4 所示。

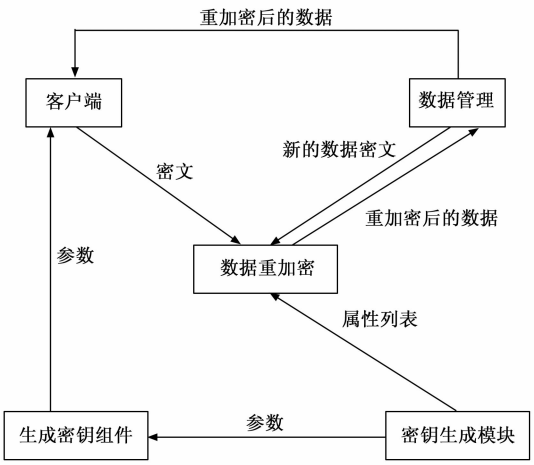

图 4 服务器模块流程图

1）生成密钥组件：

服务器模块生成密钥组件是构建安全访问控制机制的基石，它们确保了只有经过授权的用户或设备才能访问特定的私有数据。通过生成密钥组件，服务器模块能够根据数据的属性、用户的权限以及系统的安全策略来定制密钥，从而实现对数据访问的精细化管理。此外，密钥组件的生成还支持动态的密钥更新和撤销机制，使得系统能够灵活应对用户权限变更、设备替换或安全威胁等场景。总之，服务器模块生成密钥组件的作用不仅在于保障数据的安全性，还在于提升系统的灵活性和可扩展性，为物联网环境下的私有数据访问控制提供了坚实的技术支撑。

2）数据重加密：

服务器模块数据重加密可有效增强数据的安全性和适应性。数据重加密是一种安全措施，它通过使用新的加密密钥对已经加密的数据进行再次加密，从而在数据传输或存储过程中提供额外的保护层。这种做法可以有效应对密钥泄露或加密算法被破解的风险，确保即使原始加密被破坏，数据仍然保持加密状态，难以被未授权访问。此外，数据重加密还支持动态的访问控制策略，允许系统根据用户权限、设备状态或安全需求的变化，实时调整加密密钥，从而实现对数据访问权限的灵活管

理。数据重加密结构如图 5 所示。

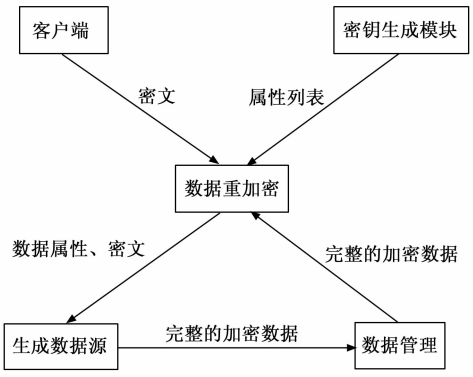

图 5　数据重加密结构图

3）数据管理：

这部分是对上传得到的数据进行储存和分类，服务器接收并上传数据，经过重加密[12]，最后储存到数据管理库中。

1.3　密钥生成模块

密钥生成模块分为两部分，生成密钥组件和属性列表管理。生成密钥组件部分负责根据系统的安全策略和用户权限，创建用于数据加密和解密的密钥组件。这些组件是构建完整密钥的基础，确保了数据加密的强度和访问控制的精确性。属性列表管理部分则负责维护一个动态的属性列表，该列表记录了与数据相关的各种属性，如用户角色、设备类型、访问时间等。通过管理这些属性，系统能够实时更新和调整访问控制策略，确保只有符合特定属性的用户或设备才能访问相应的数据。这两部分功能的协同工作，为物联网环境下的私有数据提供了灵活、安全的访问控制机制，保障了数据的安全性和系统的可靠性。

