论文-访问控制

Towards Activity-Centric Access Controlfor Smart Collaborative Ecosystems

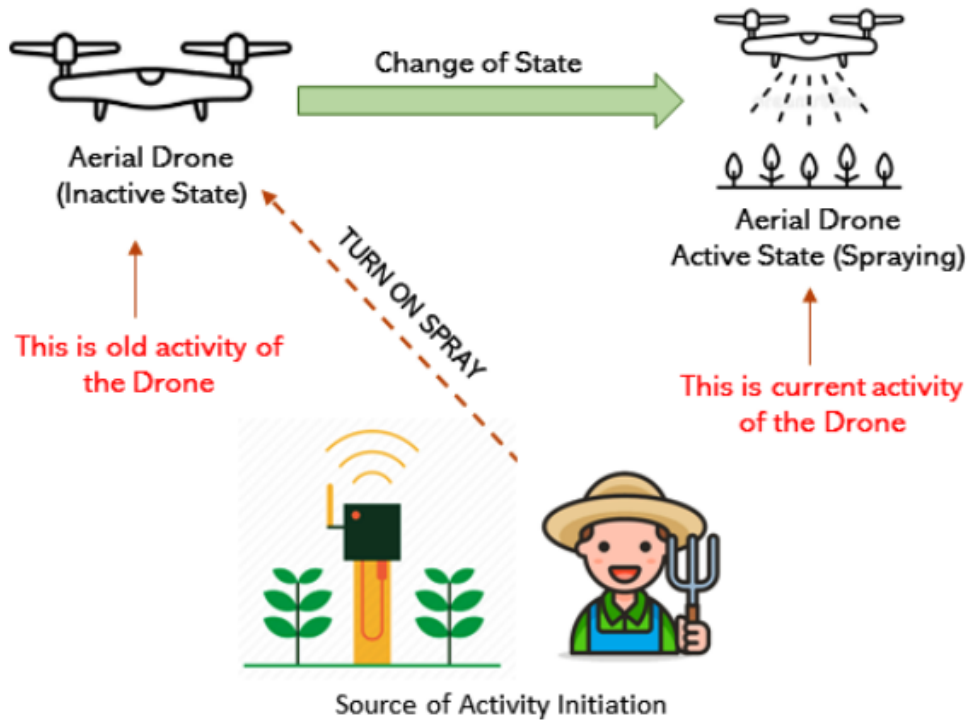


Figure 1: Overview of an Activity.

以活动为中心的访问控制方法，提供了运行时访问控制，考虑到在更广泛的协作和互联智能生态系统环境中发生（或已经发生）的上下文、使用以及各种活动。活动是框架的核心。设备上的活动是由于主体（设备或用户）执行短期或长期功能（即任务）的操作而启动的。在协作生态系统中，这些任务（或活动）通常相互关联而启动的。

图1概述了从非活动到喷洒的活动（或状态）转换。什么是活动？活动是设备的当前状态。它表示设备当前正在执行的操作。设备可以执行一个活动，也可以同时执行多个活动。一项活动是一个持续时间较长的事件。它体现了实体的粗粒度状态，与在实体的不同活动之间转换的授权操作相关。例如，在图1中，处于喷洒活动状态的无人机将以速度、航向、高度等作为其细粒度状态的参数。

