云计算环境下物联网数据的加密存储算法设计

黎结华

中科智城（广州）信息科技有限公司　广东广州　510000

摘　要：物联网（IoT）技术数据的特点集中表现在量庞大、多样化且敏感性较高，基于这个特点，物联网数据的加密存储相对会更加重要。物联网设备产生的数据通常有个人身份信息、位置信息、健康数据等敏感信息，这些数据在存储过程中需要更充分的保护，防止未经授权的访问和恶意的攻击。在物联网环境中，采用加密存储还能有效的防止数据被篡改或损坏，保持数据的一致性。其次，物联网数据会存储在云计算环境中，这就涉及多个云服务提供商，在这样的多云环境下，数据在存储和传输过程中应得到必要的保护，防范云服务提供商间的攻击和数据的泄露。由此可见，云计算环境下物联网数据的加密存储算法的相关研究是确保物联网系统安全性的关键一环，它能提供全面的数据保护方案。

关键词：云计算；物联网数据；加密存储算法

引言

本文将研究云计算环境下物联网数据的加密存储算法的设计，物联网大量的实时和敏感数据在云计算环境中，数据隐私和安全问题便产生了。物联网数据的加密存储算法是确保数据完整性和机密性不可或缺的一环。如何设计有效、高效的加密存储算法，成为当下关注的热点问题，基于这样的背景，本文将关注云计算环境下物联网数据的加密存储算法的设计与实现。通过研究为云计算环境中不断增长的物联网数据提供创新的、全面的加密存储解决方案，将推动物联网技术在更加广泛的领域中持续发展。

1 云计算环境下物联网数据的加密存储算法定义与要求

1.1 加密存储算法的定义

云计算环境下物联网数据的加密存储算法定义涵盖几个重要的方面，如常见的对称加密算法 AES（高级加密标准）对称加密算法，是使用相同的密钥进行加密和解密，通常它们的性能较为高效。RSA 是另一种常见的非对称加密算法，主要用于数据的加密和数字的签名，涉及一对密钥，其中公钥用于加密，私钥用于解密。SHA-256 即哈希函数，产生固定长度的散列值，常用在校验数据的完整性方面。混合加密是结合对称和非对称加密的优势，提高了数据传输和存储的安全性。

1.2 加密存储算法的要求

加密存储算法首先要确保数据在存储过程中是加密的，即使是云服务提供商或攻击者能够访问存储的物理介质，也无法直接获取明文数据。还要使用哈希函数或其他完整性验证手段，使之数据在存储和传输中没有被篡改。密钥管理方面，应确保密钥不会被泄露，同时还能够定期更新密钥以提高安全性。确保只有经过授权的用户或设备能够解密和访问存储的数据，实施细粒度的访问控制。还要在选择算法时考虑其在云计算环境中的性能，以确保数据加解密不会影响系统的整体性能。关于系统的可扩展性，应能够适应不断增长的物联网设备和数据量。确保选择的加密算法和实现在不同的云服务提供商之间兼容，以便在需要时进行云平台迁移。最重要的是符合相关法规和标准，例如 GDPR（欧洲通用数据保护条例）等，以确保数据隐私和安全得到法律保护。

2 物联网数据的加密存储引发的问题

2.1 系统和数据库整体性能下降

物联网数据的加密存储引发系统和数据库的整体性能下降，数据加密和解密需额外的计算资源，对于大规模的物联网数据，加密和解密操作会占用大量的 CPU 资源，使系统在处理其他任务时性能下降。加密后的数据会占用更多的存储空间，一些加密算法引入了额外的元数据或填充，使存储的数据量增加，导致存储成本的上升，并影响数据库的性能。在数据传输过程中，加密和解密操作导致数据包的大小增加，从而增加了网络传输的带宽需求，对实时性要求高的物联网应用产生负面影响。加密和解密过程会引入额外的处理时间，导致数据访问和查询的延迟，对于需快速响应的物联网应用，延迟的增加导致性能下降，影响用户体验。安全的加密存储涉及密钥的生成、存储、更新和分发，密钥管理的复杂性引入额外的系统开销，同时也需要考虑密钥的安全性，对整体性能产生负面影响。一些加密算法在大规模部署时面临可扩展性问题，尤其是在物联网环境中，设备数量和数据规模会快速增长，一些加密算法难以适应这种规模的增长，导致系统性能下降。

