区块链技术提升云计算大数据存储与传输安全的探析

毛敬玉
兰州职业技术学院　甘肃兰州　730070

摘　要: 区块链引入云计算安全体系,旨在构建一个“业务上云,信任上链”的新型融合架构,以区块链作为分布式的信任锚点,对云中的数据状态与操作行为进行存证、验证与约束。本文旨在系统探析区块链技术如何具体赋能云计算环境，分别从数据存储与数据传输两个维度，深入剖析其提升安全性的内在机理，以期为构建下一代可信云数据基础设施提供有益的理论参考。

关键词: 区块链；云计算；大数据存储；加密传输；隐私保护

引言

随着数字化转型浪潮的深入推进，云计算已无可争议地成为现代社会海量数据存储、处理与分析的基础设施，其按需供给、弹性扩展的特性，极大地降低了企业与机构的IT运营成本，赋能了从人工智能到物联网的众多前沿科技领域。然而这种高度依赖中心化服务商的“数据托管”范式，在带来便捷高效的同时，也埋下了深刻的安全隐忧。恰逢其时，区块链技术作为一种以去中心化、不可篡改和可追溯为特征的分布式账本技术，为我们解决上述困境提供了全新的视角。基于此，文章就区块链技术提升云计算大数据存储与传输安全展开了相关探析，以供参考。

1 云计算与大数据存储与传输的安全风险分析

1.1 数据存储层风险

云计算环境下的数据存储层风险根植于其固有的“所有权与管理权分离”模式，用户把海量数据的物理控制权移交予云服务提供商，从而在数据完整性、隐私性与持久性方面埋下多重隐患。在完整性层面，中心化的存储架构使得数据资产高度集中于服务商的特定物理设备中，用户缺乏有效技术手段实时验证其数据是否被未授权篡改、删除或意外损坏，服务商内部管理疏漏甚至恶意操作均可导致原始数据被破坏，而传统的审计日志本身存储于服务商服务器，其可信度存疑，难以构成有效的问责证据。隐私性方面，静态存储的巨量数据必然会吸引黑客持续性的威胁攻击，单一存储节点的突破便可能导致大规模敏感数据泄露灾难。此外，云服务商内部管理员权限如果过高，缺乏完善的监督，就会存在非授权访问与窃取数据的现实风险。尽管服务商承诺了数据备份，但区域性基础设施故障、自然灾害或商业运营中断等风险，仍可能引发数据服务不可用乃至数据永久丢失的极端情况，用户在此类系统性风险面前往往束手无策，恢复数据完全依赖于服务商的应急能力。

1.2 数据传输层风险

大数据在迁移至云端以及在云内不同服务组件间流动的过程中，其传输通道构成了安全链条上的薄弱环节，存在被窃听、拦截与篡改的严峻威胁。数据在用户终端与远程数据中心之间必须穿越复杂且不可控的公共互联网，此间如果未采用强加密通信协议，传输中的数据包便会暴露，攻击者可通过中间人攻击等手段在网关、路由器等网络节点进行窃听，轻易获取敏感信息。即便启用加密，如果密钥管理不善或加密算法存在漏洞，安全防护依然可能被击穿。更为棘手的是在云服务商内部网络，即所谓“云内传输”过程中，多租户共享底层网络基础设施的特性带来了潜在的交叉数据泄露风险，恶意租户可能利用虚拟化层面的技术漏洞，窥探流向其他用户实例的数据流量，实现非法的数据越权访问。

1.3 访问控制风险

传统云计算环境依赖中心化的访问管理机制，访问控制策略的逻辑执行高度依赖于云服务商提供的统一身份认证系统，该系统一旦出现安全漏洞，便可能导致权限的泛化滥用，使得未授权用户获得超越其职责范围的数据访问能力，引发越权数据访问事件。在复杂的多租户场景中，权限的授予、变更与撤销流程繁琐，极易出现权限残留问题，即用户身份已变更，但其旧有数据访问权限没能被及时清除，形成安全隐患。更为深层次的风险在于权限管理的透明度缺

失，策略的制定执行完全由服务商后台操控，用户难以清晰验证“谁”在“何时”依据“何种规则”访问了其数据，一旦中心化的 IAM 系统本身遭遇入侵，攻击者便可凭借窃取的高权限凭证长驱直入，对整个系统的安全防线构成毁灭性打击。

2 区块链与云计算大数据安全融合的总体架构设计

2.1 融合逻辑

区块链与云计算大数据安全的融合逻辑是构建一个“业务上云，信任上链”的协同范式，以区块链弥补传统中心化云架构在安全可信方面的固有缺陷。两者融合是进行功能的分层互补，云计算继续发挥其强大的算力、弹性存储资源与高效服务体系，承载海量原始数据本身，保证整个系统的成本效益；区块链则作为分布式的信任锚点，专注于记录关键的操作元数据、数据完整性凭证、智能合约化的访问策略以及不可篡改的审计追踪日志。本质上，云计算负责处理海量信息的“重量”，而区块链则负责担保这些信息在流转与存储过程中的“质量”，二者共同构筑了一个既具备强大数据处理能力，又兼具高可信度的新型基础设施。