2　基于密文属性的物联网数据访问控制实现流程

在对物联网数据进行访问控制时，用户访问的数据属性与数据加密解密过程相关[13]。当其属性符合设定的访问结构时，用户可以执行正确的数据解密流程，即令用户正常访问，如果不符合则允许用户访问，实现安全控制。为实现灵活且安全的数据访问控制管理，基于上述控制系统结构，把数据访问系统与数据加密结合[14]，提出了基于密文属性的物联网数据加密算法。物联网环境中的数据往往涉及多种设备、用户和应用场景，这些数据的敏感性和访问需求各不相同。基于密文属性的加密算法能够将数据的访问权限与特定的属性绑定，例如用户角色、设备类型、访问时间等，从而确保只有具备相应属性的实体才能解密和访问数据。这种属性驱动的加密方法不仅增强了数据的安全性，还提高了系统的灵活性，使得访问控制策略能够根据实际情况进行调整，有效应对不断变化的安全威胁和业务需求。因此，密文属性是实现物联网数据高效、安全数据保护的关键因素。

物联网数据加密算法算法包括 6 个部分：数据初始化、生成密钥、数据加密、数据预解密、数据解密、属性撤销。

1）数据初始化：这是加密过程的起点，涉及对原始数据进行准备和格式化，以便于后续的加密处理。在这一阶段，可能会对数据进行分块、编码或添加元数据，以确保数据能够被正确地加密和处理。

2）生成密钥：生成密钥的创建用于数据加密和解密的密钥。这些密钥通常基于复杂的数学算法生成，并且需要保证其唯一性和安全性。在物联网环境中，密钥可能还需要与特定的设备或用户属性相关联。

3）数据加密：在这一步骤中，使用生成的密钥对初始化后的数据进行加密。加密算法将明文数据转换为密文，使得未经授权的实体无法理解数据内容。加密过程需要保证加密强度，以抵御各种攻击。

4）数据预解密：数据预解密是一个可选步骤，它可能在数据解密之前进行，以准备密文数据以便于最终的解密。这可能包括验证数据的完整性、检查访问权限或准备解密所需的密钥组件。

5）数据解密：数据解密是加密过程的逆过程，使用相应的密钥将密文数据转换回明文。这一步骤需要确保只有授权的用户或设备才能成功解密数据，从而保护数据的机密性。

6）属性撤销：属性撤销允许系统管理员撤销特定用户或设备的访问权限。当用户权限变更、设备丢失或安全策略更新时，属性撤销机制能够及时更新访问控制列表，确保数据不会被未授权的实体访问。

假定、为指数的可乘循环群，而为指数的生成子，则得到了一个双线性映射。设定一个系统的一个属性组有个属性群，这个属性群的集合被描述为，并且设第个属性群拥有个数值，这个数值群被描述为。为防碰撞散列函数[15-16]。

1）数据初始化：

当运行 Setup 算法对系统进行数据初始化的时候，首先假设系统拥有 m 个访问用户，那么每个用户 $User_l$ 的数据参数 $f_l \in {}_R Z_p^*$，键值项为 $\{User_l, f_l\}(l \in m)$，可以构建出撤销参数列表 T，由此生成撤销算法需要的参数 $t \in {}_R Z_p^*$，把 T 和 t 储存到服务器中。

2）生成密钥：

当用户具有一张属性表 $L = \{L_1, L_2, \cdots, L_n\}$，向安全中心要求私钥，假设 $L_i = f_l$，根据初始化处理给使用者所产生的撤消参数，由 $User_l$ 从表格 T 中得到