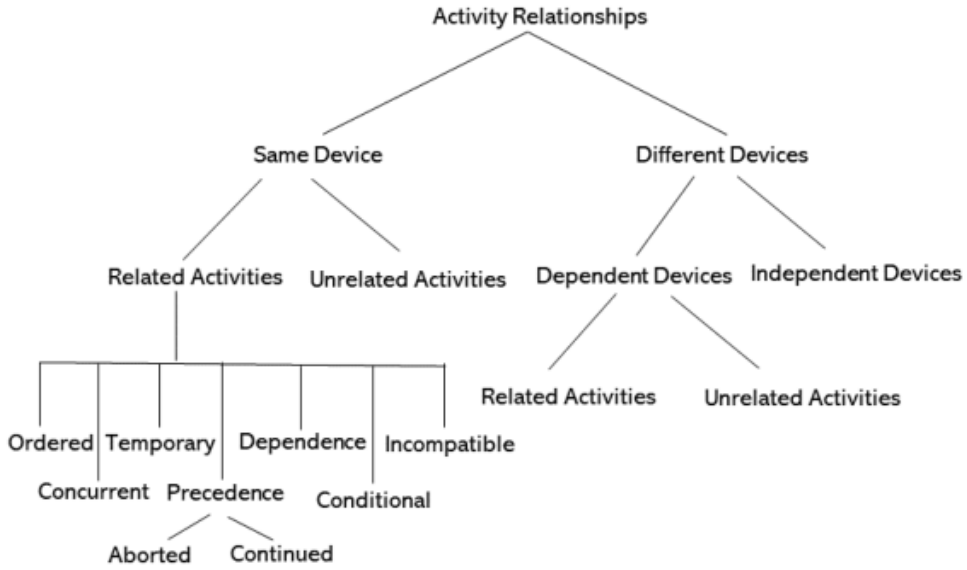


Figure 2: Activity Relation Characterization

Ordered : 仅当以特定顺序启动时，才允许这些活动集。在这种类型的活动关系中，如果活动A需要在对象上启动，那么活动B必须已经启动，或者必须在活动A在相同或不同的设备上完成后启动。这些有序和相互依存的活动可以由相同或不同的主体请求

Concurrent : 这些活动必须始终同时进行，或者允许交替进行。这涉及到彼此相关的活动，或完全不相关且彼此之间没有影响（关系）的活动。活动可以并发，但在不同的设备上，而不是在同一设备上。如果主题a试图启动活动，它会向另一个主题B触发请求或警报，后者应启动其他并发活动。

Temporary : 根据上下文（环境因素）或代理用户/主题（可能是业务部门的管理员），有时可以根据条件允许这些相关活动

Precedence : 可以有一个始终优先于其他活动集的活动。如果请求此类活动，系统中的某些现有（或当前）活动可能会被中止（预先停止或暂时停止），而某些活动可以继续。也有可能新活动只允许在一定的时间内进行，或者上下文很重要，而其他暂停的活动可以在活动完成后继续进行

Dependence : 这些活动集相互依赖。这种依赖可以是并发的、之前的或后续的。因此，并发可以被视为这些活动集的一个子案例

Conditional : 只有满足任何特定条件（或多个条件），才能允许这些相关活动。这些条件可能与启动活动的对象的位置有关，或者如果请求的相关活动位于相同或不同的设备上，或者如果允许新活动，则可能需要启动或停止另一组活动

Incompatible : 这些活动不能同时进行，或一个接一个地进行，也不能在一段时间内进行。这也可能是真的，无论是谁发起的

Efficient Data Access Control with Fine-GrainedData Protection in Cloud-Assisted IIoT

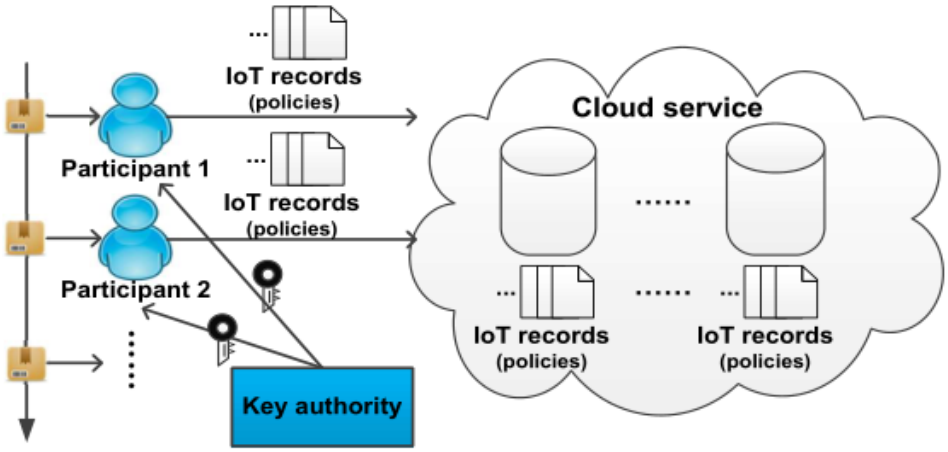


Fig. 2: The direct usage of CP-ABE in a cloud-aided IIoT system.

