# 【AC1】一种面向多维细粒度控制的智能协同认证框架

摘要：5G网络的出现为大规模终端接入和无处不在的物联网带来了广阔的前景。这一进展所引发的潜在攻击机会正在严重影响现有网络的安全堡垒，尤其是边缘接入部分。然而，现有的安全机制由于保护单一、隔离度低，无法有效地消除这些隐患。基于这些事实，我们提出了一个多维细粒度控制（MFC）框架来加强无线接入网（RANs）的安全性和可靠性。首先，我们对现有的安全方案进行了全面的调查和总结，以掌握各自的效果和局限性。其次，建立了MFC框架来描述模型的结构和实现过程。设计了一种标识符映射机制来实现网络隔离。通过对多种策略的理论比较，对MFC进行了安全性分析。第三，通过无线环境参数的设置，建立了一套完整的认证原型系统。说明了具体的验证场景。最后，我们测试了MFC框架的性能。验证结果表明，所提出的方案在访问端具有完整可靠的安全控制。与多方案相比，性能、软件时间和并发性，优化了。因此对于5G或物联网的应用，theMFC框架是可行的。

边缘访问控制，多维认证，唯一用户标识符，双向控制

# 【AC2】基于OBDD访问结构的PHR隐私撤销高效表达访问控制

摘要：随着信息和通信技术（ICT）的发展，医疗行业正在经历一场巨大的变革。健康记录正在数字化，远程存储在云中，并与不同的利益相关者共享。然而，将云用于个人健康记录（PHR）存储带来了数据安全和隐私方面的挑战。基于密文策略属性的加密（CP-ABE）正被广泛地应用于云中PHR的细粒度访问控制。表达能力、效率和属性撤销等是基于云的健康系统的一些关键要求。但是，许多提出的CP-ABE方案依赖于限制性或繁琐的接入结构，从而导致表达能力和效率降低。许多方案还缺乏有效和即时的属性/用户撤销机制。本文提出了一种基于有序二元决策图（OBDD）访问结构的具有属性/用户撤销功能的访问控制方案。在我们的工作中，我们使用属性组的方法来实现属性/用户的撤销。另外，密文和私钥被分配了版本号，以防止被撤销的组成员与未被撤销的成员串通。安全性和效率分析表明，我们提出的方案是安全的、表达性的和高效的。

OBDD可以看作二叉树，文章主要介绍了一个支持撤销的CP-ABE算法。

# 【AC3】多域环境下基于语义业务角色的智能角色访问控制模型与框架

摘要：当今快速发展的通信技术和动态的协作商业模式使得数据和资源的安全性比以往任何时候都更加重要，尤其是在云和网络物理系统（CPS）等多域环境中。它迫使研究界为跨多域分布式环境开发增强的访问控制技术和模型，以便通过考虑变更环境的动态性和访问控制策略的多功能性来满足所有参与组织的安全需求。基于角色的访问控制（RBAC）模型的流行性是毋庸置疑的，因为它的管理开销很低，并且在企业组织中得到了大规模的实现。但是，它没有包含动态变化的策略，并且缺少语义上有意义的业务角色，这可能会对多域业务环境中的访问决策产生不同的影响。本文通过智能RBAC（I-RBAC）模型的实现，描述了我们提出的使用语义业务角色和智能代理的访问控制框架。它包括作为多个领域角色的职业权利。我们使用标准职业分类（SOC）提供的原始职业角色数据集，本文的创新之处在于结合真实世界的语义业务角色和智能代理技术，开发了一个核心I-RBAC本体，以实现高度动态的多域环境下的访问控制。智能代理使用WordNet和双向LSTM深层神经网络从非结构化文本策略中自动填充组织本体。这种动态学习的组织本体与我们的核心I-RBAC本体进一步匹配，以提取统一的语义业务角色。对所提出的I-RBAC模型进行了数学描述，并说明了I-RBAC的总体框架及其实现架构。最后，通过实现结果验证了I-RBAC模型在存在大量权限分配和多个查询时的线性运行趋势。

# 【AC4\*】基于令牌的访问控制

摘要：传统的集中式访问控制在健壮性、可信性和可循环性等方面存在不足。区块链具有容错和信任的优势。智能合约具有自动执行和灵活扩展的特点。令牌可以很好地记录凭证信息，并且易于传输。本文将区块链、智能合约和代币相结合应用于访问控制，以解决传统访问控制的不足。首先，简要介绍了访问控制、区块链、智能合约和代币。其次，给出了访问控制令牌的一般数据结构，详细阐述了访问控制令牌的等价、拆分、合并和验证算法，并阐述了基于令牌的访问控制系统结构。最后，通过一个基于令牌的访问控制仿真系统，验证了基于令牌的访问控制在健壮性、可信度、流通性、并发性等方面具有一定的比较优势。

本文将区块链、智能合约和代币统一起来，将区块链作为一个可信、安全的存储和运营环境，充分利用智能合约自动执行和代币高效智能流通的特点，提出了一种基于令牌的访问控制（TBAC）。TBAC的解决方案旨在实现以下目标：1）分布式可信访问管理模式；2）灵活高效的访问传输模式；3）高频率容错访问执行机制。

将令牌应用于访问控制，以区块链网络作为存储、认证和流通环境，以智能合约发布和应用为逻辑处理形式，以令牌为数据体，记录访问控制的规则和逻辑，执行访问控制的认证处理，确保正确的主体正确地访问正确的对象是一种称为基于令牌的访问控制的访问控制模式。

结构：分布式数据共享是一种典型的分布式应用系统。基于TBAC的分布式数据共享技术机构如图3所示。在基于TBAC的分布式数据共享体系结构中，主要有以下几个对象。

1. 数据提供程序（DP）。作为数据共享网络的供应方，数据提供者可以是数据的生产者、管理者、经营者等，数据可以分为各种类型，如结构化数据、非结构化数据、原始数据和二次处理数据。随着5G时代的来临，越来越多的数据以分布式的状态在多个对象数据库中生成和存储，这些数据库可以是一个专有的数据库，也可以是大型的共享数据中心。为了向更多的需求方提供数据服务，在该方案中，许多数据提供者通过数据服务节点在区块链上注册自己的数据，以方便对需求方的搜索和获取。
2. 数据请求者（DR）。作为数据共享网络的需求方，数据需求方可以是个人、企业、机构等。数据需求者通常需要从多个数据提供者获取数据。他们可以通过数据服务节点直接从区块链进行搜索，或者在区块链上注册自己的需求，以方便数据提供商按需提供数据。数据需求方只能根据数据提供者发布的、数据所有者授权的ACT，通过数据服务节点向数据提供者请求数据访问。
3. 数据所有者（DO）。作为数据共享网络中数据认证的主体，数据认证主要决定数据所有权的主体。未经数据所有权主体许可，数据的其他角色不能非法处理数据。数据的所有权可以是单一的独占实体，也可以是多共享的实体。同一个实体也可能有大量的数据分布在不同的数据库中。因此，在该方案中，数据认证也记录在区块链上，实现分布式授权。在现实中，DP和DO可以是同一主体，也可以是单独的主体。区别在于数据是由DO本身管理和提供的，还是由DP代表它来管理和提供的。DP和DO可以是ACT的独立或联合发布者。
4. 数据服务节点（DSN）。数据服务节点是一个区块链节点，通过TBAC程序进行发布。ACT的产生、撤销、转移和处理可以通过TBAC程序和区块链程序共同实现。通过数据提供者和请求者的连接，可以实现分布式授权和分布式权限处理的目标。数据服务节点可以在网络中进行多个分布式部署，数据提供者和数据请求者可以灵活地选择不同的数据服务节点来提供或获取数据服务。
5. 区块链。区块链作为一种分布式数据共享数据服务总线（DSB:data service bus），既是ACT的存储载体，也是ACT的执行环境。它的特点有助于形成开放的访问控制机制，突破传统访问控制机制的安全瓶颈、并发瓶颈和流程瓶颈。

基于TBAC的分布式数据共享主要通过DSN来实现。在这个节点上，不仅需要一般的区块链节点服务功能，还需要访问控制的基本功能。这些功能包括管理、判断和ACT过程。

1. ACT管理（ACTM）：主要实现ACT的产生、撤销和转移等功能。为了更方便地实现对ACT的管理，除了建立ACT数据库外，还需要创建和管理metadata数据库和ACT模板数据库。metadata是正确理解和统一整个系统语义的基础。任何授权节点应用都可以通过该模块根据需要创建管理访问控制的基本信息，并将相应的密钥信息和原始数据以哈希的形式存储在区块链上。ACT模板是为了方便ACT的创建和统一管理而设计的ACT的metadata、ACT模板和其他原始数据可以直接保存在区块链上，也可以保存在链下分布式数据库中。考虑到链上不能保存太多的数据，因此最好使用链下的分布式数据库。
2. ACT判断（ACTJ）：从ACT处理器获取访问请求，并根据访问请求调用相关的ACT信息、元数据信息和ACTT信息，根据访问控制规则计算逻辑，最后给出访问控制决策结果并返回给ACT处理器。
3. ACT过程（ACTP）：用于接收来自数据请求者的访问请求，调用ACTJ来决定是否以及如何开始数据访问，最终通过数据提供者提供的通道获取允许的对象数据。

总结：本文结合区块链、智能合约和ABAC的特点，提出了一种新的基于ACT的访问控制机制TBAC。与传统的集中式访问控制相比，TBAC在安全性、可靠性、流通性、并发性等方面具有一定的比较优势，TBAC在分布式数据共享中的应用有利于形成一个具有抗攻击、高容错、抗篡改、抗抵赖的数据服务网络，易扩展、高并发性，更好地促进更大范围的数据互联。

本文在讨论链上ACT的存储时，也将其透露给整个区块链网络。虽然其他节点不能使用该ACT，但通过对该ACT的分析，有可能获得一些持有者不愿意公开的信息，比如他们的权限信息。因此，本文下一步的工作就是如何保证该ACT的信息不被泄露，但可以被证实。

实际上就是把访问策略放在token中，token放在区块链上，用户根据Token中的限制确定自己是否满足访问策略。用户向区块链申请访问数据，区块链根据用户信息与数据的Token中的访问策略比对，如果满足则提供数据。

和Disac比不同之处在于：访问控制是由区块链完成的，Disac的访问控制是在每个用户本地完成的。区块链避免了风闻控制的单点失效问题，但需要构建一个相对比较完善的系统，比如需要区块链中的多个peer提供服务。并且如果数据提供方和数据所有方不是同一个体，则数据明文放在数据提供方处也有一定的风险。