$\{User_l, f_l\}(l \in m)$，从而得出使用者的私钥 SK：

$$SK = (L, f_l, T, \{T_i\}_{1 \leqslant i \leqslant n}) \tag{1}$$

3）数据加密：

采用随机选取的对称密钥 ck，对明文 M 进行加密，得到密文 $E(M)$[17]。一个参数 z'，将对称密钥 ck 转化为明文：

$$ck' = ck \oplus M(z') \tag{2}$$

然后将盲化后的明文 ck'' 发送至服务器，服务器从数据初始化阶段生成的撤销参数表 T 中取出所有用户的 $f_l(l \in m)$。

当服务器完成了撤消算法的过程时，将 ck'' 返回一个数据源，后者通过参数 z' 来完成解盲：

$$ck^* = ck'' \oplus M(z') \tag{3}$$

数据源使用 ck^* 与访问策略 W 作为后续加密算法的输入，加密对称密钥 C_0：

$$C_0 = ck^* z' \tag{4}$$

完成后的密文为：

$$CT = (W, C) \tag{5}$$

4）利用生成的密钥对数据完成预解密：

访问者向数据储存库获取密文 $K' = K^{\mp}, K_i$ 的密钥 K，并生成用于解密服务器计算的转换密钥 K'：

$$K' = K^{1/Z}, K'_i = K_i{}^{1/Z}(1 \leqslant i \leqslant n) \tag{6}$$

访问者将 (CT, K') 发送到解密服务器，以便进行解密操作。

5）属性撤销：

假定要取消用户 $User_j$ 的数据访问权，那么服务器就会按照用户 ID，在取消参数表 T 中找到相应的参数 f_j，并产生一个新的取消参数 $t^* \in_R Z_p^*$ 后进行建立撤销函数 R：

$$R = M(t) \oplus M(t^*) \tag{7}$$

$$R' = \prod_{l=1}^{m} f_l, R'_l = \frac{R'}{f_l} \tag{8}$$

3 私有数据访问控制系统功能的测验

为了验证所设计的物联网环境私有数据访问控制系统的有效性，选取一个物联网场景作为实验测试环境。在这个场景中，家庭主人、家庭成员、访客以及服务人员与多种智能设备进行交互，包括智能灯泡、智能插座、智能摄像头、智能温控器和智能门锁。这些设备不仅种类多样，而且各自产生不同类型的数据，如能耗数据、安全录像、温度数据、门锁状态和照明状态。在访问权限方面，设定了不同的用户角色和相应的权限级别。家庭主人拥有对所有设备和数据的完全访问权限，而家庭成员则对部分设备拥有读写权限，对其他设备则仅有只读权限。访客的权限更为有限，仅能查看智能灯泡的状态。服务人员，如清洁工，则被赋予对特定设备的临时读写权限，以满足其工作需求。

为了确保数据的安全性，所有数据在传输和存储过程中均已经加密处理，并且访问控制是基于用户角色和设备类型来实施的。此外，系统支持动态的属性撤销功能，这意味着在必要时可以迅速撤销特定用户或设备的访问权限，从而增强系统的安全性和灵活性。

网络环境为 100 Mbps 带宽和低延迟（< 50 ms），并且采用了 WPA3 加密技术来保障 Wi-Fi 网络的安全性。通过这样的网络环境，我们可以模拟真实世界中的数据传输和设备响应，从而全面测试私有数据访问控制系统的各项功能。

在上述环境中，应用本研究所设计系统与文献［3］设计的系统（区块链系统）和文献［4］所设计系统（智能合约系统）分别完成物联网环境私有数据访问控制。

3.1 功能测试

由于访问控制的本质就是验证用户属性是否符合设定的访问结构、用户能否可以执行正确的数据解密流程，所以加密、解密、密钥获取时间对控制系统的性能至关重要，为此在测试中，将数据属性个数由 0 增加到 800，对比本研究所设计系统与文献［3］设计的系统（区块链系统）和文献［4］所设计系统（智能合约系统），测验结果如图 6 所示。

由图 6 可知，本研究所设计系统加密、解密以及密钥获取所需时间随着数据属性个数的增加而增加，基于智能合约的访问系统和基于区块链的加密访问系统也伴随着属性的增加，所需时间也有所增加。但相比之下，本研究所设计系统的加密耗时、解密耗时以及密钥获取耗时的最高耗时分别为 30、10 以及 20 ms。证明了本研究所设计系统能够在最短耗时内完成物联网私有数据的加密储存。说明研究系统能够快速的数据加密储存确保了数据在传输和存储过程中的安全性，这对于保护敏感信息、防止数据泄露至关重要。其次，高效的加密过程减少了系统资源的占用，提高了物联网设备的响应速度和整体性能，这对于需要实时数据处理的应用场景尤为重要。

