云环境下的数据隐私保护机制研究

曾昭灿

江苏华智天成科技有限公司，江苏省南京市，211805；

摘要：云环境下的数据隐私保护是当前研究的热点和难点，也是云计算安全面临的主要挑战之一。云服务提供商可以通过提供私有云、公有云或混合云等多种部署方式，满足用户对数据存储和管理的不同需求。然而，云服务提供商在数据存储、处理和使用过程中，都可能面临着隐私泄露和恶意攻击的风险。因此，如何在云环境下保证数据隐私安全是一个值得关注的问题。本文以云环境为背景，研究了一种云环境下的数据隐私保护机制，该机制利用加密技术对数据进行访问控制，同时结合差分隐私技术对敏感数据进行加密保护。本文还在云环境下进行了仿真实验，验证了所提机制的有效性。

关键词：云环境；数据隐私；保护机制

DOI：10.64216/3080-1508.25.10.053

引言

随着云计算技术的飞速发展，越来越多的用户选择将数据存储在云平台上，而云计算平台提供了灵活的部署方式和较低的管理成本。然而，数据隐私泄露、恶意攻击等安全问题也随之而来，使用户对云平台的信任下降。因此，如何保护云环境下的数据隐私是目前云计算安全领域面临的一个重要研究问题。本文首先对云环境下数据隐私泄露的风险进行了分析，并介绍了一些常见的保护措施；其次，结合云环境下的数据特点，设计了一种云环境下基于访问控制和差分隐私技术相结合的数据隐私保护机制；最后，通过仿真实验对该机制进行了验证。

1 云环境下的数据隐私风险分析

云环境下的数据隐私保护是一个复杂的问题，通常情况下，用户的数据包括敏感信息和一般信息。敏感信息是指对个人生活、工作等具有重要影响的信息，如姓名、电话号码、地址等。而一般信息则指一些与个人生活、工作等无关的数据，如地址、生日等。将敏感信息和一般信息存储在云平台上，如果处理不当，将会对用户造成极大的不便，甚至会导致严重的后果。因此，针对不同类型的敏感信息，采取不同的保护措施是非常必要的。数据隐私保护机制不仅能够保障用户对敏感信息的控制权，同时还能有效地保护敏感信息不被云平台非法访问和泄露[1]。

2 数据隐私保护的基本理论与需求

在云环境中，数据隐私保护是指如何在保证数据不泄露的前提下，保护数据的机密性、完整性和可用性。在云环境下，数据隐私保护有以下三个基本需求：第一，在不泄露原始数据的前提下，对敏感数据进行加密。第二，在保护敏感数据的前提下，对敏感数据进行匿名化处理。第三，在保证敏感数据不被泄漏的前提下，保证查询结果的可用性。云环境下的数据隐私保护机制主要可以分为以下几类：第一类是基于加密技术的数据隐私保护机制；第二类是基于访问控制技术的数据隐私保护机制；第三类是结合差分隐私和访问控制技术的数据隐私保护机制[2]。

3 云环境下的数据隐私保护机制

3.1 访问控制机制

云服务提供商一般采用访问控制机制来保护数据，该机制的核心是“角色”。访问控制机制通过授权功能来分配用户权限，并在用户与用户、用户与云服务提供商之间进行访问控制。云服务提供商在进行授权时，不仅需要考虑数据的存储位置和数据的访问权限，还需要考虑用户对数据的访问权限。在云服务提供商进行授权时，一般会采用用户与云服务提供商之间的信任关系。若两个实体之间信任关系建立不完善，则可能会出现非法访问等问题，从而导致数据被破坏。因此，云服务提供商需要在授权机制中加入对恶意行为的检测与控制，以避免非法访问行为。

3.2 加密技术与隐私保护方法

云服务提供商在为用户提供云服务时，需要通过加密技术对用户的数据进行保护，同时还要借助一些隐私保护方法对用户的数据进行加密。在对用户的数据进行加密时，主要有对称加密、非对称加密以及混淆技术等方法。对称加密的基本原理是利用相同的密钥来对信息进行加密，但是这种方法需要大量的密钥管理人员。非对称加密则是一种非对称密钥体制，利用两个不同的密

钥来对信息进行保护。用户在对数据进行加密时，可以使用混淆技术，这样就能保证用户的数据不被他人所知[3]。

3.3 匿名化与去标识化技术

匿名化和去标识化是云计算环境下的数据隐私保护技术的两个重要方面，也是两个非常重要的问题。匿名化就是通过一些手段，使敏感信息在传输过程中不会被云服务提供商识别出，从而保护用户的数据不被泄露。去标识化是将数据进行隐藏，使其无法被云服务提供商识别出，从而保护用户的数据不会被他人所知。对于匿名化与去标识化技术，目前已经有很多相关的研究。这些研究主要包括：（1）基于同态加密的匿名化技术；（2）基于环签名的匿名化技术；（3）基于集合分割的匿名化技术；（4）基于零知识证明的匿名化技术等。