# 【AC5】FADB：一种基于区块链的VANET数据细粒度访问控制方案

摘要：V-Ad hoc网络是智能交通系统的重要基础，广泛应用于交通管理、自动驾驶、道路优化等领域。随着VANET的逐步普及和进一步发展，产生了大量的VANET数据。然而，当使用vanetdata为用户提供服务时，它会对安全和隐私提出挑战。本文结合块链和基于密文的属性加密（CP-ABE）技术，提出了一种基于区块链的VANET数据细粒度访问控制方案。在FADB中，我们使用区块链来代替第三方服务提供商来管理用户身份和数据存储和不同的VanetDataAccessRights可以根据属性设置. 通过改进CP-ABE，轻量级VANET设备可以将复杂的加密和解密操作外包给更强大的用户，并进一步改进EF最终数据访问能力通过仿真测试和安全性分析，证明FADB可以提供有效的数据安全性和较低的性能开销。

# 【AC6】基于安全数字证书的区块链数据访问控制方案

摘要：以前区块链中的合约协议通过使用集中可信节点来确保其公平性和可追溯性。如果可信节点是不诚实的或与签名者合谋，那么其他节点就会受到损害。同时，参与者节点敏感信息的泄露对区块链中数据访问的隐私安全构成严重威胁。针对这一问题，本研究提出一种基于数字证书的安全控制方法。该方法将区块链技术与数字证书技术相结合，设计了一种不需要验证第三方参与者加密身份签名的区块链隐私数据安全认证协议。本文提出的高效网络转发协议可以支持多个签名者通过区块链进行Fair Contract Signing。该协议可以保护合同的隐私和参与者的身份。实验结果表明，所提出的方案在通信开销、存储开销和检测率方面都优于其它方案。

加密的签名

本文的主要贡献如下：1）提出了基于特征的区块链数据划分方案，并建立了与密钥的关系。当用户执行查询时，使用与密钥相关的访问控制策略来评估查询是否合法，从而实现数据访问控制。2） 设计了一种基于区块链的通信协议，包括通用时隙协议、开销平衡策略和容错策略。3） 为了保护数据访问者，实现了一个公开的匿名认证。此外，设计了三种分布式证书检测方法，以避免恶意非用户对证书的破坏。实验结果表明，该方案对合谋攻击和节点捕获攻击具有良好的防护能力。此外，用户的可听性、通信成本、存储成本和检测效率令人鼓舞。未来的研究应改进现有方案，并将其应用于实际区块链节点。在大规模事务处理中，我们将进一步研究同态属性加密和存储空间平衡等理论，考虑低延迟存储模块的需求，探索分层可插拔存储模型。此外，为了提高存储模块的效率和可扩展性，研究了海量数据环境下的并行可扩展分布式存储方案。

# 【AC7\*】AuthPrivacyChain：一种基于区块链的云端隐私保护访问控制框架

摘要：云是一种提供共享和支持无处不在的按需访问计算的计算模式，为许多行业提供了新的数据处理和服务，显著降低了用户的计算和存储成本，提高了易用性。随着云规模的不断扩大和云计算的集约化，云安全已经成为云计算领域的一个重要问题。访问控制是保护企业和个人存储在云中的敏感数据的关键安全技术之一。由于云端采用集中访问控制机制，云中的敏感数据容易被黑客或云内部管理人员篡改或泄露。为了解决这个问题，我们提出了一个基于区块链的访问控制框架，该框架具有隐私保护功能，称为AuthPrivacyChain。首先，我们以区块链中节点的账号地址作为身份，同时重新定义云数据的访问控制权限，并对云进行加密存储。在此基础上，设计了AuthPrivacyChain中的访问控制、授权和授权撤销过程。最后，我们实现了基于authChain的授权用户访问企业资源的安全机制（authChain），并最终实现了基于授权链的用户访问隐私的安全机制。

本文提出了一种基于区块链的访问控制框架AuthPrivacyChain来解决上述问题。我们的贡献如下：

1. 分散访问控制体系结构。Authprivacychain利用去中心化、防篡改的区块链[23]-[25]存储访问控制权限，以区块链账户地址为身份，设计访问控制、授权和授权撤销流程。
2. 授权隐私保护。由于区块链的透明性，很容易泄露用户隐私。Authprivacychain在区块链中加密存储访问控制权限，有效保护用户隐私。
3. 安全。Authprivacychain不仅能保证资源的机密性、完整性、可用性、真实性和责任性，还能抵抗各种外部和内部攻击。

为了解决上述问题，我们提出了一种基于区块链的访问控制框架AuthPrivacyChain。本节包含系统模型、初始化、访问控制、授权和吊销。系统模型如图2所示，由四个实体组成：

•云。它为用户提供身份验证和数据存储。云通过区块链确定DU或DO的访问权限。

•区块链。它具有开放、透明、防篡改、不可逆等特点，与分布式数据库一样，我们将其作为访问控制的授权策略数据库。

•DO。将资源上传到云并发布资源对区块链的访问权限。

•DU。如果DU有云的许可，他可以访问这些资源。

我们假设云是半可信的，即云的软件、硬件、非对称密钥和业务流程是可信的，而云SA是不可信的。区块链被认为是可信的。首先，将资源上传到云端，然后通过区块链中的注册交易发布授权。DU向云发送资源请求，云查询区块链，判断请求是否有权限，最后回复请求。

云、DU\DO先在区块链上注册，拥有账号和私钥等信息。当有数据资源发布时，数据上传到云端，数据的metadata发布到区块链上，这两个步骤都可以通过区块链的功能完成。访问控制是用户在云中请求资源，云根据区块链中存储的权限决定用户是否可以访问资源。如果用户有权限，云将允许用户访问资源，访问记录将存储在区块链中。

授权相关信息直接存储在区块链中。访问记录也存储在区块链中。对于性能，在身份验证方面，AuthPrivacyChain优于传统的访问控制，因为它使用Addr而不是用户名和密码。在身份认证授权和访问控制方面，AuthPrivacyChain略低于传统的访问控制，因为它需要访问区块链，但可以通过选择合适的超级节点来访问区块链来缩小差距。

还是针对云存储，只是访问控制转移到区块链上了。

# 【AC8】FGACFS:\*nix用户空间文件系统的细粒度访问控制

摘要：在本文中，我们介绍了fgafs-一个细粒度的访问控制文件系统，它是为创建和管理\*nix操作系统家族中的共享访问而设计的。提出的访问控制模型扩展了POSIX-acl。它的基本特征是：1）可执行权限的广泛列表，2）分离文件和目录权限，3）两种不同的权限继承机制—一种用于经典继承，另一种用于复制新创建对象的权限。总的来说，有19个文件和29个目录权限类型。这些权限被设计为在单个工具中实现，并允许同时控制系统用户和程序。

为了评估我们的方法，我们基于这个模型开发了一个软件实现。FGACFS是通过实现FUSE接口创建的用户空间文件系统。我们的文件系统独立于底层网络和磁盘文件系统。在我们的实验中，我们评估了两种不同的权限存储方法和一种我们开发的用于加速操作的权限缓存方案。进行的性能测试显示了我们方法的效率，并证明我们的解决方案已经准备好部署并至少在小型工作组中使用。

# 【AC9】一种高效的基于隐私增强属性的访问控制机制

摘要：随着网络研究的迅速发展，基于属性的访问控制（ABAC）以其良好的表现力、灵活性和可扩展性，越来越受到人们的关注。不幸的是，收集用户属性是完成标准ABAC决策过程所必需的，这增加了隐私泄露的风险。这个问题增加了公众对ABAC的怀疑，阻碍了ABAC的普及。该文通过引入一种新的基于哈希的二叉搜索树，提出了一种隐私保护和高效的基于属性的访问控制（EPABAC）方案，以防止ABAC决策过程中访问主体的隐私泄露。分析和实验结果表明，EPABAC在可接受的额外计算开销下，实现了决策过程中的用户隐私保护。

针对上述问题，本文提出了一种支持隐私属性保护的访问控制机制，在不泄露用户敏感属性的前提下，支持隐私访问决策。首先，利用hash函数的单向性，提出了一种基于hash的二叉搜索树结构和相应的生成器，保证特定生成器的持有者只能获取树中相应叶节点的信息，并将上述结构引入ABAC模型，将访问控制决策过程转化为一个基于特定哈希的二叉搜索树生成器的挑战。其次，根据ABAC模型中属性的性质，提出了一种将访问控制规则和属性分别转换为基于hash的二叉搜索树中的挑战和生成器的方法。最后，我们对该机制的性能和安全性进行了测试，结果表明，该机制在实现隐私访问决策过程的同时，能够抵抗用户欺骗攻击，具有可接受的性能。我们工作的主要贡献总结如下。

1. 利用hash函数的单向性，提出了一种基于二叉树结构的数据结构和相应的方案，以支持ABAC模型中的决策过程，保证被验证人只能回答发生在其权限范围内的挑战。
2. 在标准的ABAC授权阶段和决策阶段引入哈希二叉搜索树，在不暴露静态用户属性值或被用户欺骗的情况下，实现了正确的决策。
3. 通过引入非对称加密和数字签名，我们将隐私增强方案中的决策过程从在线第三方的参与中解放出来。
4. 我们从理论上分析了EPABAC模型的有效性和效率，并通过实验评估了其有效性和效率，以证明我们在可接受的开销内增强了隐私保护。

EPABAC模型在标准ABAC模型的基础上扩展了属性的授权和决策机制，实现了对隐私属性的保护。如图1所示，在授权阶段，对于每个敏感属性，属性权威（通过颁发属性证书来分配权限的权威）将根据客户端的相应值向客户端发送一组证据生成器，而非敏感属性的处理与经典ABAC解决方案（步骤1和步骤2）中的方法相同。此后，在决策阶段，当客户端发起访问请求时，服务提供商将首先收集所有涉及的非敏感属性，然后由标准ABAC匹配组件处理（步骤3）。随后，对于每个敏感属性，服务提供商将要求用户提供满足策略的证据，这些证据将在隐私模块中进行验证。请求的证据独立于对象的属性值，可以使用证据生成器计算（步骤4）。最后，服务提供商将综合隐私和非隐私属性的决策结果，并通过强制执行工具实现访问控制（步骤5）。

是将用户的隐私属性保护起来，不直接传输属性内容，而是将属性输入生成器，输出属性证据，将属性证据传给验证方，通过对证据的验证得出结果，期间验证方不清楚用户具体的属性。没有涉及基于属性的加密。不过属性的保护是一个启发，大部分算法不考虑用户属性的泄露，因为使用属性本身就是对用户身份的一种保护。

# 【AC10】云计算访问控制机制研究综述

摘要：基于互联网的应用和服务在今天的云计算技术中给最终用户带来的好处是非常显著的。通过在后台使用一些机制，可以实现云计算提供的互联网上即时扩展的分布式服务。对最终用户来说，控制对资源的访问是一项至关重要的任务，因为缺乏控制往往会导致安全风险。此外，这可能导致系统故障。本文描述了七种不同的访问控制机制在云计算平台中的不同用途。此外，还讨论了从以前的基于服务的体系结构中开发并用于云计算的各种模型的优缺点详细分类。期间这些评估、NIST的衡量指标作为参考，以及在研究中，对过去十年的109篇文章进行了审查。我们还将我们的研究与现有的调查论文进行了比较。