实验同时测试在不同的加密时间下，本研究所设计系统与基于智能合约的访问系统、基于区块链的加密访问系统的物联网数据加密强度，如图 7 所示。

由图 7 可知，随着加密时间的增长，3 种系统的物联网数据加密性能也随着上升。本研究所设计系统对的加密性能强度在 50 s 内维持在 60.7%～89.7%，加密时间为 50 s 时，加密性能强度在 89.7%，且性能强度始终高于 60%；基于智能合约的访问系统加密性能强度在 32.1%～44.6%，加密时间到 50 s 时，加密性能

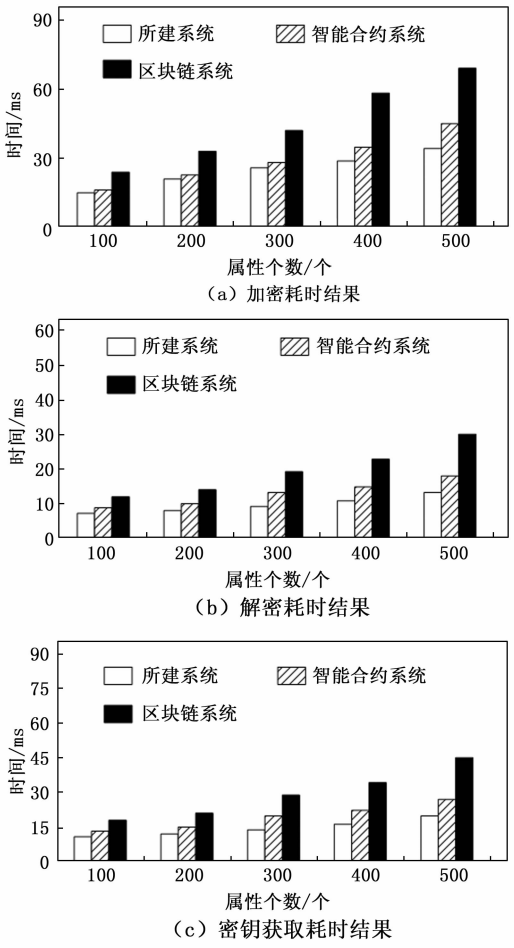

图 6　不同系统的耗时指标对比

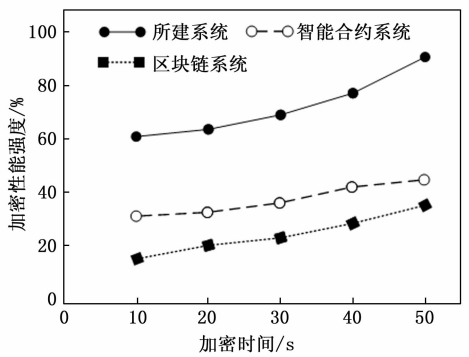

图 7　加密强度对比结果

强度在 44.6%；基于区块链的加密访问系统加密性能强度在 50 s 内最低为 17.4%～35.2%，加密时间到 50 s 时，加密性能强度在 35.2%。可以说明，本研究所设计系统有比较优越的物联网私有数据加密性能，且随着加密时间的增加，数据加密效果越好。这意味着数据在传输和存储过程中更难以被破解，从而为敏感信息的保护提供了更坚实的屏障。这对于防范黑客攻击、数据泄露以及确保用户隐私安全至关重要。

3.2　物联网数据加密前后直方图对比

为进一步验证研究设计的物联网环境私有数据访问控制系统对数据的加密有效性，以物联网数据的频率直方图为评判指标，对比不同系统应用后的物联网数据频率直方图。频率表示物联网数据在单位时间内出现的次数，设置物联网数据的量从 100 GB 增至 400 GB，获取该过程的数据频率直方图如图 8 所示。