将云服务构建为一个混合基础设施，由计算服务提供商（CSP）和存储服务提供商（SSP）组成。CSP是位于IIoT域中的私有云，而SSP是位于云域中的公共云。

为了克服CP-ABE的效率障碍，使所有行业参与者能够委托专业配置、资源丰富的云服务来执行昂贵的CP_ABE任务。参与者依靠SSP存储加密的物联网记录，依靠CSP执行CP-ABE任务。

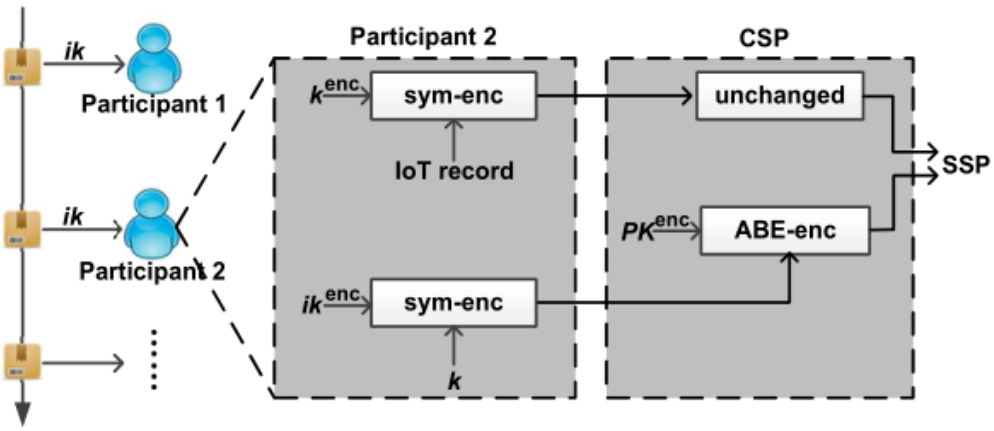


Fig. 3: Work flow of tag-aided encryption technique

对于CSP，CP-ABE的使用提出了三种类型的CP-ABE任务：（1）当参与者提交物联网记录时，它委托CSP为该记录执行CP-ABE加密任务；（2） 当参与者检索物联网记录时，它委托CSP为该记录执行CP-ABE解密任务；（3） 当参与者想要更改其物联网记录之一的策略时，它会委托CSP为该记录执行CP-ABE重新加密任务

委托CP-ABE加密/解密：要将CP-ABE-加密/解密任务委托给CSP，对于物联网记录，参与者使用数据密钥k对其进行对称加密，并要求CSP对ABE加密k。要检索物联网记录时，参与者要求CSP向ABE解密k，并使用k自行解密物联网记录。然而，由于CSP可以访问k，该程序会公开物联网记录的内容。

在参与者之间安全地发布一种名为项目密钥的新型密钥，而无需依赖任何第三方（如密钥机构和云服务）来加密数据密钥，然后再发送给CSP。由于参与者在大型IIoT系统中可能互不认识，我们建议利用RFID标签作为安全媒介，云服务和密钥颁发机构无法访问以分发项目密钥。当标记项目在IIoT系统内流动时，其项目密钥ik自然会发给所有参与方。我们的技术的工作流程如图3所示。