# 【AC11】NDN中基于CP-ABE的多权限可撤销访问控制方法

摘要：对于互联网的未来，由于信息中心网络（ICN）在内容分发、移动性和安全性等方面具有天然的优势，被认为是解决当前许多问题的潜在解决方案，甚至是关键。命名数据网络（NDN）是美国发起的网络体系结构研究项目之一。NDN是一个比ICN更受欢迎的项目。NDN中的信息缓存将内容与内容发布者分离，但由于缺乏安全控制，内容安全受到威胁。因此，需要提出一种基于CP-ABE的多权限可撤销访问控制方法。该方法构造了一个代理辅助的访问控制方案，该方案能够在NDN网络中实现有效的数据访问控制，具有较高的安全性。由于在NDN节点上进行了部分解密，减轻了用户客户端的解密负担，实现了有效的用户和属性撤销，保证了前向安全和后向安全，防止了合谋攻击。最后，通过对本方案的其他安全性和性能分析，证明了该方案是安全有效的。

只是对数据进行了CP-ABE加密

# 【AC12】基于匿名分散属性的云辅助物联网访问控制

摘要：基于属性的加密（ABE）作为一种强大的加密工具，在云辅助物联网数据共享等广泛应用中带来细粒度访问控制。随后，提出了具有不可信属性权限的分散ABE来去除在线可信权威（TA）。在分散体系结构中，用户作为数据客户（如物联网设备）将其属性提交给不可信的权威机构以获取私钥。在该架构中，用户的隐私，针对不可信的权威，是一个必须确保的重大挑战（例如，e-health云应用程序）。本文针对分散式ABE中的隐私问题，在标准模型中提出了一种新的基于属性的匿名分散加密算法。它以一种有效的方式保护用户对权威机构的匿名性。在我们的解决方案中，我们使用加密累加器匿名验证用户的属性。然后，在密文中加入累加器，以保证对未授权用户的访问控制。

此外，在某些应用中，访问结构（加密/解密策略）包含敏感信息，应该从每个人（不包括密钥属性满足访问结构的用户）中进行模糊处理。为了保证隐藏策略的安全性，我们提出了一种高效的分散策略混淆技术来保护策略对公共云服务器（PCS）的隐私性。对于一个分散的环境，权威不受信任，可能与PCS串通。

为了适用于物联网资源受限的设备，我们将昂贵的解密计算外包给强大的云服务器。然后，我们正式分析了该方案的安全特性，并进行了实验验证。最后，我们简要地解释了提案的特性如何满足一些实际应用的需求。关键词：基于属性的加密、解密外包、隐私、隐藏策略、云辅助物联网。

主要针对不可信的AA。如何隐藏用户属性。

# 【AC13】基于区块链的知识管理系统访问控制的ECDSA方法

摘要：由于很难建立安全机制和防止恶意用户模仿角色，访问控制在一些组织中变得有问题。此外，用户在参与角色、甚至控制角色方面没有灵活性。为了缓解这些问题，人们提出了几种基于角色的访问控制（RBAC）机制，但其安全性并没有得到充分的实现。然而，在这项工作中，我们提出了一个基于区块链技术的RBAC模型，以在知识管理系统（KMS）中访问和使用知识之前增强用户身份验证。我们基于区块链的系统模型和智能合约确保了透明度和知识资源的不变性。我们还提出了智能合约算法，并对模型进行了讨论。作为应用于KMS环境的RBAC模型的重要组成部分，信任在网络中得到了保证。评价结果表明，该系统是有效的。

# 【AC14】下一代大数据联盟访问控制：一个参考模型

摘要：本文讨论了下一代大数据（BD）联合平台最重要的挑战之一，即Hadoop访问控制。联邦范围内的隐私和安全仍然是业界和学术界的重要关注点。Hadoop当前的原始访问控制存在安全问题和限制，例如部署的复杂性和资源的消耗。然而，这一重大关切并不是文献中深入研究的课题。本文对这些安全限制进行了严格的回顾和研究，并提供了一个名为BD federation access broker的框架来解决8个主要的安全限制。本文提出联邦访问控制参考模型（FACRM）来形式化apachehadoop堆栈中安全BD解决方案的设计。此外，本文还讨论了访问代理的实现及其在安全漏洞检测和数字取证调查中的作用。所提出的访问代理的效率并没有持续地影响性能开销。实验结果表明，在WebHDFS中，每100mb的读/写操作只占1%。总的来说，本文的研究结果为Hadoop堆栈安全性和隐私性的一系列革命性和最先进的增强以及未来趋势铺平了道路。

# 【AC15】分布式权限管理的访问控制模型

摘要：访问控制是保护敏感信息和关系系统资源的重要机制。传统的访问控制模型，如DAC、MAC、RBAC等，由于缺乏动态的权限管理，已不再适用于开放式网络。网络节点的增加使得信息存储和资源访问变得分布式。传统的访问控制模式由于采用集中管理模式，具有适应性差、部署和应用模式单一等特点。因此，这种访问控制环境不可避免地给访问控制授权带来访问控制压力。为了克服传统访问控制模型的不足，本文提出了一种新的访问控制模型DMPAC（Distributed management of permission for access control model）。该模型的授权机制具有分布式、动态管理的访问权限，模型覆盖的所有节点都有机会参与访问和控制的执行。DMPAC模型在安全访问和动态管理方面提供了传统访问控制模型的优点。文中还描述了模型的框架和执行过程，以及DMPAC在访问控制中的应用。最后，我们将给出一些实验结果，证明DMPAC在通过访问权限管理来保持分布式访问控制的有效性的同时，可以达到传统访问控制模型的性能。

基于分布式授权的访问控制模型的设计原则是改变传统的基于单一集中式访问控制的授权访问模型。分布式管理的实现过程是将传统的访问控制矩阵或访问控制列表以访问控制列表的形式存储到该访问控制模型所覆盖的参与访问并与其有访问关系的每个节点。也就是说，每个节点存储自己的可访问节点和自己的控制策略，同时为自己访问的节点授权代理。采用分布式访问控制策略代替传统的集中式访问控制矩阵，网络中与之有访问关系的节点管理整个网络的访问控制策略。这种方法可以改变传统的访问控制策略集中存储部署模式单一、适应性差、容易受到网络攻击的缺点。同时，分布式访问控制策略的管理模式更加安全，防止了访问控制策略在执行过程中被篡改的可能性，从而在保护网络资源的安全访问方面起到更科学的控制作用。传统的访问控制鉴别存储在中心或接入端进行鉴别，这将给中心节点或访问控制的访问者带来更多的策略分析。

相当于建立了一个分布式的访问控制框架，分布式是因为有很多节点都能进行访问控制，而不是单纯的一个节点。

# 【AC16】基于属性的加密在移动云计算安全数据访问控制中的应用——一个案例研究

摘要：云计算已经成为一种重要的模式，吸引了许多业界和学术界的用户。很多人每天都在使用云，而不知道它的技术。所有版本的电子邮件、驱动器、对未实际安装在本地系统上的应用程序的访问—它们利用云的功能。移动云计算（MCC）通过移动设备为用户提供基于云的服务。与移动设备共享/上传到公共数据存储的数据提高了生产效率，但另一方面也带来了安全漏洞。在基于属性的加密（ABE）方案中，属性是从移动设备中动态收集的。它在生成用于加密数据的公钥和控制用户访问策略方面起着至关重要的作用。作者回顾了为移动云计算环境提供安全数据访问控制的ABE方法。

# 【AC17】智能健康防护的效率和安全属性访问控制体系结构

摘要：智能医疗系统有望显著提高医疗服务质量。这些系统保存患者相关记录，并通过不安全的公共通道提供服务，这可能会导致智能健康系统中的数据安全和隐私问题。另一方面，基于密文属性的加密（CP-ABE）提供了可能的加密数据安全性。CP-ABE中存在一些安全缺陷，现有的访问策略是明文形式的，用于访问加密的敏感数据。另一方面，它支持小属性宇宙，这限制了CP-ABE的实际部署。此外，外部对手观察到了通信，这也对CP-ABE模式造成了严重威胁。为了克服安全和隐私风险，设计并下放了医疗服务的有效访问控制。虽然我们也对Zhang等人提出的方案进行了安全性分析，但该方案容易受到无效的安全证明和中间人攻击。在所提出的方案中，我们提出了一个高效且安全的保护方案，以克服Zhang等人的系统的弱点。该协议通过隐藏访问策略来满足医疗用户的属性值。在标准模型下进行了验证，保证了协议的安全性。性能分析比较表明，该方案比现有方案更有效。

# 【AC18】SBAC：一种基于安全区块链的以信息为中心的网络访问控制框架

摘要：信息中心网络（ICN）的提出是为了满足人们对高效内容交付日益增长的需求。然而，ICN的网内缓存机制给内容提供商（CPs）提供数据安全性和隐私性带来了困难。虽然人们提出了许多访问控制方案来提高ICN的安全性，但是仍然存在一些问题没有解决。一方面，尽管提出了集中式访问控制方案来提高数据共享的安全性，但单点故障问题不可避免。另一方面，分散访问控制方案允许内容提供者控制加密内容的密钥分配，但将其应用于分层访问时效率低下，并且忽略了对内容访问的审核。本文提出了一种基于区块链的安全访问控制框架SBAC，为内容提供商提供对其内容的安全共享、审计和撤销能力。具体来说，我们设计了一种基于匹配的访问控制模型来实现分层访问，并提出了一种基于区块链的访问令牌机制来抵抗单点故障，平衡隐私和审计。在验证过程中引入布谷鸟过滤器，实现对访问令牌的高效查询。此外，我们的SBAC保持了ICN的普适缓存特性。安全性分析和实验结果表明，SBAC是可行的。

在本文中，我们构建了一个基于区块链的安全访问控制框架（SBAC），以解决上述对ICN的挑战。在SBAC中，为分层访问设计了基于匹配的访问控制模型，并提出了一种基于区块链的访问令牌机制来传输访问令牌和审计内容访问。总之，我们作出了以下贡献。

•提出了一种基于区块链技术的ICN安全访问控制框架，保证用户对发布内容的完全控制。

•为了解决“区块链上/下”的同步问题，现有的区块链钱包不仅可以处理区块链上的交易，还可以管理区块链外的访问，例如生成/验证访问令牌、内容管理和ICN缓存。

•为了实现高效的访问，采用基于匹配的访问控制模型将一个访问令牌映射到多个资源，并引入布谷鸟过滤器，以避免令牌验证过程中强制遍历整个区块链的开销。

•我们分析了所提出框架的安全性，并评估了原型的性能。

和加密签名没有太大关系，只是在区块链上做了访问控制

# 【AC19】具有细粒度访问控制的隐私保护区块链

摘要：本文提出一种简单、高效、易于使用的机制，为传统区块链添加隐私和细粒度访问控制功能。它使用标准的密码算法和技术，以及一个新的密钥导出算法和一个模糊抽取器组件（从生物特征中导出密码密钥），使得非专家用户的访问控制功能非常简单。这样的区块链适合在长期隔离的环境中存储参与者的数据记录。