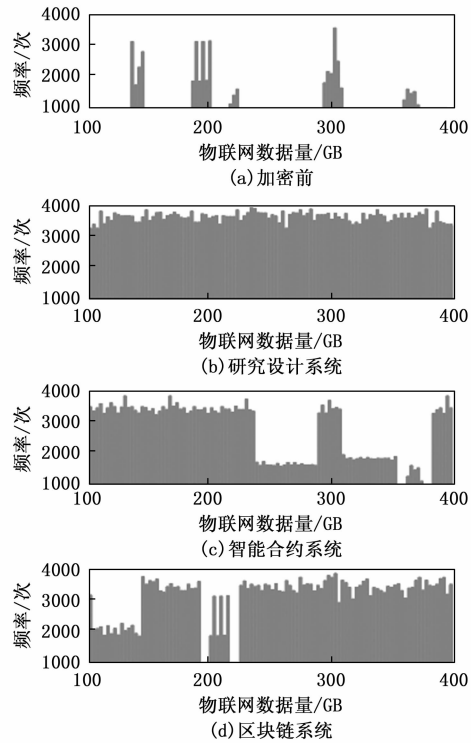

图 8　不同系统应用后物联网数据频率直方图

根据图 8 可知，加密前物联网数据直方图表现出一定程度上频率波动特性，易被侵入者识别。但经过不同系统加密后，物联网数据均表现为类噪声形态，说明 3 种系统均具有一定的加密性能。但是相比之下，研究系统对物联网数据加密后，得到的数据频率直方图的类噪声形态更理想，不存在差异性的频率波动特征。

该实验结果说明利用研究系统加密后的数据分布更加均匀，不存在明显的频率波动特征。这种特性使得入侵者更难以通过分析数据频率来识别出真实数据的模式，从而提高了数据的安全性。在实际应用中，这一系统的优势体现在以下几个方面：①增强了数据保护的匿名性和不可预测性，使得恶意用户或攻击者难以通过常规的数据分析手段来破解或推断出原始数据。②这种加密方式有助于防止基于频率分析的攻击，如频率分析攻击，从而为物联网环境中的数据传输提供了额外的安全层。③理想的数据频率直方图形态也表明系统在处理大量数据时能够保持高效和稳定，这对于需要处理海量数

据的物联网应用来说是一个重要的性能指标。

3.3 安全性测试

为了验证所设计的系统在对恶意用户访问限制方面的优势，对比本研究所设计系统与基于智能合约的访问系统、基于区块链的加密访问系统。设定当恶意用户比例在 10%～60%时，得出 3 个系统的访问成功率，关系图如图 9 所示。

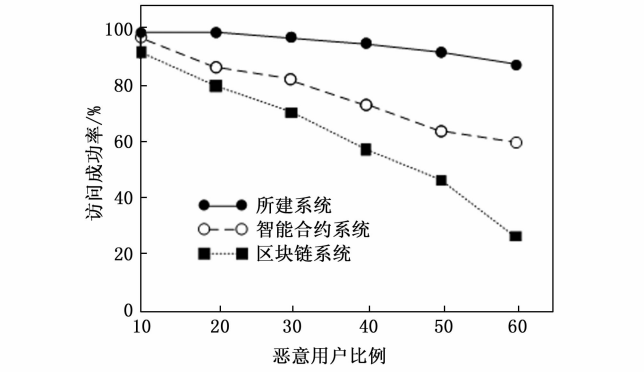

图 9 访问成功率与恶意用户比例关系图

由图 9 可知，本研究所设计系统、基于智能合约的访问系统以及基于区块链的加密访问系统随着恶意用户比例的不断增加，访问成功率都有下降。当恶意用户比例达到 60%时，本研究所设计系统访问成功率也能到到 90%以上。说明即使在恶意用户占多数的极端情况下，系统依然能够有效地识别和阻止未授权访问，确保合法用户的正常使用，这表明系统具有强大的抗攻击能力和鲁棒性。相对于基于智能合约的访问系统和基于区块链的加密访问系统，本研究所设计系统的设计使恶意用户无法修改密钥组件，更大程度上限制恶意用户访问数据的行为，保证访问控制系统安全稳定的运行，这对于依赖物联网进行关键操作的应用场景（如工业自动化、智能医疗等）至关重要。