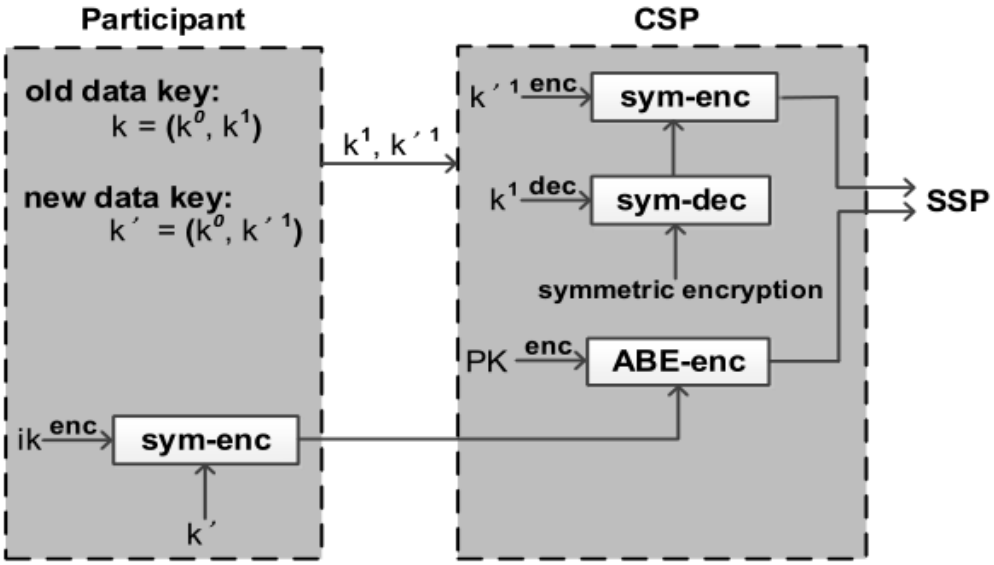
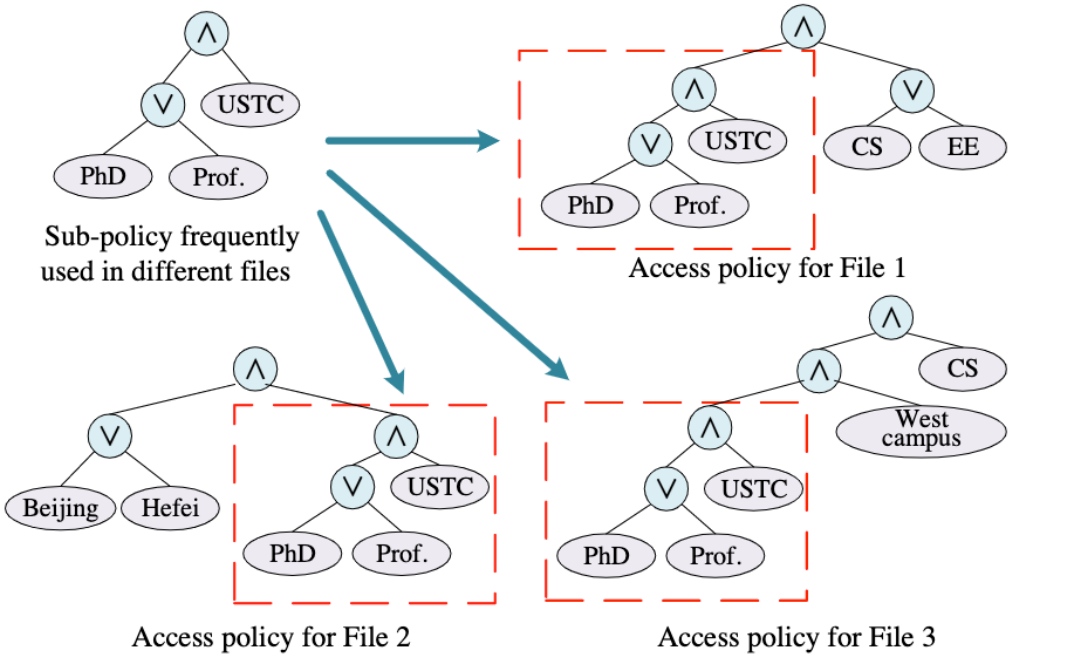