在这篇文章中，我们提出一个密码方案来构造一个隐私保护区块链，对谁可以读取特定的条目进行细粒度的访问控制。这个新方案采用了一个基本的区块链结构，并为存储在链上的数据（在典型的区块链实现中没有的属性）添加了隐私和访问控制。该方案的一个重要组成部分是一种新颖的密钥导出算法，该算法在安全地构造对用户希望共享的数据的各个部分进行细粒度访问控制所需的所有密钥的同时，最大限度地减轻了用户的负担（就用户需要记住的内容而言）。所提出的机制简单、有效，即使对精神健康状况恶化的参与者也非常容易使用。

没太大关系。

# 【AC20】一种可伸缩的基于属性的云存储访问控制方案

摘要：如今，云服务器已成为全球多个用户存储和共享数据的主要选择。使用云服务器共享数据的主要挑战是保护数据不受不信任的云服务提供商和非法用户的攻击。基于属性的加密（ABE）已经成为一种有用的加密技术，可以以细粒度的方式与合法接收者安全地共享数据。已经有人提出了几种使用ABE的解决方案来使用云服务器安全地共享数据。然而，大多数解决方案都是以数据所有者为中心的，侧重于为数据所有者提供对其外包数据的完全控制。现有的云计算解决方案无法在用户之间提供共享访问权限，也无法使云用户灵活地委托其访问权限。为了同时实现细粒度访问控制、可扩展性的概念，并为云用户提供共享访问权限和访问权限授权的灵活性，提出了一种基于属性的可伸缩云存储访问控制方案。该方案扩展了基于密文策略属性的加密机制，实现了访问权限和共享访问权限的灵活委派，并具有可扩展性和细粒度的访问控制。该方案利用用户的层次结构实现了可扩展性。此外，基于密文策略属性加密的安全性，我们正式证明了我们提出方案的安全性。我们还实现了该算法，以显示其可扩展性和高效性。

实际上是对一个属性相同的小组内的用户实行权限共享，减少了不必要的密钥生成等操作，主要是一个算法。

# 【AC21】时间和属性因素相结合的公共云时间敏感数据访问控制

摘要：将数据外包到云端的新模式是一把双刃剑。一方面，它将数据所有者从技术管理中解放出来，并且更容易让数据所有者与预期用户共享他们的数据。另一方面，它对隐私和安全保护提出了新的挑战。为了保护数据的机密性不受诚实但好奇的云服务提供商的影响，已经提出了许多支持细粒度数据访问控制的工作。然而，到目前为止，还没有一个方案能够同时支持细粒度的访问控制和时间敏感的数据发布。本文通过在CP-ABE（密文策略基于属性的加密）中嵌入定时释放加密，提出了一种时间和属性因素相结合的公共云存储时间敏感数据访问控制（TAFC）。在此基础上，我们进一步提出了一种针对时间敏感数据的访问策略设计方法。大量的安全性和性能分析表明，我们提出的方案是高效的，能够满足公共云中时间敏感数据存储的安全要求。

在这些场景中，访问权限的定时释放机制和细粒度的访问控制机制应该结合起来考虑。以企业数据公开为例：公司通常会为不同的目标用户准备一些重要的文件，这些用户可以在不同的时间点获得访问权限。例如，这家公司的未来计划可能包含一些商业秘密。因此，在早期，访问权限只能释放给CEO。然后一些相关部门的经理可以在以后的时间点获得访问权限，当他们负责计划的执行。最后，公司某些特定部门的其他员工可以访问这些数据来评估企业计划的完整性。在将时间敏感的数据上传到云端时，数据所有者希望不同的用户在不同的时间点后访问内容。对于外包的数据存储，CP-ABE可以描述不同的用户，并提供细粒度的访问控制。然而，据我们所知，这些方案不支持渐进访问权限释放。

# 【AC22】云访问控制中高效的基于属性的密文策略加密

摘要：将数据外包到一些云服务器可以实现云计算资源的大规模、灵活使用，并且通常由不同的组织和数据所有者持有。然而，由于在不受信任的云环境中托管敏感数据，并且这些数据的所有者在上传到云端后失去了对这些数据的控制，从而引发了各种安全问题。访问控制是第一道防线，它禁止未经授权访问存储的数据。此外，可以使用高级加密机制在不受信任的云上实施细粒度访问控制。有人提出了一些使用密文策略基于属性的加密（CP-ABE）来实现这种访问控制的方案，这些方案可以强制数据所有者的访问策略来实现这种加密访问控制，并解决其中的大多数问题。然而，由于托管云数据文件中所有者访问策略的加密强制频繁更改的复杂性，给数据所有者带来了计算和通信开销，因此一些挑战仍然悬而未决。这些挑战包括：1）制定动态决策以授予对云资源的访问权限；2）解决被视为性能杀手的吊销过程问题；3）构建一个抗共谋的系统。我们的工作目标是构建一个访问控制方案，该方案能够在云端提供敏感数据的安全存储和共享，并适用于资源有限的设备。

在这篇论文中，我们分析了现有的一些相关问题，并提出了一个扩展现有相关技术的方案来解决CP-ABE中固有的问题，而不会产生大量的计算开销。特别是，大多数现有的撤销技术需要为所有未撤销的用户重新颁发许多私钥，以及重新加密相关的密文。我们提出的方案提供了一种新的技术来执行动态改变合法用户的访问权限的解决方案。该方案通过更新访问策略和激活用户撤销属性来驱动访问权限。我们的技术将处理密集型任务分配给云服务器，而不会出现任何信息泄漏，从而降低资源有限的计算设备的计算成本。我们的理论分析和实验结果以及与现有相关系统的比较表明，与现有的相关系统相比，我们的方案是高效、安全和更实用的，特别是在策略更新和密文重加密方面。因此，我们提出的方案适用于需要一个实用的、安全的访问控制方案的物联网应用。

此外，为了实现安全的公共云存储，并尽量减少CP-ABE的局限性，CP-ABE主要支持将数据存储在仅由一个机构管理的私有云存储系统上，我们将所提出的访问控制方案扩展为一个具有多个权限的安全、关键的访问控制方案。该方案需要仔细设计，以实现细粒度的访问控制并支持外包数据的机密性。另外，由于在分布式环境下难以解决撤销问题，现有的多权限访问控制方案都没有很好地考虑撤销问题。因此，建立一个多权限的CP-ABE方案，同时解决策略属性和用户的变化问题，促使许多研究者开发出更合适的方案，但收效甚微。在本文中，我们利用现有的工作，提出了第二个CP-ABE方案，该方案克服了现有工作的大部分局限性，并允许在公共云存储系统上安全地存储数据，使用多个权限来管理一组联合属性。此外，该方案利用第一个提出的单权限访问控制方案中使用的两种技术来允许动态策略更新和使被撤销用户的密钥失效，从而有效地维护了撤销，从而消除了共谋攻击。在计算开销方面，该方案将昂贵的加密和解密操作外包给云服务器，以减轻数据所有者和数据用户的负担。我们的方案分析以及理论和实现结果表明，我们的方案具有可扩展性和高效性。

主要是关于撤销的算法。

# 【AC23】物联网动态访问控制框架（博士论文）

摘要：在不久的将来，物联网生态系统将使数十亿个智能物联网并交流有关自身及其物理环境的信息。在这些环境中，高密度的智能设备允许进行细粒度的数据采集，从而能够开发高级服务和新的应用程序，从可穿戴设备到空调到全自动汽车。然而，密集和普遍的数据收集、处理和传播可能会释放出有关个人的敏感信息，引发不小的安全和隐私问题。物联网安全和隐私的一个解决方案是使用访问控制和授权技术限制对敏感数据的访问。尽管标准访问控制模型的许多基本原则继续适用，但物联网环境的高度动态性、物联网设备的资源限制以及易受物理和虚拟攻击的脆弱性提出了独特的挑战，使得现有的访问控制方案不适合物联网。本研究针对物联网环境，提出一个整体的、动态的存取控制架构。该框架由三个部分组成：自动和上下文感知的策略规范方法、连续的策略执行机制和自适应策略调整技术。为了响应访问请求，自动策略规范组件动态生成访问控制规则，这些规则根据预定义的原始事实授予访问权限。原始事实描述了注册到系统中的物联网设备的属性以及这些设备可以交互的操作环境。持续策略强制机制在资源使用时不断监视操作上下文的符合性，并根据操作上下文和/或访问策略的更改重新评估正在进行的访问会话。自适应策略调整组件评估物联网设备的访问行为，根据设备行为模式调整访问控制策略，并向策略管理员建议策略调整以供最终批准。实验结果表明，该框架对物联网部署的动态安全性和隐私性要求具有更高的适应性，并在访问控制策略管理方面具有更好的灵活性。

在本论文中，我们指出传统的物联网存取控制机制的三大局限性：人工存取策略管理、不连续存取决策执行和静态存取权限指派。下面，我们将总结这些局限性及其各自的挑战：

手动访问策略管理：传统的访问控制系统和授权技术是针对封闭计算环境提出的，在这种环境中，系统的所有用户和资源都是预先知道的，并依赖于预配置的访问控制策略来满足在运行时不太可能更改的系统安全和隐私要求。然而，物联网设备之间的无限交互会导致资源管理员的安全和隐私需求频繁变化，从而导致底层访问控制策略的频繁变化。例如，预计物联网实体将随时自行决定加入和离开系统。在这种环境中，手动策略管理（如添加/删除访问规则、识别和解决访问控制策略中的冲突）成为一项复杂且容易出错的任务。实际上，系统管理员必须维护正确、一致和最新的访问控制策略，以跟上高度动态环境中安全和隐私要求的频繁变化。否则，配置不正确，冲突或过时的访问控制规则可能会将系统资源暴露给未经授权的访问。因此，需要实现访问策略生成过程的自动化，以克服传统策略管理技术的灵活性，消除访问控制策略中的错误和冲突，确保在高度动态的物联网环境中进行授权访问。

非连续访问决策实施：传统的访问控制模型是为了保护那些永久存储在静态或不经常变化的访问控制策略中的数据。通常，这些模型只在请求时间访问时执行访问决策，而不考虑资源使用时访问条件的更改。物联网技术的进步以及无处不在的连通性，催生了基于实时数据访问的新一代智能服务。无处不在的数据访问的普及和这些服务的加速采用给用户和数据隐私带来了重大挑战。因此，在上下文不断变化的高度动态环境中控制对这些服务的访问变得更具挑战性。物联网在我们日常生活中的广泛应用，如医疗保健和军事行动，需要持续和严格的访问控制，以防止未经授权和意外的访问。当上下文发生变化时，在做出访问决策时的延迟可能会导致造成伤害和损害的后果。因此，在高度动态的物联网环境中，不仅在请求时，而且在整个访问会话中，访问策略执行的连续性成为一个必要条件。