2.2 模糊匹配问题频发

物联网数据的加密存储导致算法存在模糊匹配问题，加密数据的存储会使对数据进行搜索和查询变得更为复杂，传统的模糊搜索难以在加密数据中实现，因为在加密状态下，相似性的度量和比较变得困难，导致模糊匹配的性能下降。加密数据通常需在解密之后才能进行有效的索引操作，这导致在加密数据上执行模糊匹配时，无法直接使用传统的索引技术，而需要在解密后才能进行模糊搜索，增加了系统开销。一些加密模式导致相同的明文在加密后产生不同的密文，这使得模糊匹配更加复杂，例如使用块加密模式时，即使输入数据只有微小的变化，导致整个密文的变化。模糊匹配算法依赖于特定的数据结构，而这些数据结构在加密状态下变得难以处理，例如一些树状结构或哈希表需要在明文状态下构建，但在加密状态下无法直接应用。加密过程导致数据失去原有的特征，使得一些模糊匹配算法难以从密文中提取有用的信息来进行模糊搜索。

2.3 存储空间需求增大

使用算法加密后导致存储空间需求增大，加密算法在对数据进行加密时引入了填充（padding）或扩展的操作，以满足块加密的要求，这导致加密后的数据比原始数据更大，从而增加了存储空间的需求。许多加密算法采用块加密模式，将数据划分为固定大小的块进行加密，如果原始数据的大小不是块大小的整数倍，需要对最后一个块进行填充，导致加密后的数据增大。一些加密算法具有“密

文扩散”的特性，即明文中的微小改变会导致密文中的广泛变化，这导致了加密后的数据在存储时比原始数据更大，因为小的变化传播到整个数据块。使用加密算法时，通常需要存储初始向量（IV）以确保加密的唯一性，增加了每个加密块的元数据，导致整体存储空间的需求增加。不同的加密算法具有不同的性能和空间开销，某些高级的加密算法，尤其是对安全性要求更高的算法，会导致较大的密文，增加存储需求。数据库索引通常依赖于数据的大小和结构，而加密后的数据不再适用于原有的索引结构，导致需要重新设计或采用更大的存储空间来存储索引。

3 云计算环境下物联网数据的加密存储算法的运行原理

在云计算环境下，物联网数据的加密存储算法通常会涉及对数据进行加密和解密的过程，以保护数据的机密性。首先，选择适当的加密算法，可以是对称加密算法（如 AES）或非对称加密算法（如 RSA）等。对称加密算法需要使用相同的密钥进行加密和解密，而非对称加密算法使用一对公钥和私钥，生成并确保密钥的安全性是关键的一步。将要存储的物联网数据使用选择的加密算法和密钥进行加密，这可以是整个数据块或数据的特定部分，取决于设计选择。将加密后的数据（密文）存储在云存储系统中。此过程确保在云端存储的数据是经过加密的，即使存储介质被未经授权的用户或攻击者访问也难以理解。在需要访问数据时，合法用户需要获得相应的解密密钥，这涉及到密钥的管理系统，确保只有授权用户能够获得解密密钥，使用获得的密钥对存储的密文进行解密，这还原了原始的明文数据，以便用户能够正确理解和使用数据。在获得解密密钥之前，通常需要进行身份验证，确保只有授权的用户或设备能够获取解密权限。设计并实施访问控制策略，确保只有经过授权的用户或系统能够访问解密后的数据，这可以包括基于角色的访问控制、访问令牌等。定期更新密钥以增加系统的安全性，防止长期使用相同密钥导致的潜在风险。安全地分发和管理密钥，确保密钥的安全性，防止泄露或滥用。