Fig. 4: Work flow of layered re-encryption technique

参与者直接要求CSP重新加密其物联网记录。由于项目密钥的使用，加密的物联网记录由对称密文和CP-ABE密文组成，对称密文通过数据密钥k对记录进行加密，CP-ABE-密文对受ABE密钥保护的项目密钥k进行加密。

委托CSP以保护隐私的方式重新加密对称密文。为此，我们将物联网记录的数据密钥k分为长期部分k0和临时部分k1。物联网记录首先由k0加密，然后由k1加密。k=（k0，k1）仅通过刷新临时部分刷新为新版本k'=（k0,k'1）。通过这种方式，CSP可以使用k1和k'1重新加密从k到k'的对称密文。在这个过程中，长期部分k0仍然受到项目密钥的保护，因此CSP无法对对称密文进行解密。

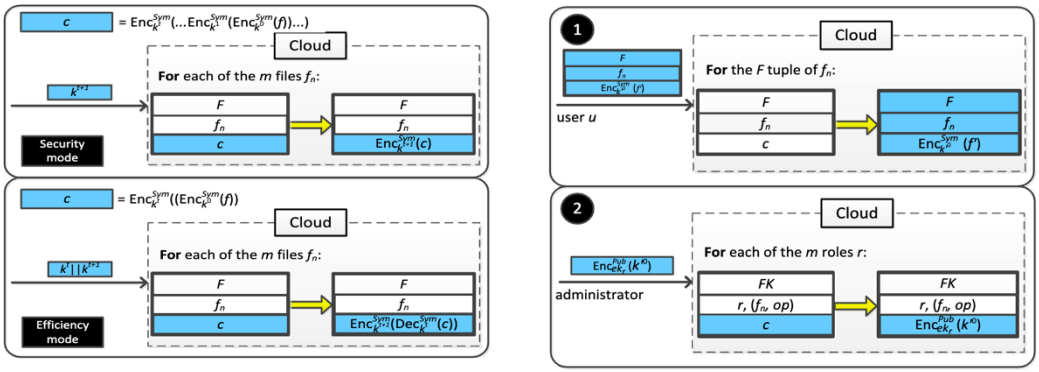
Efficient and Secure Attribute-based Access Control with Identical Sub-Policies Frequently Used in Cloud Storage



提出了一个基于属性的访问控制模型，考虑到所有者将多个文件外包至云服务商，并将文件的访问权限发布给嵌入相同子策略的不同用户集。当所有者首次执行加密算法时，除了加密结果外，相同的子策略参数也可以安全地存储在他/她的设备上。此参数稍后可用于协助执行后续加密。

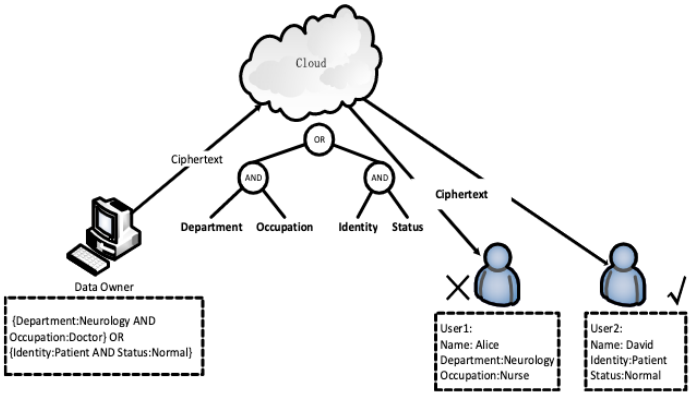
对于用户来说，当他/她首次访问其中一个文件时，解密不仅输出明文，还输出存储在他/她设备中的相关相同子策略参数。将来，当被访问的数据具有相同的子策略并由同一所有者发布时，可以重复使用保存的参数来帮助用户跳过子策略相关的操作，从而显著提高解密效率。