静态访问权限分配：通常，访问控制模型基于身份或角色等静态考虑因素分配访问权限。然而，这些模型通常会导致定义访问策略，这些策略分配的访问权限多于资源请求者所需的权限。为了缓解这一问题，研究者们致力于提高访问控制策略的表达能力，使策略管理员能够定义定制的访问控制策略，除了身份和角色外，还考虑了动态访问条件因素，如时间、位置、访问目的和用户之间的相互关系。访问控制文献将这些因素统称为访问上下文。然而，物联网的高度动态性使得人们很难（如果不是不可能的话）期望所有的访问上下文并为每个上下文分配适当的访问权限。物联网的这种独特特性需要一种自适应的权限分配技术，在运行时调整访问控制策略，以防止对过时访问控制策略的利用，减少用户滥用或滥用过度访问权限的机会。

介绍了物联网访问控制和其他的不同之处，需要迅速反应，适合动态环境，考虑上下文的访问控制等

# 【AC24】云访问控制中基于属性的密文策略加密（博士论文）

摘要：将数据外包到一些云服务器可以实现云计算资源的大规模、灵活使用，并且通常由不同的组织和数据所有者持有。然而，由于在不受信任的云环境中托管敏感数据，并且这些数据的所有者在上传到云端后失去了对这些数据的控制，从而引发了各种安全问题。访问控制是第一道防线，它禁止未经授权访问存储的数据。此外，可以使用高级加密机制在不受信任的云上实施细粒度访问控制。有人提出了一些使用密文策略基于属性的加密（CP-ABE）来实现这种访问控制的方案，这些方案可以强制数据所有者的访问策略来实现这种加密访问控制，并解决其中的大多数问题。然而，由于托管云数据文件中所有者访问策略的加密强制频繁更改的复杂性，给数据所有者带来了计算和通信开销，因此一些挑战仍然悬而未决。这些挑战包括：1）制定动态决策以授予对云资源的访问权限；2）解决被视为性能杀手的吊销过程问题；3）构建一个抗共谋的系统。我们的工作目标是构建一个访问控制方案，该方案能够在云端提供敏感数据的安全存储和共享，并适用于资源有限的设备。

在这篇论文中，我们分析了现有的一些相关问题，并提出了一个扩展现有相关技术的方案来解决CP-ABE中固有的问题，而不会产生大量的计算开销。特别是，大多数现有的撤销技术需要为所有未撤销的用户重新颁发许多私钥，以及重新加密相关的密文。我们提出的方案提供了一种新的技术来执行动态改变合法用户的访问权限的解决方案。该方案通过更新访问策略和激活用户撤销属性来驱动访问权限。我们的技术将处理密集型任务分配给云服务器，而不会出现任何信息泄漏，从而降低资源有限的计算设备的计算成本。我们的理论分析和实验结果以及与现有相关系统的比较表明，与现有的相关系统相比，我们的方案是高效、安全和更实用的，特别是在策略更新和密文重加密方面。因此，我们提出的方案适用于需要一个实用的、安全的访问控制方案的物联网应用。

跟上篇论文差不多

# 【AC25】EPDA：一种高效、保密的多接收者AMI网络数据采集与访问控制方案

摘要：高级计量基础设施（AMI）网络允许收集用户的细粒度功耗数据（PCD），以执行实时监控和能源管理。然而，PCD会泄露消费者活动的敏感信息。各种隐私保护的数据收集方案已经被提出用于AMI网络，以允许收集聚合的PCD来保护消费者的隐私。然而，这些方案大多是针对单接收者AMI网络而设计的，不能有效地用于多接收者AMI网络，在多接收者AMI网络中，多个实体应该能够访问不同用户集合的聚合PCD以用于合法用途。在本文中，我们提出了一个有效且隐私保护的多接收者AMI网络的数据收集和访问控制方案EPDA。我们开发了一种新的代理重加密方案，它允许在重加密之前进行数据聚合，并且可以根据需要在重新加密后对聚集的数据进行完全或部分访问。该方案可用于多接收者AMI网络的细粒度访问控制，其中每个接收者只能访问其预期的数据。EPDA在加密、聚合和解密中使用轻量级操作，从而降低计算和通信开销。我们的安全分析表明，EPDA是安全的，能够抵抗合谋攻击，隐藏用户的分配，这是公平的电力交易市场所需要的。实验结果表明，EPDA在提高AMI网络中每个实体的计算开销和较低的通信开销的同时，也提高了性能。

没啥用

# 【AC26】云存储中基于属性的授权搜索访问控制

摘要：在云存储中，基于属性的加密技术被广泛应用于实现数据机密性和细粒度访问控制。为了使用户能够识别大量数据集中的可访问数据，需要在密文中添加清晰的属性，这会导致属性隐私暴露。文中提出了一种基于密钥属性的安全访问策略（AKP-ABE），并将其扩展为一种基于加密属性的安全访问策略（eacp）。具体地说，通过将密钥委托技术集成到AKP-ABE中，EACAS使数据用户能够根据其访问策略定制搜索策略，并使用数据所有者授予的密钥生成相应的陷门来检索他们感兴趣的数据。此外，在数据加密和陷门生成中使用没有语义意义的虚拟属性，使云能够在不知道底层属性或外包数据的情况下对外包密文执行基于属性的搜索。数据拥有者可以对外包数据进行细粒度的访问控制，数据用户可以通过定制搜索策略，灵活地基于受保护属性搜索自己感兴趣的数据。最后，我们证明了EACAS在计算和存储开销方面比现有的解决方案更有效。

更安全的ABE算法

# 【AC27】云计算中移动多媒体数据的高效隐私保护访问控制

摘要：基于密文策略属性的加密（CP-ABE）由于允许加密者在加密消息之前定义访问策略的性质，被广泛采用作为云辅助移动多媒体数据共享系统设计的原语。然而，在以前的大多数工作中，与密文一起发送的访问策略仍然是明文形式，这会将用户的隐私暴露给任何可以获得密文的人，即使他没有被授权解密。此外，资源受限的移动设备无法执行CP-ABE导致的频繁的加密和解密任务。这些缺点可能会降低消费者通过移动设备共享多媒体数据的热情。文中提出了一种基于名字和属性保护的移动数据共享方案。属性值嵌入到chphertext中，访问策略中只显示属性名。加密分为在线和离线两个阶段。在离线阶段，数据所有者可以准备中间密文组件。一旦接收到特定访问策略和多媒体数据的加密要求，数据所有者可以在联机阶段快速形成最终的合法密文。通过使用解密外包技术，匹配测试和解密的大部分计算开销被卸载到云服务器上。安全性证明了PPCMM在标准模型下是自适应安全的。性能分析表明，PPCMM大大降低了在线加密和用户解密的计算成本。

一个新的CPABE算法，密文隐藏访问策略，解密外包，降低资源需求。

# 【AC28】物联网场景下基于隐私的区块链分布式密钥管理体系结构

摘要：物联网的快速发展和用户设备产生的有价值数据的爆炸式增长，导致了对访问控制的强烈需求，尤其是从组通信的角度进行的分层访问控制。然而，这种未来互联网的密钥管理策略大多基于可信的第三方，它需要密钥生成中心（KGC）或中央权威机构（CA）的完全信任。最近的研究表明，集中化的云中心不太可能为客户提供满意的服务，因为我们过于信任第三方；因此，这些中心不适用于面向用户隐私的场景。针对这些问题，本文提出了一种基于区块链的分布式密钥管理体系结构（BDKMA），采用雾计算来减少延迟，并在云中运行多个区块链以实现跨域访问。该方案利用区块链技术来满足分散性、细粒度可审计性、高可扩展性和可扩展性要求，以及物联网分层访问控制的隐私保护原则。设计了系统操作方法，引入了不同的授权分配方式和组访问模式，增强了系统的可扩展性。我们利用现有的各种模型对其性能进行了评估。仿真结果表明，多区块链结构大大提高了系统性能，并且随着网络规模的增大，系统的可扩展性也很好。此外，动态事务收集时间调整使性能和系统容量能够针对各种环境进行优化。

是个密钥管理系统

# 【AC29】基于区块链的访问控制安全云存储框架

摘要：现在越来越多的数据被外包给云服务。为了保证数据的安全性和隐私性，数据通常以密文的形式存储在云服务器上。当用户请求访问加密数据时，需要第三方分发的访问密钥。然而，如果第三方不诚实，系统的安全将受到威胁。针对这一问题，本文利用以太坊区块链技术，提出了一种具有访问控制的安全云存储框架。我们的新方案是以太坊区块链和基于密文策略的加密（CP-ABE）的结合。提出的云存储框架是分散的，即系统中没有可信的第三方。我们的计划有三个主要特点。首先，由于采用以太坊区块链技术，数据拥有者可以通过智能合约在区块链网络中存储数据的密文。其次，数据所有者可以为数据用户设置一个有效的访问周期，使得密文只能在有效访问期间被解密。最后，由于每个智能合约的创建和调用都可以存储在区块链中，从而实现了跟踪功能。安全性分析和实验表明，该方案是可行的。

本文将以太坊区块链技术引入到一种基于密文策略属性的加密算法中，并利用以太坊智能合约技术将公开的信息存储到区块链网络中，同时实现对数据访问行为的监督和跟踪。所有访问记录都记录在区块链网络中。在我们的框架中，使用区块链技术实现了访问控制的分散，没有任何可信的中心授权。

本文的主要贡献如下：

（1）提出了一种基于区块链的访问控制的安全云存储框架，该框架将以太坊区块链和基于密文策略的加密（CP-ABE）算法相结合，实现对云存储的细粒度访问控制。我们的方案不需要可信属性授权。关键信息通过以太坊智能合约技术存储在区块链网络中。因此，在我们的云存储框架中实现了去中心化。

（2） 当属性集被分配给数据用户时，数据所有者可以为数据用户追加一个有效的访问周期，并在以太坊区块链上存储信息的访问周期时间。只有当数据用户的有效访问时间和属性满足访问控制策略时，数据用户才能正确地执行数据解密算法。

（3） 在Ubuntu-linux系统环境下，智能合约被创建并部署在本地以太坊专用网络上。对相应的性能和成本进行了分析，实验证明了该方案的可行性。

文章内有过程图，需要data owner制定智能合约并上传，还要把合约地址等信息给云服务器，不适合DVCS，相当于每个文件都有一个智能合约，用户又要去向DATA OWNER申请，又要去云服务器拿智能合约地址，比较繁琐。