2.2 系统结构框架

基于上述融合逻辑，可构建一个清晰的四层系统结构框架。最底层是云存储计算层，其由传统的 IaaS/PaaS 服务构成，负责以加密形式实际存储海量原始数据，执行繁重的计算任务，是整个体系的性能基础。其上是核心的区块链信任层，通常采用权限可控、性能更优的联盟链架构，该层不直接存储大数据本身，而是持久化地记录数据的哈希摘要、访问控制智能合约、数据资产所有权凭证以及所有操作的精炼日志，形成一个多方共同维护的安全证据链。协议层作为连接云与链的桥梁，提供了标准化的 API、SDK 以及安全通信协议，其负责自动化地执行诸如“计算数据哈希并上链”“触发智能合约进行权限验证”“同步操作事件至分布式账本”等任务，保证两层之间的数据同步与逻辑联动高效可靠。最顶层的应用层则面向最终用户，承载各类具体的大数据业务场景，用户通过该层享受云服务的便捷，同时其每一步操作的安全性都由底层的区块链信任层予以保障。

3 区块链提升云大数据存储安全的机制研究

3.1 去中心化存储提升数据完整性

区块链技术通过其去中心化架构，为云大数据完整性验证提供了一种无需信任第三方的解决方案。其主要机制在于把云中存储数据的哈希值，一段定长且唯一的数字指纹锚定在不可篡改的分布式账本上。具体而言，当用户把文件上传至云端存储后，系统会即时计算该文件的密码学哈希值，此哈希值作为一项交易记录写入区块链区块中，随后通过共识机制在网络中广泛传播并得到永久确认。任何后续对云端文件的微小修改，哪怕是单一比特位的变动，都会导致其哈希值发生雪崩效应，产生与链上记录完全不符的新哈希。因此，用户或任何验证方无需下载整个原始文件，仅重新计算云端文件的当前哈希并与区块链上存储的原始哈希进行比对，即可高效地判定数据自存储以来是否保持了完整无损。为进一步优化大文件处理效率，系统可以引入 Merkle 树结构，大文件分割成多个数据块，只把树的根哈希存储于链上。验证时，只要提供特定数据块到根哈希的路径哈希集合，即可完成该数据块的局部完整性证明，极大地降低链上负载，使得海量云数据的完整性审计变得轻量化、常态化与自动化，彻底消除了对云服务商单方面承诺的依赖。

3.2 数据访问控制的智能合约化

区块链的智能合约是把数据访问控制策略从中心化服务器的配置文件中解放出来，转化为在去中心化网络中自动执行、规则透明的数字法律，实现了权限管理的范式转移。访问规则如“允许角色 A 在时间 T 内访问资源 B”被编码成智能合约代码，部署到区块链上，其逻辑对所有相关方公开可见且一旦部署便无法被任何单一实体擅自修改。当用户发起数据访问请求时，请求会触发链上对应的智能合约。合约自动验证请求者数字签名的真实性、检查其身份属性是否满足预设条件、核实访问上下文。只有全部条件通过验证，合约才会自动执行，向请求者颁发一个有时效性的加密访问令牌，或直接向云服务端发送一条授权指令。整个过程排除了人工干预的可能性，保证了权限授予的公平性。更重要的是，任何权限的变更，例如授予新权限或撤销旧访问权，都必须通过向智能合约发送新的合法交易来完成，这些操作本身被作为不可逆的记录永久刻在账本上，形成了完整且可追溯的权限生命周期管理轨迹，从根本上杜绝了权限滥用的发生。

3.3 数据主权与可信审计

区块链技术通过建立不可篡改的数据操作流水账，重塑了云环境下的数据主权边界。在此机制下，用户对其数据的所有权和控制权得到了密码学的强化证明，数据主权通过

链上记录的数据哈希、所有权声明以及访问规则合约得到了实质性的彰显。所有围绕数据生命周期的事件，包括但不限于数据的创建、授权、访问、修改、共享乃至删除意图，都被转化为标准化的交易，经过数字签名后按时间顺序记录于分布式账本，形成一个全局一致、时序明确、无法单方面否认的操作历史序列。审计员无需再依赖云服务商提供的、可能被过滤或修改的中心化日志，而是可以直接接入区块链网络，作为一个平等节点独立验证完整的操作历史。任何试图掩盖违规访问或恶意操作的行为都变得不可能，因为要篡改审计线索，攻击者必须同时控制分布式网络中超过 51% 的节点并改写整个链条，在实际中成本极高近乎无法实现。这种可独立验证的审计追踪能力，极大地增强了系统的可问责性，也为合规性检查、纠纷仲裁提供了具有法律效力的电子证据，最终在用户与服务商之间建立了一种基于技术验证的全新信任关系。