Crypt-DAC: Cryptographically Enforced Dynamic Access Control in the Cloud



一个文件由一个对称密钥列表加密，该列表记录了一个文件密钥和一连串的撤销密钥。在每次撤销中，一个专门的管理员将一个新的撤销密钥上传到云端，要求它用新的加密层对文件进行加密，并相应地更新加密的密钥列表。

A Traceable and Revocable Ciphertext-policy Attribute-based Encryption Scheme Based on Privacy Protection



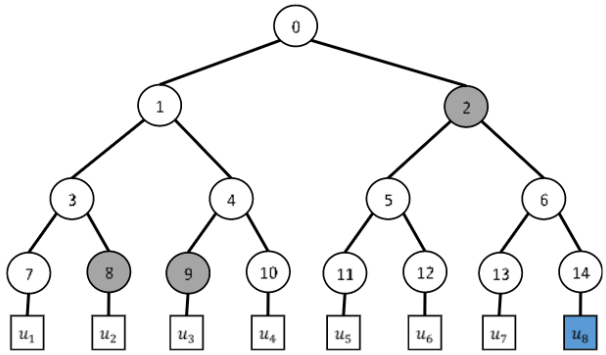


Fig. 2. Binary Tree T

(1) 使用线性秘密共享方案（LSSS）来表示访问策略。属性分为属性名和属性值，用于加密，与密文相关的访问策略只包含属性名。 用户不能知道具体的属性值，这使得策略是部分隐藏的（2）可追溯性：采用白盒可追溯性，通过给定一个格式良好的解密密钥绑定用户的身份，可以追溯恶意用户。 用户的身份信息由系统中所有用户创建的二进制树的叶节点值表示。然后叶子节点值被加密并包含在解密密钥中。用户信息可以直接加密而不需要初始化用户信息列表，（3）撤销：二叉树由所有用户创建，其中叶子节点与用户信息相关。 撤销信息从二叉树中得出，然后在加密阶段进行加密，作为密文的一个独立部分。在追踪用户后且用户撤销列表更新时，只有与撤销列表相关的密文需要被更新。 相比密钥更新需要更新所有未撤销用户的密钥而导致大量的密钥更新开销，密码文本只需要更新一次。

PARBAC: Priority-Attribute Based RBAC Model for Azure IoT Cloud

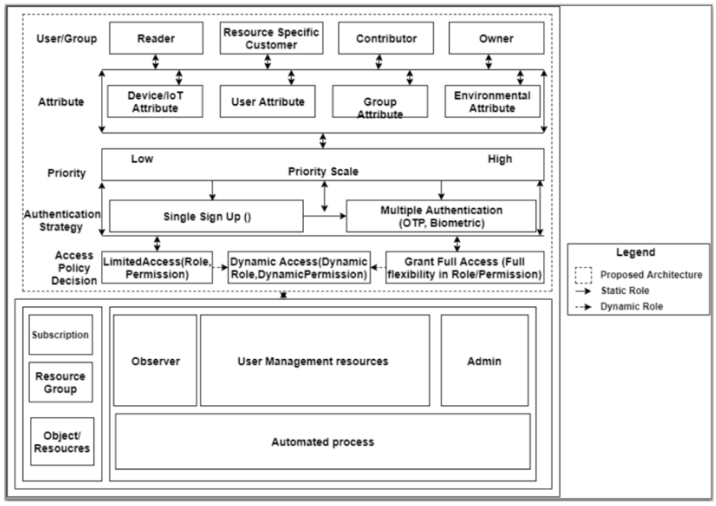


Figure 2: Proposed PARBAC model architecture for Azure IoT cloud

通过纳入简化的基于优先级的认证和授权机制，在进行授予角色之前进行根据属性进行动态角色分配，并且在同一角色请求资源时，根据颁发的优先级来告知服务方对请求进行简化的权限认证还是复杂的权限忍着，这在 Azure 物联网云中提供了灵活性并提高了目前访问控制模型的性能。同时，它利用优先权属性而不是角色来对用户权限进行分类，从而减少了效率低下、无效的情况，并支持对个人政策的一致执行。