# 【AC30】云计算应用中基于时间和属性的双重访问控制和数据完整性验证方案

摘要：在大数据时代，基于云的工业应用可以为资源受限的智能设备提供可用、便捷的数据访问。基于属性的加密可用于确保数据安全，同时提供细粒度的数据访问。然而，现有的基于属性的加密方案很少考虑时间的访问控制和数据的完整性验证。针对以上两个问题，我们提出了一种基于时间和属性的云计算应用中的双访问控制和数据完整性验证方案（DCDV）。首先，在基于属性的加密技术中引入了层次时间树，利用分层身份加密技术为用户的属性密钥和密钥设置有效的访问时间段和指定的可解密时间段enc公司Rypted单独进行。只有当热属性满足保险丝要求时，才能执行解密操作数据所有者的访问策略和用户属性密钥的有效访问时间段完全覆盖了数据所有者设置的解密时间段。通过对数据进行时间和属性的双重控制，解决了私钥泄露导致的隐私数据泄露问题。其次，利用倒排索引和Merkle哈希树设计了数据验证树。数据用户无需解密即可验证云服务器返回的密文数据的完整性，解决了云服务器可能删除或修改数据的问题。最后，通过安全性证明和效率分析，证明了该方案的安全性和实用性。

不适合DVCS

# 【AC31】云计算访问控制模型与技术综述

摘要：访问控制是保护信息和系统资源的一项重要措施，以防止非法用户访问受保护对象，合法用户试图以超出其允许的方式访问对象。对从主体到对象的访问的限制由访问策略决定。随着云计算的快速发展，云安全问题日益成为人们普遍关注的问题，应当认真对待。本文以互联网的发展为主线，通过考察不同的网络环境和用户需求，对不同应用场景下，特别是云计算的访问控制模型和策略进行了研究。我们调查的重点是不同模型和技术之间的关系，以及应用场景以及每个模型的优缺点。云计算的访问控制将受到特别关注，这反映在访问控制模型和方法的总结中。我们还指出了访问控制的一些新问题，并指出了云计算未来的研究方向。

这个综述很概括，没啥用

# 【AC32】网络隐私保护的访问控制协议设计研究

摘要：为了为网络隐私提供更可靠的安全保障，研究了网络隐私保护的访问控制协议的设计。本文首先介绍了无线网络安全中存在的问题，指出了其中的关键技术，包括隐私保护、用户认证、信任管理、网络安全通信体系结构等。然后，简要分析了Priccess协议的组成、无线通信网络中的漫游认证方案和无线传感器网络的隐私数据保护方案。在此基础上，建立了无线通信网络中的漫游认证方案和无线传感器网络的数据隐私保护机制。最后，对Priccess协议的消息负载进行了评估，结果表明该协议对大多数用户接入设备都是有效的，可以为网络通信的隐私提供更有效的保护。

# 【AC33】基于关系的访问控制策略挖掘的贪婪进化算法

摘要：基于关系的访问控制（Relationship based access control，ReBAC）提供了高度的表达能力和灵活性，从而促进了安全性和信息共享。我们将ReBAC描述为基于属性的访问控制（ABAC）的面向对象扩展，其中关系通过引用其他对象的字段来表达，路径表达式用于跟踪对象之间的关系链。ReBAC策略挖掘算法可以部分自动化从现有访问控制策略和属性数据开发ReBAC策略，从而显著降低从传统访问控制系统迁移到ReBAC的成本。本文提出了两种从访问控制列表（acl）和以对象模型表示的属性数据中挖掘ReBAC策略的算法：启发式的贪婪算法和基于语法的进化算法。通过对四个样本策略和两个大型案例的评估，证明了算法的有效性。

# 【AC34\*】基于区块链的可审计访问控制系统定义方法

摘要：本文提出利用区块链技术来定义访问控制系统，以保证访问控制策略评估的可审核性。我们建议的关键思想是将基于属性的访问控制策略编成智能合约，并将其部署到区块链上，从而将策略评估过程转变为完全分布式的智能合约执行。不仅策略，而且其评估所需的属性都由区块链上部署的智能合约管理。可审计性来自区块链技术的不变性和透明性。本文不仅介绍了所提出的访问控制系统的一般性，而且还将其应用到需要保护的资源本身就是智能合约的创新参考场景中。为了证明我们方法的可行性，我们提出了一个参考实现，利用XACML策略和部署在以太坊区块链上的可靠书面智能合约。最后，通过一组实验结果对系统的性能进行了评估，并讨论了我们提出的方案的优缺点。

在这项工作中，我们提出了另一种解决方案，让资源所有者将访问控制功能外包出去。事实上，本文介绍了一个基于区块链技术的基于属性的访问控制系统的设计、实现和验证。拟议的系统遵循XACML标准（OASIS，2013）定义的参考架构，其创新之处在于，大多数架构组件都作为智能合约实现，在（基于智能合约的）区块链上部署、存储和执行。我们方法背后的关键思想是将访问控制策略编成可执行的智能合约，并通过区块链对其进行管理，从而获得分散的自我评估策略。

在本文中，我们深入分析了我们的提案在一个特定创新场景中的应用，即智能合约的准入监管。将要保护的资源（即智能合约）和保护资源的系统都部署在同一个区块链上，这将缓解在其他应用场景中采用我们的方案可能会出现的许多问题，如本文其余部分所述。在将访问控制过程外包给第三方方面，我们的方法提供了一些相关的优势。例如，资源所有者和发出访问请求的主体可以很容易地检测到不适当的授权或拒绝访问，这要归功于可公开审核的不当行为证据。实际上，第三方访问控制服务可以恶意地强制系统返回deny，从而禁止对某个主题的访问，尽管策略会授予它。即使在政策不满足的情况下，它也可以返回许可证，从而允许访问没有相应权利的主体。在前两种情况下，资源所有者和主题都无法在后验中检查访问决策过程结果的正确性，因为已经考虑的访问上下文细节可能不再可用。

这个好像很复杂，着重于访问控制这一点，将访问控制全部在区块链上实现，利用区块链来存储访问控制策略和管理属性，以及执行访问决策过程。没有过多的提加密和数据签名等。

所以这个文章实际上是将一般的访问控制转移到区块链上实现，满足了分布式和可审计性，并不是针对某一种系统定制的访问控制策略。我们需要将文件加密是因为实际可能需要public repository，这个是诚实且好奇的，所以需要保证保密性，我们不能说把DVCS和区块链加到一起，因为DVCS已经是可以直接使用的，所以加入DVCS的文件必须加密，而如何解密就是访问控制。这里使用ABE进行加密，甚至不需要区块链进行访问控制，自己就可以达到访问控制的目的。但是我们的方案其中密钥管理这一点，可能需要更多的设计。

# 【AC35】使用数据仓库和内存数据库在统一框架中管理基于属性的访问控制策略

摘要：在过去的几年中，各种类型的访问控制模型被提出，以满足组织日益增长的需求。其中，使用基于属性的访问控制（ABAC）规范和实施灵活的动态决策安全策略越来越受到人们的关注。但是，要将另一个模型中指定的现有安全策略迁移到ABAC中并不容易。此外，没有一种全面的方法可以指定、执行和管理ABAC策略以及组织中可能已经存在的其他策略作为统一的安全策略。在本文中，我们提供了一个独特而灵活的解决方案，通过在多维和多粒度的数据模型中存储和查询数据，实现了此类安全策略的并发规范和实施。具体来说，我们提出了一个统一的数据库模式，类似于传统的数据仓库设计，它可以表示不同类型的访问控制策略，并将相关策略存储为内存数据，从而显著减少访问请求评估的执行时间。我们还提出了一种通过元策略组合多个访问控制策略的新方法。为了便于管理，提出了一个管理模式，可以指定不同类型的管理策略。在大量数据集上进行的大量实验证明了该方法的可行性。

设计了一个放数据的系统，不适合DVCS

# 【AC36】大数据管理系统的访问控制技术：文献综述与未来趋势

摘要：数据安全和隐私问题因大数据的数量、种类和速度以及到目前为止缺乏参考数据模型和相关的数据操作语言而被放大。在本文中，我们重点讨论了数据安全的关键服务之一，即访问控制，通过强调与传统数据管理系统的区别，描述了任何一个大数据平台的访问控制解决方案都可以满足的一系列要求。然后，我们描述了目前的研究现状，并讨论了开放的研究问题。

# 【AC37】基于区块链的RFID系统中基于属性的访问控制模型

摘要：射频识别（RFID）系统的日益广泛采用，尤其是在医疗保健领域，这表明RFID对于医疗机构来说是一项积极的资产。RFID能够为人员和资源提供实时的可追溯性、标识、通信、温度和位置数据，从而为组织节省时间和成本。然而，RFID系统所面临的挑战是财务、技术、组织，尤其是隐私和安全。因此，最近的研究集中在基于属性的访问控制（ABAC）方案上。目前，ABAC大多基于集中式模型，在供应链等环境中，ABAC存在可伸缩性、同步性和各方之间信任等问题。在本文中，我们在RFID系统中实现了一个基于区块链的分散模型的ABAC模型。详细介绍了选择适当区块链的常用标准。我们的访问控制策略是通过分散应用程序（DApp）执行的，该应用程序通过智能合约与区块链连接。智能合约和区块链技术一方面解决了当前的集中式系统问题，同时也是灵活的基础设施，代表了ABAC模型中必不可少的信任和支持关系，以提供RFID系统的安全性。我们的系统是为供应链环境设计的，其使用案例适用于医疗保健系统，因此包含相关RFID标签的手术器械等资产只能访问特定区域。我们的系统部署在本地和Testnet环境中，以便进行深入的比较和确定技术可行性。

不太合适DVCS

# 【AC38】基于属性加密的云计算访问控制机制综述

摘要：总结了一堆算法，没啥用

# 【AC39】隐私意识分散访问控制系统

摘要：物联网安全和隐私已被证明是一个重大挑战。传统的访问控制协议由于其规模庞大、无处不在的连通性和分布式等特点，不适合于物联网。基于区块链的访问控制方法提供了分散的安全性，但它们涉及可扩展性问题、高交易费用、显著的延迟以及资源受限的物联网设备无法接受的计算开销。此外，区块链上发布的数据是公开的，这在许多情况下并不理想。在本文中，我们提出了一个新的基于纠结的分散访问控制系统，它允许用户对自己的资源进行访问。在我们提出的分布式访问控制模型中，策略和访问权限都发布在Tangle上，这样既保证了分布式可审计性，又防止用户欺诈性地拒绝授予的访问权限。本文的主要贡献是利用Masked Authenticated Messaging（MAM）数据通信协议来提供策略的隐私性。通过实现验证了所提出的工作，并用avisa工具进行了测试，该工具确认了入侵者存在时的安全性。

# 【AC40】基于区块链的电子病历访问控制研究

摘要：对于医疗行业来说，存在着医疗数据共享不畅、篡改、私密数据泄露等问题。针对这些问题，本文提出了一种基于角色访问控制模型的基于区块链的电子病历访问控制研究方案。首先，采用适当的访问控制策略，解决用户在访问过程中的医疗隐私信息泄露问题。然后，利用信息熵技术对医学数据进行量化，使医学数据得到有效、最大限度的利用。利用区块链的分布式总账特性及其固有的安全属性，可以消除数据孤岛，促进医疗系统之间的数据共享，防止访问记录被篡改，更好地支持医学研究和精准医疗。通过本研究，不仅可以在服务过程中实现用户的医疗隐私信息保护，而且患者可以自主管理自己的医疗数据，有利于医疗数据共享下的隐私保护。