4 区块链提升云大数据传输安全的机制研究

4.1 分布式密钥管理体系

传统云数据安全严重依赖中心化的密钥管理服务，该服务一旦被攻破，整个系统的加密防线会瞬间崩塌。区块链技术通过引入分布式密钥管理体系，从根本上瓦解了单点故障风险。在该体系中，用于加密传输数据或验证身份的私钥不再由单一机构托管，而是通过先进的密码学方案进行分布式安全存储。例如，采用门限签名或秘密共享技术，主私钥分割成多个密钥分片，分发给由不同参与方维护的区块链节点。当要进行数据解密或交易签名时，必须收集超过预设阈值的足够数量的密钥分片，才能在本地临时重构出完整的私钥完成操作，而完整的私钥自始至终不会在任何单一节点上完整出现。即使个别节点被入侵导致其密钥分片泄露，攻击者也无法凑齐重构私钥所需的全部碎片，系统整体依然安全，密钥的管理权从中心化服务商交还给了用户或其信任的分布式网络共同体，实现了密钥管理的“去中心化信任”，为数据传输的端到端安全建立了信任根基。

4.2 可信身份认证机制

区块链以其不可篡改的特性，为云数据传输的参与方构建了一套全新的可信身份认证机制。该机制的重心在于把实体的身份信息转化为可独立验证的去中心化标识符和可验证凭证，将其所有权和控制权归还给实体自身。用户的身份凭证，如数字证书、属性证明等，经由可信发行者签名后，其哈希或精炼后的证明被记录在区块链上，作为验证该凭证真实性的信任锚点。在进行数据传输前，参与方无需向中心化的认证服务器提交用户名和密码，而是通过呈现其拥有的可验证凭证，利用对应的私钥完成一次数字签名，即可向对方证明其身份所有权且无需暴露任何敏感信息。接收方则可通过查询区块链上的对应记录，快速验证对方所提供凭证的签名有效性。此过程完全在点对点之间完成，消除了对中心化身份提供商的高度依赖，有效防止了因认证服务器被攻破而导致的全局身份信息泄露。同时，基于区块链的身份认证天然具备抗审查的特性，即使某个认证节点离线，用户仍可通过其他节点或直接与链上数据交互来完成身份验证。

4.3 加密传输与篡改防护

在传输发起前，基于区块链的可信身份认证机制保证了通信双方身份的可靠性，双方随后可以利用区块链平台安全地交换或协商用于本次会话的对称加密密钥，例如把临时生成的公钥记录于链上或通过智能合约执行安全的密钥交换协议，从而保证只有经过验证的合法参与方才能获取解密密钥。在数据传输过程中，所有流通的报文均使用高强度对称加密算法进行加密，使得即使在不可信的网络通道中被截获，黑客得到的也只是一堆无法解读的密文。同时，区块链的时间戳特性为数据传输提供了强大的篡改探测能力。发送方可以为数据包或数据流生成哈希摘要，同步锚定至区块链，接收方在解密数据后，可重新计算哈希值并与链上记录进行比对，任何在传输途中发生的数据篡改或丢包，都会导致本地计算的哈希值与链上凭证无法匹配，从而使此次传输失效。

5 结语

综上所述，本文系统论证了区块链技术如何为云计算大数据的安全存储与传输构建可信基础，通过“业务上云、信任上链”的融合架构，区块链以其去中心化、不可篡改和可追溯的技术特质，化解了传统云环境在数据完整性、隐私保护、访问控制和安全审计方面的固有风险。智能合约实现了权限管理的自动化，分布式账本奠定了可信审计的基础。尽管在性能与标准化方面仍面临挑战，但“云链结合”无疑为构建下一代安全高效的数据基础设施指明了发展方向，对推动数字经济健康发展具有深远意义。

参考文献：

[1] 杨伟超 , 尹廷钧 , 赵海涛 , 等 . 基于区块链技术的本

地化云计算大数据的应用探析 [J]. 科技视界 , 2022(14):9.

[2] 邓攀 , 温雪 . 工业互联网中基于区块链的大数据加密传输与存储机制探究 [J]. 中国宽带 , 2025(5):46.

[3] 王晨宇 , 王洪彬 , 徐士博 , 等 . 基于区块链技术的数据存储和传递系统设计 [J]. 物流科技 , 2023(7):29–31.

[4] 李世寅 . 未来已来 : 区块链技术在智慧法院建设中的运用前景探析 [J]. 信息安全与通信保密 , 2019(10):12.

[5] 方健 . 基于区块链和 IPFS 的物联网安全模型与数据共享研究 [D]. 浙江工商大学 ,2023.

作者简介：毛敬玉（1981—），女，汉族，甘肃临夏，硕士，副教授，研究方向： 计算机网络，云计算。