4 云计算环境下物联网数据的加密存储算法设计流程

4.1 破解加密数据的方式与途径

破解加密数据是一项非常复杂和困难的任务，特别是在使用安全的加密算法和适当的密钥管理措施的情况下。攻击者尝试通过穷举所有可能的密钥来解密加密数据，这是一种基本的攻击方式，依赖于破解者能够在合理的时间内尝试足够多的可能密钥。攻击者使用预先生成的密码字典，尝试对数据进行解密，这种攻击方式依赖于用户使用弱密码或者常见的密码。攻击者通过监测加密和解密过程中的时序信息，可能获取有关密钥的信息，例如通过观察操作所需的时间，攻击者可能推断出关于密钥的一些信息。攻击者可以通过分析加密设备的功耗，推断出关于密钥的信息，这通常需要专业的设备和知识。关于社会工程学攻击，通过欺骗、诱骗或其他社会工程学手段，攻击者可能试图获取存储加密密钥的位置或获取合法用户的访问权限。通过恶意软件，攻击者可能试图获取用户的加密密钥或绕过加密过程，在物理设备上植入恶意硬件，可能导致泄露密钥或绕过加密算法。虽然目前量子计算机的实用性仍然是个未解之谜，但如果它们能够在未来被广泛应用，它们可能会破解当前使用的某些传统加密算法，例如 RSA 和椭圆曲线加密。

对抗这些潜在的攻击，要采取强大的加密算法、密钥管理实践、定期更新密钥、采用多层次的安全控制、教育用户使用强密码等。此外，还要及时关注新的安全威胁和漏洞，对系统进行定期的安全审计和漏洞扫描也是非常重要的。

4.2 明文与密文对比分析

在云计算环境下，物联网数据的加密存储算法设计旨在确保对抗各种攻击，包括对明文和密文的对比分析。对比分析试图通过观察明文和相应密文之间的模式、关系或其他特征，攻击者通过分析密文中的频率分布来猜测可能的明文，使用块密码模式，并在每个块中使用适当的填充（padding）以打破明文和密文之间的频率关系。攻击者尝试通过分析密文中的模式来推断明文，使用强随机性的初始化向量（IV）和适当的块密码模式来破坏可能存在的模式。攻击者通过分析密文和明文之间的相关性来推断密钥，选择适当的块密码模式，确保密文和明文之间的关系是复杂的、不可预测的。攻击者通过分析不同输入之间的差异来推断密钥，使用块密码时，采用差分密码分析抵抗性强的设计，并在设计中考虑差分分析攻击的可能性。攻击者通过分析流密码的流以推断密钥，采用强大的伪随机数生成器，确保生成的流密码是具有良好随机性的。

4.3 概率统计分析解密

在实践中，有时攻击者可能尝试通过统计分析来破解加密数据。针对使用传统块密码加密的数据，攻击者可能通过分析密文中的频率分布来猜测可能的明文，这对于一些较简单的加密算法和较短的密钥可能更为有效。攻击者尝试通过分析密文和明文之间的相关性来推断密钥，如果存在某种相关性，攻击者可能利用这种信息来逐步猜测密钥的一部分或整个密钥。如果存在一定的模式或结构在加密数据中，攻击者可能尝试通过模式识别方法来分析密文并猜测出明文的一部分或整体。针对使用流密码加密的数据，攻击者可能尝试通过分析密钥流和密文之间的关系来猜测密钥，包括通过分析密钥流的周期性或其他模式。这种攻击方法涉及对不同输入之间的差异进行分析，以推断密钥的一部分或整体，这对于某些块密码可能是有效的。需要注意的使现代的强加密算法（如 AES、RSA 等）都经过广泛的研究和分析，它们的设计目标是抵抗各种攻击，包括概率统计分析。在设计加密存储算法时，选择经过验证和广泛接受的加密算法，并采取适当的密钥管理措施，以增加攻击者破解的难度。

5 结语

综上所述，通过本文的讨论，深入探讨了加密存储算法的定义、要求、运行原理以及可能的攻击方式。强调了合适的加密算法的选择、密钥管理的重要性、访问控制的实施、性能和效率的平衡，以及遵循合规性法规的必要性。通过持续的研究和创新，可以进一步提升云计算环境下物联网数据的安全水平，为数字化时代的可持续发展做出贡献。

参考文献：

[1]高煌红.云计算数据存储安全的研究[D].杭州：浙江工业大学，2014.

[2]张健.全球云计算安全研究综述[J].电信网技术，2010（09）：15-16.

[3]李杰.云存储中文件加密存储和删除方法研究[J].小型微型计算机系统，2015，36（4）：836-839.

[4]高露.云计算环境下的工业物联网数据安全探讨与分析[J].通信电源技术，2021，38（18）：3.

[5]侯戌非.物联网环境下海量多源异构数据的存储算法[J].宁夏师范学院学报，2022，43（7）：6.

[6]王健.云计算网络环境和大数据结合的物联网信息化建设[J].中文科技期刊数据库（全文版）工程技术，2021（6）：2.