# 【AC41】CSCAC:一种可信执行环境下的恒大小cpae访问控制方案

摘要：通用移动设备的普及使人们越来越担心它们的安全性。如何保护敏感数据是一个亟待解决的问题。基于属性的密文加密（cpae）是一种实用的数据加密方法，可以利用用户的属性对敏感数据进行加密。本文利用可信执行环境对属性生成的动态密钥进行管理，提出了一种固定大小的CPABE访问控制（CSCAC）模型。原始数据通过一个对称的存储密钥进行加密，然后在“与门”访问策略下对存储密钥进行加密。只有拥有一组满足访问策略的属性的用户才能恢复存储密钥。安全性分析表明，该访问控制方案的设计降低了单一权限情况下的负担和风险。

设计了一个ABE算法

# 【AC42】云计算大数据访问控制的高效可撤销CP-ABE

摘要：由于大数据量巨大，云是存储大数据的较好选择。由于云不可信，隐私和访问控制是一个很大的问题。基于密文策略属性的加密（CP-ABE）是一种很有前途的技术，可以在云中实现隐私和访问控制。然而，直接在云端大数据中应用CP-ABE方案是一项具有挑战性的任务。现有的带有撤销机制的CP-ABE算法效率低下。本文提出了一种有效的基于代理更新的云环境下大数据访问控制的可撤销CP-ABE（R-CP-ABE）方案，在撤销过程中，代理服务器代替数据所有者和数据用户分别执行密文和密钥更新。撤销期间的这种外包更新减少了数据所有者和数据用户的通信和计算开销。在安全性分析中，我们证明了我们的R-CP-ABE方案对选择明文攻击和用户合谋攻击是安全的。此外，我们还证明了我们的方案实现了前向和后向保密。性能分析表明，与现有方案相比，该方法是有效的。

# 【AC43】一种基于CP-ABE的支持属性变更的云存储系统访问控制方案

摘要：基于CP-ABE的访问控制方案能够更好地实现对云存储架构中共享的多对多密文的访问控制，但仍然面临着系统开销过大、策略属性撤销或恢复不灵活等问题。提出了一种基于CP-ABE的云存储系统中支持属性变更的访问控制方案。通过对策略属性集采用最小共享重加密密钥的重加密机制，实现细粒度的访问控制。然后通过为每个叶节点属性创建相应的虚拟属性来展开访问结构树。分析结果表明，该方案不仅提高了属性转换的效率和灵活性，而且降低了系统成本。

# 【AC44】RACC：一种高效可撤销的云存储细粒度访问控制模型

摘要：为了实现灵活、可扩展、可靠和细粒度的访问控制，云数据共享的需求变得越来越重要。目前，分布式访问控制模型广泛应用于云环境下的数据共享。现有的多权限分散数据共享模型在解密和属性撤销方面效率低下，不利于实际应用。现有的分散数据共享模型大多不支持属性撤销方法。本文提出了一种支持解密外包和属性撤销的数据共享模型。在我们提出的模型中，大部分解密的计算操作都被转移到用户先前执行的云服务器上。线性秘密共享方案的使用加强了访问控制策略。与通信开销、密钥更新、密文更新和解密开销相比，该模型的性能优于LWABE。我们的模型在加密过程中所花费的成本与LWABE几乎相同。

适合云服务器

# 【AC45】雾计算中一种外包计算的分布式访问控制

摘要：随着信息技术和物联网技术的飞速发展，数据安全和健康隐私受到越来越多的关注。为了存储、访问和共享电子健康记录，这些数据的存储被传输到第三方云服务器。存储在数据中心或云服务器上的电子健康记录的安全性和隐私性不受保证。在发送到数据中心或云服务器之前，应该对这些数据进行加密。为个人健康档案设计一个高效、安全的细粒度访问控制策略正面临着巨大的挑战。电子健康档案的安全性和隐私性是非常重要的，因为电子健康数据在医疗服务和治疗中起着重要的作用，直接关系到特定的病人。基于属性的加密（ABE）可以有效地实现细粒度的访问控制。然而，在ABE格式中，双线性对的计算需要大量的计算开销。为了降低计算开销，保证电子病历的机密性，本文提出了一种面向物联网的分布式细粒度访问控制方案。在我们提出的方案中，接收者和发送者几乎不需要进行计算。外包计算减轻了计算负担。安全性和性能分析表明，与以往方案相比，本文提出的方案是安全有效的。

一个分布式的外包计算ABE加解密的访问控制。外包的原因是要降低资源消耗，因为有移动设备资源受限，适合物联网。

# 【AC46】一种基于属性控制的公共云存储协同访问控制方案

摘要：在公共云存储服务中，数据被外包到数据所有者的可信域之外的半可信云服务器。为了防止不可信的服务提供商访问数据所有者的敏感数据，外包数据通常是加密的。在这种情况下，对这些数据进行访问控制成为一个具有挑战性的问题。基于属性的加密（ABE）已经被证明是一种强大的加密工具，可以对外包数据提供细粒度、灵活、安全的访问控制。然而，现有的基于ABE的访问控制方案不支持用户通过协作获得访问权限。本文探讨了一种特殊的基于属性的访问控制方案，在这种情况下，如果数据所有者允许他们在访问策略中进行协作，那么具有不同属性集的多个用户可以协作获得访问权限。同时，访问策略中未指定的协作应视为共谋，拒绝访问请求。通过在访问结构中指定翻译节点，提出了一种基于属性的受控协同访问控制方案。安全性分析表明，我们提出的方案可以保证数据的机密性，并具有许多其他关键的安全属性。大量的性能分析表明，我们提出的方案在存储和计算开销方面是有效的。

就相当于，有属性A和B才能解密密文，现在可以控制，让有A属性和有B属性的用户合作解密数据。比较新颖，因为普通的此类操作会被视为共谋。是个比较特殊的算法。（薛开平，TIFS）

# 【AC47】基于区块链的个人健康档案系统隐私保护访问控制模型

摘要：个人健康记录系统（PHR系统）存储个人的健康相关信息。PHR系统允许数据所有者管理并与选定的个人共享其数据。由于错误信息的不可逆后果，原始性或抗篡改特性对PHR系统至关重要。区块链技术以其不变性和不可逆性成为一种潜在的解决方案。不幸的是，存在一些技术障碍，如存储有限、隐私问题、同意不可撤销、效率低下和能耗。本文旨在解决这些区块链的缺陷，并提出一个基于区块链的PHR模型。所提出的模型是使用区块链技术来支持防篡改特性的。代理重加密和其他加密技术被用来保护隐私。该模型的特点包括细粒度和灵活的访问控制、同意的可撤销性、可审计性和抗篡改性。详细的安全性分析表明，该模型在保密性和抗篡改性方面是安全的。性能分析表明，与文献中现有的方法相比，该模型具有更好的整体性能。因此，该模型更适合PHR系统的应用。

# 【AC48】基于区块链的智能合约访问控制系统

摘要：研究表明，智能合约已经成为一项重要而有前途的技术。然而，由于缺乏成熟稳定的访问控制等安全机制，使得智能合约非常脆弱。为了解决这一问题，我们提出了一个基于区块链的基于属性的访问控制系统，通过建立合同管理员和合同所有者的分层管理机制来实现。在将区块链固有的同步功能与我们设计的系统级智能合约相结合后，所有的节点都可以轻松地及时获取访问控制规则。此外，我们对原有的智能合约有限状态机进行了修改，以防止通过系统契约对规则进行恶意修改。在我们的评估中，该系统只引入了2%-5%的额外成本，并保证了超级账本的安全性。

A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems

BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT

# 【区块链\*】基于区块链的分散存储系统中细粒度访问控制的数据共享框架

摘要：在传统的云存储系统中，基于属性的加密（ABE）被认为是解决数据隐私和细粒度访问控制问题的重要技术。然而，在所有的ABE方案中，私钥生成器（PKG）能够对云服务器中存储的所有数据进行解密，这可能会带来密钥滥用和隐私数据泄露等严重问题。同时，传统的云存储模式以集中存储的方式运行，单点故障可能导致系统崩溃。随着区块链技术的发展，分散存储模式已经进入大众视野。分散存储方法可以解决传统云存储系统中的单点故障问题，并且与集中式存储相比具有许多优势，例如价格低、吞吐量高。本文研究了分散存储系统的数据存储和共享方案，提出了一个将分散存储系统IPFS、以太坊区块链和基于属性的加密（ABE）技术相结合的框架。在该框架中，数据所有者能够为数据用户分配密钥，并通过指定访问策略对共享数据进行加密，从而实现对数据的细粒度访问控制。同时，基于以太坊区块链上的智能合约，实现了对分散存储系统密文的关键字搜索功能，解决了传统云存储系统中云服务器可能无法返回所有搜索结果或返回错误结果的问题。最后，在linux系统和以太坊官方测试网络Rinkeby上对该方案进行了仿真，实验结果表明该方案是可行的。

这类云存储系统已经非常成功，并得到越来越多的认可，但由于此类系统只依赖于存储能力较强的大公司来存储和传输数据，而大公司则被视为可信的第三方，因此不可避免地继承了依赖单点故障的缺点第三方服务。即使云存储系统是为了数据可用性而备份的，云存储服务提供商仍然可能会受到某些不可抗力因素（如政治审查）的影响，导致用户无法访问自己的数据。另外，随着存储技术的发展，存储设备的成本越来越小。集中式云存储服务的成本主要来自员工工资、法律成本和数据中心租金等，这些固定的成本不变或逐渐增加。集中式云存储服务的价格将更高。

从以上观点来看，未来需要一种去中心化的存储方式，为人们提供数据存储和共享服务。它不需要相信第三方会诚实地为我们传输和存储数据，也不需要担心数据无法访问。幸运的是，随着比特币的出现，其底层技术区块链可以为这种分散存储系统带来优雅的实现。区块链的出现使我们能够将P2P加密货币与存储空间、带宽、CPU功率等连接起来。想象一下，我们可以通过互联网免费租用额外的硬盘空间，并从加密货币中获得回报[1]。用户不必担心自己无法访问自己的数据，因为数据的可用性可以通过部署在区块链上的智能合约来保证，他们只需为自己存储的数据支付定期费用。

在传统的云存储系统中，如果用户想秘密共享存储在第三方云服务器上的数据，就需要一种技术来实现对只有特定用户才能访问和解密的数据的访问控制。在这种需求的驱动下，基于属性的加密机制[2]（ABE）被提出并迅速发展。通过这种机制，数据所有者可以根据用户的身份和属性指定数据访问策略，实现对数据的细粒度访问控制。几乎所有的ABE加密方案都需要一个可信私钥生成器（PKG）来建立系统并为用户分发相应的密钥[3]。这样的制度有很多问题。首先，在现实中很难找到一个值得信任的PKG。其次，这样的系统存在密钥滥用的问题，用户数据的所有权没有掌握在自己手中。PKG具有解密服务器中所有数据的能力，PKG可能会因为某些利益或政治审查等原因而泄露用户数据。一旦数据所有者丢失了自己的密钥，他甚至无法解密自己的数据，PKG仍然可以解密用户的数据。在实际应用中，我们需要数据拥有者能够控制自己的数据并为用户分配密钥。例如，一个医院的数据管理员应该能够为他的医生和相关人员分发密钥，以便他们能够根据他们的位置访问不同级别的数据。