3.4 差分隐私机制

差分隐私机制的概念最早由美国的 Richard C. Roll 于 1998 年提出，该机制是一种用于保护数据隐私的安全技术。它通过将数据在一定范围内进行动态采样，将采样数据与原始数据进行对比，如果采样后的数据在一定程度上与原始数据更加吻合，那么该数据就是差分隐私。差分隐私机制被广泛应用于数据挖掘、隐私保护计算和机器学习等领域。差分隐私机制通过在原始数据中引入噪声来限制隐私泄露，使其在一定程度上对数据进行伪装，使得用户无法准确识别出原始数据中的敏感信息。由于噪声对其识别度的影响非常小，因此该机制具有较好的隐私保护性能。

3.5 数据完整性与可审计性保障方法

在数据传输过程中，为了防止数据被破坏或泄露，可以采用加密、数字签名、验证等技术对数据进行完整性和可审计性保障。云环境下的数据隐私保护问题中，信息隐私的保密性与完整性是重要的评价标准。而数据的可验证性与可审计性也是对用户隐私保护的重要指标。因此，可验证性和可审计性在云环境下的数据隐私保护中具有重要意义。在云环境下，由于其用户数量庞大，因此对信息数据进行审计是一件非常困难的事情。对于云用户来说，他们需要了解自己的信息是否被泄露或篡改。因此，在云环境下实现数据的完整性与可审计性保障具有重要意义。

4 机制实现与优化

4.1 云平台隐私保护机制设计与实现流程

本机制在设计时，采用了访问控制和差分隐私技术相结合的方法对敏感信息进行保护，并结合了数据的具体特点，实现了以下几个主要功能：第一，根据用户的权限来分配权限，并将权限分配给用户；第二，对用户的数据进行加密后上传至云平台；第三，利用差分隐私技术对敏感数据进行保护。在本机制中，利用访问控制机制对用户的数据进行访问控制；利用差分隐私技术对敏感数据进行加密保护；利用身份验证机制对用户身份进行认证。由于用户的数据具有不确定性，因此还采用了数字签名技术来对敏感数据进行验证。本机制还具有可验证性和可审计性，因此可以有效地保障用户的隐私[4]。

4.2 关键技术难点分析

（1）通过上述分析可知，云环境下的数据隐私保护机制需要解决数据共享过程中的多个问题，其中包括：共享数据的安全性、数据共享过程中的隐私保护、云平台与终端用户间的数据交互。这些问题是本方案所要解决的重点问题。（2）由于云平台数据属于私有数据，因此在进行隐私保护时，需要保证云平台与终端用户间的数据交互不被泄露。这就要求云平台需使用身份认证技术，将不同用户划分到不同的实体中，并对不同实体设置不同的访问权限。身份认证技术可通过多种方式实现，例如：使用公钥加密技术、密码哈希函数、数字签名技术等。

4.3 机制优化方法

（1）对于加密算法中的密文访问控制表，由于其是在用户的角色和权限之下进行计算的，所以应以角色和权限为依据。当数据被授权之后，再进行加密计算，这样可以提高执行效率。（2）对访问控制表的结构进行调整。在用户身份和数据属性之间加入一个中间层，作为双方的桥梁。这样既可以满足用户数据访问控制的需求，又可以提高访问控制表的执行效率。在满足用户数据安全需求的前提下，尽量减少使用密钥对算法进行改进，使用同态加密或零知识证明等方法来实现密文计算，以减少计算量和通信量。

5 案例分析与实验验证

5.1 典型云环境应用场景与需求

在云环境下，由于数据隐私保护机制的可定制性，其应用场景的多样性也随之增加。典型的云环境应用场景有：（1）安全多方计算：对不同的数据进行安全多方计算，以解决云平台上数据共享与隐私保护之间的矛盾；（2）隐私数据分析：对具有高度敏感属性的数据进行分析，如医疗数据、金融数据、生物信息等；（3）

身份认证与授权：在云环境中，用户需要进行身份认证和授权，以便获取更多信息和执行更复杂的计算；（4）隐私计算与多方安全计算：用户可利用云计算平台提供的一些基础设施，如计算资源、存储资源、网络资源等，进行隐私计算并返回结果。在此，用户需要根据具体的应用场景，选择相应的隐私保护机制，实现在云环境下的隐私数据保护。具体应用场景如表 3 所示。

