跨平台文件型数据库用户访问多阶段身份认证方法

薛婷婷[1] 王静武[1] 张 静[1] 戴欣彤[1] 呼 鑫[1]
XUE Tingting WANG Jingwu ZHANG Jing DAI Xintong HU Xin

摘 要 目前，用户身份认证方法主要依赖单一或双因素认证机制，通过预设的认证协议验证用户身份，由于缺乏对机构节点的信任评估，导致认证安全性不佳。对此，文章提出了一种跨平台文件型数据库用户访问多阶段身份认证方法。通过引入权威节点作为信任锚点，将椭圆曲线加密技术生成公私钥对，采用用户端结合机构节点的验证操作，使公钥与身份标识绑定后注册至认证节点。同时，以节点注册过程中收集到的节点信息作为初始数据，通过构建加权有向图，对机构节点全局可信度进行计算。综合用户对跨平台文件资源的上传及下载记录数据和计算节点贡献值，并根据用户综合认证可信度的阈值判断结果，实现多阶段身份认证。在实验中，对提出的方法进行了认证安全性的检验。最终测试结果表明，采用提出的方法进行用户身份认证时，平均数据隐私保护率达到 96% 以上，具备较为理想的认证安全性。

关键词 跨平台；文件型数据库；用户访问；多阶段；身份认证

doi：10.3969/j.issn.1672-9528.2025.09.037

0 引言

在数字化时代，数据已经成为推动社会发展和企业运营的核心资产。随着信息技术的飞速发展，跨平台文件型数据库作为一种数据存储和管理的重要形式，已经广泛应用于金融、医疗、教育、科研等众多领域。允许用户在不同的操作系统和设备上无缝访问和管理数据，极大地提高了数据的可用性和灵活性。跨平台数据库的数据来自于多个不同的平台以及数据源，因此在进行数据访问时，需要对用户身份进行严格的认证，从而防止未授权访问或数据泄露的情况发生。目前常规的用户身份认证方法主要依赖于单一的用户名 / 密码验证操作，但由于密码容易被破解，或通过钓鱼手段进行窃取，所以导致安全性不高。同时，随着业务规模的不断扩大，也为数据库的维护和管理提出了更高的要求。随着跨平台文件型数据库的广泛应用，其安全性面临着前所未有的挑战。用户访问数据库时的身份认证问题，成为保障数据安全的关键环节。

近年来，身份认证技术取得了显著的发展成果。例如，文献 [1] 通过 SM2 算法生成公私钥对，将公钥与身份标识上传至认证服务器。在用户认证阶段，服务器生成随机挑战值，用户利用私钥签名后返回，服务器通过 SM2 验证签名并比对

1. 甘肃科源电力集团有限公司 甘肃兰州 730046

[2] 薛翔 , 沈斯杰 , 陈榕 . 一种使用索引式备份的范围查询方法 [J]. 小型微型计算机系统 , 2018, 39(8): 1781-1786.
[3] 那海洋 , 杨庚 , 束晓伟 . 基于 B+ 树的多关键字密文排序检索方法 [J]. 计算机科学 , 2017, 44(1):149-154.
[4] 吴润泽 , 蔡永涛 , 陈文伟 , 等 . 面向多源异构数据源的实际范围索引树索引方法 [J]. 电力系统自动化 , 2016, 40(11): 121-125.
[5] 王洪强 , 李建中 , 王宏志 . 基于 F&B 索引的 XML 查询处理算法 [J]. 计算机研究与发展 , 2010, 47(5): 866-877.

【作者简介】
王长河（1982—），男，山东邹城人，研究生，主任，研究方向：软件开发设计、电力运维。
张春花（1981—），女，山东曹县人，本科，部门经理，研究方向：软件开发设计、电力运维。
张凌霄（1997—），男，山东济宁人，本科，市场经理，研究方向：软件开发设计、电力运维。
高新立（1989—），男，山东曹县人，专科，工程经理，研究方向：软件开发设计、电力运维。
宋圣坤（1995—），男，山东青岛人，本科，研究方向：软件开发设计、电力运维。

（收稿日期：2025-04-22 修回日期：2025-09-12）

公钥哈希值完成身份确认。但由于该方法过于依赖静态公钥基础设施，导致在复杂认证场景下，方法的认证安全性无法得到有效保证。文献[2]通过智能合约对用户的身份进行注册，并基于时间戳与随机数，动态生成一次性验证令牌，通过区块链共识机制验证交易合法性；身份权限更新通过链上投票机制实现，确保去中心化控制。但由于动态令牌生成依赖本地时钟同步，若时钟偏差超过阈值将导致认证失败，同时也会对认证安全性产生一定影响。