为了更好地保护数据的隐私性和可用性，我们应该将数据的存储和共享从集中式的云存储系统转移到分散式的存储系统，这种存储系统的价格比传统的云存储要低，既有数据吞吐量大的优势，又不必担心单点故障。在现有的分散存储系统中，实现数据的加密和存储非常简单，但如何解决数据的秘密共享是一个亟待解决的问题。本文提出了一个能够实现对分散存储系统中数据的细粒度访问控制的框架，并基于感兴趣的关键字对数据进行搜索。

（1） 我们提出了一个将分散存储系统IPFS、以太坊区块链和基于属性的加密（ABE）技术相结合的框架，以实现对分散存储系统中数据的细粒度访问控制。数据拥有者是唯一控制自己数据的人，系统不需要可信PKG，并且数据拥有者能够为数据用户分发密钥，这比传统的ABE方案更灵活。同时，利用以太坊区块链对用户的密钥进行管理，解决了传统ABE方案中的密钥管理问题。当用户忘记了自己的密钥时，他只需要从以太坊区块链中存储相应的交易数据，并对其进行解密以获得自己的密钥信息。

（2） 通过对共享文件建立加密关键字索引，将加密后的关键字索引信息存储在以太坊区块链上，并在以太坊区块链上部署智能合约，实现分散存储系统中的关键字搜索。智能合约一经部署，就会按照智能合约的逻辑诚信运作，只有用户检索到正确的搜索结果，才会支付服务费。该方案解决了传统云存储环境下搜索服务提供商不能如实返回搜索结果的问题。

（3） 在Ubuntu-linux系统下，通过以太坊官方测试网络Rinkeby对系统方案进行了仿真，并对相应的性能和成本进行了分析。

DO为申请的用户产生解密密钥，通过区块链分发，区块链同时还有搜索密文的功能。所以是区块链分发密钥+ABE加密完成了分布式的访问控制。不适用于DVCS的点有：1）一个合作的project会有很多的DO，每个人想获取新文件都需要向DO申请key的话过于复杂，DO的操作量也很大 2）不能支持DVCS的写访问控制

# 【区块链】区块链物联网系统中的细粒度访问控制启用属性撤销

摘要：基于属性的加密（ABE）技术在区块链中的细粒度访问控制中引起了广泛的关注，特别是在支持区块链的防篡改物联网（IoT）系统中。然而，由于典型区块链的巨大可变性和ABE的属性更新/撤销之间的不兼容性，它的采用受到了严重阻碍。在本文中，我们提出了一个新的基于区块链的物联网系统，该系统与该技术兼容，并通过将变色龙哈希算法集成到区块链中来实现细粒度的访问控制。我们设计并实现了一种新的基于多层区块链结构的验证方案，以保证对恶意攻击的抗篡改性和业务采样。系统可以提供更新-面向访问控制，其中HistoricalOn ChainDataCanOnly对新成员是可访问的，而被吊销的成员则无法访问。这是区别不同的现有解决方案，它是由向被吊销成员的数据泄漏造成的。我们还提供了分析和仿真，表明我们的系统在开销、搜索复杂性、安全性和兼容性方面优于其他解决方案。

在本文中，我们提出了一个新的多层区块链物联网数据服务系统，该系统能够在基于ABE的细粒度区块链访问控制机制中实现安全属性更新。我们开发了一个可编辑的密钥链和一个标准的数据链，以保护和控制对数据链的访问。通过可重定义哈希函数的授权，可重定密钥链允许密钥链更新ABE的访问策略矿工们数据链可以是具有任何可扩展结构的任何现有区块链，并保持物联网数据的不变性。总的来说，这些结晶原语解决了区块链的不变性与更新属性以管理区块链访问的必要性之间固有的不相容性。据我们所知，拟议中的区块链物联网数据服务系统是第一个实现属性更新并在更新时提供有效访问控制的同类系统。该系统兼容区块链中主要类型的密码原语和共识算法。

# 【区块链】BaDS:IoT中与ABS和CP-ABE共享数据的基于区块链的架构

摘要：物联网（IoT）和云计算日益融合，从物联网设备（通常计算和存储资源有限）收集的数据被发送到云端进行处理等，以便为决策提供信息，并促进其他运营和业务活动。然而，云可能不是一个完全可信的实体，比如泄露用户数据或损害用户隐私。因此，我们提出了一种基于区块链模型和基于属性的密码体制的隐私保护和用户控制的数据共享体系结构。另外，我们系统中的一致性算法是拜占庭式的容错机制，而不是工作证明。

1. 物联网数据首先被加密（例如AES）。然后，我们将智能合约技术与属性加密方案[19]相结合，实现智能合约的细粒度共享。在加密密钥上设置访问策略（加密密钥由属性加密，ABE）决定谁可以获得这个加密密钥来解密密文。
2. 在我们的架构中使用的智能契约是为了保证访问控制表的可伸缩性。系统中的所有数据共享（或访问）请求通过事务（如第3.5节中的智能合约）与智能合约交互。

主要是针对物联网的系统，没有数据修改等需求。不是针对DVCS的，有设备请求时，云服务器连接区块链判断是否有权限，有权限就给数据。

# 【AC50】公共区块链中的分散访问控制加密

摘要：公共区块链自诞生以来，由于其完全分散和持续性的特点，引起了学术界和业界的广泛关注。然而，公共区块链中的隐私问题仍然具有挑战性。虽然公共区块链中存在隐私保护机制，但几乎所有这些机制都只能解决部分隐私问题，无论是用户隐私还是数据隐私。在这项工作中，我们提出了一个分散的存取控制加密方案，在公共区块链中同时保证使用者和资料的私密性。使用我们的加密解决方案，一个特定事务的有效性可以公开验证，而其内容只能由其预期的接收者检索。此外，除了网络中的接收者外，任何参与者都无法识别出交易的来源。我们的分析表明，我们的解决方案确实适合部署在公共区块链中，并且在数学假设下被证明是安全的。

# 【AC51】基于元数据和智能合约的智能建筑分散访问控制

摘要：管理大型商业建筑的居住者和访客进入不同建筑区域、控制系统和设备的特权是一项具有挑战性的任务。目前的最佳实践包括给予长期居住在大楼内的员工（例如在大楼工作的员工）进入其组织区域的特权，并要求访客由他们陪同。这种做法既保守又不灵活。理想情况下，需要一个自动化的解决方案来管理访问授权；然而，传统的基于角色的访问控制模型很难实现，因为它们需要对所有角色及其相对权限进行规范，这对于拥有多个组织和大量访问者的大型建筑来说是一个挑战。在本文中，我们提出了一种基于区块链智能合约的方法来描述、授予和撤销以分散方式构建用户的细粒度权限。使用RDF的两个应用程序接口（API）实现了对资源的访问控制。利用真实建筑的元数据，我们将所提出的方法应用于一些实际用例中的权限管理，结果表明，该方法在提供细粒度访问控制的同时，可以大大降低管理开销。

# 【AC52】基于区块链的大数据去中心化访问控制基础设施

摘要：大数据技术已经在多个领域证明了它的有效性，几个项目证实了创新机会的存在。然而，在这些环境中，安全和隐私问题逐渐被放大。传统的访问控制机制不能保证用户的匿名性和隐私性。本文提出了一种新的基于区块链技术的大数据访问控制基础设施，发布策略，部署在智能合约中，表达对资源的访问权，并提供识别和认证过程。在我们的基础设施中，策略对公众可见，任何用户都可以知道与资源配对的策略以及谁有权访问，这会损害隐私。为了解决这个问题，我们对智能合约表示的访问策略中的属性进行加密。我们还对访问请求程序中的属性进行加密，验证仅在比较加密属性的基础上进行，无论它们是否相同。如果是，则生成授权令牌以允许访问。

不牵扯数据的加密存储

# 【AC53】基于区块链的分布式访问控制

摘要：在单个管理域中规范和实施网络范围的策略在当今的网络中很常见，并且被认为已经解决了。但是，对于多管理域，例如在不同企业之间，情况并非如此。在这种情况下，出现了新的问题，对pki等经典解决方案提出了挑战，这些解决方案受到可伸缩性和粒度问题的困扰。在本文中，我们对基于组的策略（一种广泛使用的网络策略语言）进行了扩展。为此，我们利用授权区块链实现（Hyperledger Fabric）以安全和可审核的方式分发访问控制策略，同时保持每个组织的独立性。网络管理员指定呈现到区块链交易中的策略。LISP控制平面（RFC 6830）允许执行访问控制的路由器查询区块链的授权。我们实现了一个端到端的实验原型，并从可扩展性和网络延迟方面对其进行了评估。

# 【AC54】不相关

# 【AC56】一种新的可验证外包密文-策略属性加密，用于云计算中的大数据隐私和访问控制

摘要：云中大数据最重要的安全问题是隐私和访问控制。基于密文策略属性的加密（CP-ABE）是解决上述问题的一种有效的密码方案，但现有的CP-ABE方案由于加密和解密过程需要大量的计算时间而不适合云中的大数据。在本文中，我们提出了一种新的可验证的外包CP-ABE，用于云中的大数据隐私和访问控制。我们的方案通过将繁重的计算外包给代理服务器来降低加密和解密的计算开销。我们的方案也验证了数据的正确性以及外包计算。此外，我们的方案限制了一组用户的数据访问，而不是提供无限次的数据访问，这是商业应用所必需的。在安全性分析中，我们证明了我们的方案对于选择明文攻击、共谋攻击和代理攻击是安全的。性能分析证明了该方案的有效性。

目前也有针对云存储提出的基于区块链的分布式访问控制方案，虽然能够防止访问控制的单点失效问题，但都不适用于支持多人共同协作的DVCS。

【4、7】提出了基于区块链的访问控制方案，访问控制过程放在区块链上运行。【4】将区块链、智能合约和代币结合起来，设计了基于令牌的访问控制方案，在区块链中存储含有访问策略的令牌，用户搜索令牌来来获取权限。【7】的访问控制是用户向云请求资源，云根据区块链中存储的权限决定用户是否可以访问资源。这两种访问控制方案都能提供数据存储的保密性，但对于需要多人协作的DVCS，方案无法提供写权限控制。

【1】为云存储提供了基于区块链的分布式访问控制，其中云上的数据由ABE加密，密钥的分发由区块链完成。DO为发出请求的用户产生解密密钥，通过在区块链中进行交易分发密钥。这是比较安全的针对云存储的分布式访问控制方案，但其不支持写访问控制，并且在DVCS中一个合作的project中会有多个文件和多个DO，频繁的进行密钥申请和生成也会有很多开销。

摘要：