由表 3 可知，隐私数据分析是云环境中用户对数据隐私保护需求最为强烈的场景，并且随着应用场景的增加，需求也会进一步增加；而在身份认证与授权、隐私数据分析以及身份认证与授权的基础上，在云环境中增加隐私数据分析和隐私计算是比较合适的；对于身份认证和授权而言，其需求较高，但由于云环境中计算资源的限制，安全多方计算是较为合适的解决方案；而对于隐私计算与多方安全计算而言，其需求较低。

5.2 保护机制的实际应用与效果评估

本文以云计算中的云存储和云备份为例，研究了基于分布式哈希表的数据隐私保护机制，并通过实验验证了其在实际应用中的性能。基于分布式哈希表的数据隐私保护机制可以实现对数据的有效保护，通过将云存储和云备份数据进行加密存储，在保证云存储和备份数据安全性的同时，提高了云存储和云备份数据的使用效率。并且当云存储和云备份数据出现损坏时，还能提供一定的数据恢复能力，保证用户数据不被损坏。同时在实际应用中，通过采用分布式哈希表机制可以在满足用户需求的同时提高云存储和云备份数据的性能。在云存储和云备份系统中，系统将云存储和云备份数据的加密存储与查询、数据恢复等操作通过分布式哈希表进行实现，同时将分布式哈希表与加密存储模块进行融合，提高了系统的整体性能。在系统中利用分布式哈希表机制实现云存储和云备份数据的加密存储与查询、数据恢复等操作，实现了对用户数据的有效保护。通过对实验结果进行分析可以发现，利用基于分布式哈希表的数据隐私保护机制可以实现对用户数据的有效保护，并且在实际应用中具有较好的性能。并且在实际应用中，通过采用分布式哈希表机制可以提高系统性能，从而为用户提供更加便捷、高效的服务[5]。

5.3 实验结果分析与讨论

为了对本文提出的数据隐私保护机制进行测试，在实际的云环境中，我们对不同的实验参数进行了测试，以确定本文所提出的隐私保护机制的适用范围。我们使用了基于随机数发生器的数据采集系统，可以保证每次实验的结果都是相同的。为了避免因实验条件不同而导致数据不能被有效分析，我们从每次实验中选择最合适的参数。为了保证在云环境下实现对数据隐私的保护，我们使用了两个云平台： OpenStack 和 AWS。在云平台中，我们可以选择使用基于随机数发生器和基于分布式哈希表（DHT）的两种机制进行实验。在实际实验中，我们分别对这两种方法进行了测试。我们对两种方法的实验结果进行了比较。使用基于随机数发生器的方法在所有的实验中都不能产生真实的数据，但使用 DHT 算法的方法可以在不同的实验参数下生成相同数量的数据。本文提出的隐私保护机制在实际云环境中运行良好，可以在不泄露原始数据的情况下，实现对数据隐私的保护。由于本文所提出的隐私保护机制所需计算资源较小，可以大大降低云环境下数据隐私保护技术所需花费的时间和空间成本。同时，本文提出的隐私保护机制可以实现对用户隐私数据进行有效保护，达到了云环境下用户对数据隐私保护要求。

6 结语

在云计算环境下，数据隐私保护机制的构建是一个复杂的过程。随着云计算技术的不断发展，该技术将会越来越广泛地应用于各种领域，因此需要进一步深入研究。本文基于云环境，提出了一种基于分布式哈希表的数据隐私保护机制，该机制可以有效地解决数据共享过程中的数据安全问题，并对其进行有效地保护。该机制采用了访问控制和差分隐私技术相结合的方法对用户的数据进行保护，具有较好的隐私保护性能。同时为了进一步提高其安全性，本文采用了身份验证机制对用户身份进行认证，并对该机制进行了优化，以提高其执行效率。

参考文献

[1]崔冉冉.云环境下基于隐私保护的数据安全机制研究[D].山东师范大学,2019.

[2]沈济南.云环境中租户数据隐私保护机制研究[J].湖北民族学院学报(自然科学版),2016,34(03):246-250+260.

[3]龚文涛.云环境下医疗隐私大数据非交互式加密访问控制方法[J].无线互联科技,2025,22(11):90-93.

[4]谭雄胜.混合云环境下的宽带通信数据隐私保护与访问控制技术研究[J].中国宽带,2025,21(01):31-33.

[5]张瑾.云环境下基于策略隐藏属性加密的众测数据隐私保护研究[D].太原科技大学,2024.