4 结束语

为了方便用户在信息分享的同时提供更加安全的访问控制技术，设计了基于密文属性的物联网环境私有数据访问控制系统。通过加密物联网的数据属性，产生数据密钥组分及有关参数，由服务器生成密文，把密文储存到数据库中，通过解密服务器对密钥机密得到明文。同时在解密过程中增加属性撤销部分，保证在用户取消访问时，服务器随之更换参数，确保数据不外泄。通过系统测试，本研究所设计系统能在短时间内完成数据加密、解密以及密钥获取。在恶意用户比例增加时，访问系统依然能保证较高的访问成功率，适用于物联网环境下私有数据的访问控制。

参考文献：

[1] 王晨华，侯守璐，刘秀磊. 边云协同计算中成本感知的物联网数据处理方法 [J]. 计算机科学，2022，49 (S2)：820－826.

[2] 宁建廷，黄欣沂，魏立斐，等. 支持恶意用户追踪的属性基云数据共享方案 [J]. 计算机学报，2022，45 (7)：1431－1445.

[3] 张晓东，陈韬伟，余益民，等. 基于区块链和密文属性加密的访问控制方案 [J]. 计算机应用研究，2022，39 (4)：986－991.

[4] 张江徽，崔 波，李 茹，等. 基于智能合约的物联网访问控制系统 [J]. 计算机工程，2021，47 (4)：21－31.

[5] GARCÍA-TEODORO P，CAMACHO J，MACIÁ-FERNÁNDEZ G，et al. A novel zero-trust network access control scheme based on the security profile of devices and users [J]. Computer Networks，2022，212：109068.

[6] KIRAN G M，NALINI N. Ontology-based data access control model supported with grid computing for improving security in healthcare data [J]. Transactions on Emerging Telecommunications Technologies，2022，33 (11)：e4589.

[7] 张泽林，王化群. 基于区块链的工业互联网动态密钥管理 [J]. 计算机研究与发展，2023，60 (2)：386－397.

[8] 韩益亮，郭凯阳，吴日铭，等. 格上基于 OBDD 访问结构的抗密钥滥用属性加密方案 [J]. 通信学报，2023，44 (1)：75－88.

[9] 庞家乐，张 彦. 基于支持完全外包的云存储数据加密方法仿真 [J]. 计算机仿真，2022，39 (9)：483－486.

[10] 刘家森，王绪安，王 涵，等. 云服务器中基于同态加密的关键词检索方案 [J]. 科学技术与工程，2021，21 (8)：3180－3185.

[11] 宋丽华，朱宗科，李梦晨，等. 基于区块链的细粒度物联网访问控制模型 [J]. 计算机工程与设计，2022，43 (2)：352－360.

[12] 宋翔飞，王化群. 一个具有前向安全和后向安全的可验证多关键字可搜索加密方案 [J]. 计算机学报，2023，46 (4)：727－742.

[13] 王静宇，周雪娟. 一种支持属性撤销的密文策略属性基加密方案 [J]. 计算机工程，2021，47 (7)：95－100.

[14] 王经纬，宁建廷，许胜民，等. 面向可变用户群体的可搜索属性基加密方案 [J]. 软件学报，2023，34 (4)：1907－1925.

[15] 王镇道，李 妮. 一种优化的 MD5 算法与硬件实现 [J]. 湖南大学学报（自然科学版），2022，49 (2)：106－110.

[16] 潘瑞杰，王高才，黄珩逸. 基于属性访问控制策略管理方法 [J]. 计算机工程与设计，2022，43 (3)：601－607.

[17] 唐 慧，汪学明. 基于格的多授权密文属性加密方案 [J]. 计算机应用研究，2022，39 (2)：563－566.