本文提出了一种跨平台文件型数据库用户访问多阶段身份认证方法。该方法通过融合全局可信度以及节点贡献值，通过多阶段的认证流程来确保用户身份的真实性和合法性。首先，该方法引入了基于行为分析的可信度评估机制，通过分析用户的历史行为数据，评估用户行为的可信度；其次，该方法结合了节点贡献值，即用户对数据库系统的贡献程度，通过节点贡献值来调整认证流程的严格程度；最后，该方法通过多阶段的认证流程，包括但不限于行为分析、知识问答、生物特征验证等，来综合评估用户的身份。这种方法不仅提高了用户身份认证的安全性，同时也提升了用户体验，因为它能够根据用户的具体情况动态调整认证流程，既保证了安全性，又避免了不必要的繁琐认证步骤。

1 跨平台文件型数据库用户访问多阶段身份认证方法

1.1 跨平台文件型数据库用户访问认证节点注册

为了实现跨平台的文件型数据库用户访问多阶段身份认证，本文提出了一种新的方法，即引入权威节点的概念。这种方法利用了先进的椭圆曲线加密技术，通过结合全局参数和随机数来生成公私钥对。此外，结合机构节点的验证操作，可以实现用户访问身份的节点注册。这种方法不仅提高了安全性，而且也使得用户访问更加便捷。具体的注册流程如图1所示。

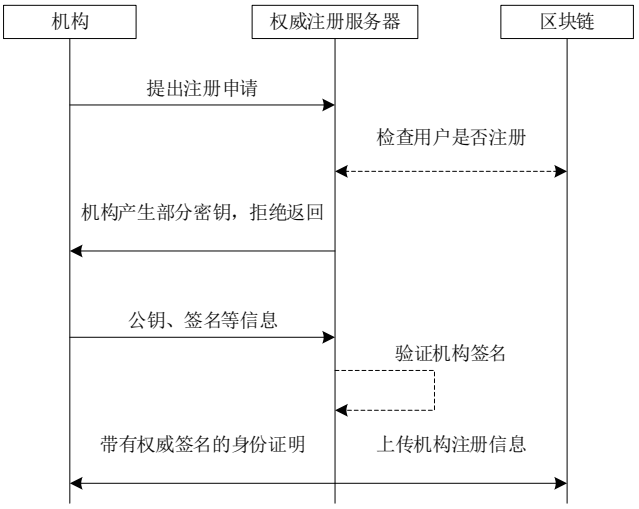

图1 跨平台文件型数据库用户访问认证节点注册流程

在跨平台文件型数据库的上下文中，假设每个组织、企业或机构的实体节点被称为机构节点。这些节点不仅拥有独立的身份标识，还配备了一套完整的权限管理体系[3]。当权威注册服务器接收到来自跨平台文件型数据库用户的注册申请时，它首先会进行时间戳的合理性检查。这一过程涉及验证时间戳是否落在了允许的注册时间窗口内。随后，服务器会查询区块链，以确认在该时间段内是否已经存在了相同机构的注册记录。如果发现该机构已经存在，则权威注册服务器会直接拒绝该注册申请，这样做是为了防止重复注册的发生，同时避免了由此可能引发的安全风险；反之，如果确认该机构不存在，则注册流程会继续进入下一步[4]。一旦注册申请通过了初步验证，权威注册服务器将基于全局参数为机构节点生成一对公钥和私钥。这一对密钥的生成是基于椭圆曲线加密技术，其具体的数学表达式为：

$$R_i = \mathrm{mod}\, q\left(\delta_i \times P + r_i + \beta_j\right) \tag{1}$$

式中：R_i 和 δ_i 分别代表机构节点 i 的公钥以及秘钥；P 代表椭圆曲线上加法群的生成元；r_i 代表权威节点选择的随机数；β_j 代表相邻权威节点选择的随机数；q 代表一个素数。

机构节点在接收到权威注册服务器返回的公钥和私钥（初始部分）后，验证返回的信息是否与提交的信息相符。待验证通过后，机构节点会选择一个随机数 ε_i，并结合全局参数 α_2 以及第二个碰撞哈希函数 H_2，生成完整的公钥 $R_i^{'}$ 和私钥 $\delta_i^{'}$。具体表达式为：

$$R_i^{'} = R_i + \varepsilon_i + P^{\alpha_2} \tag{2}$$

$$\delta_i^{'} = \delta_i + \varepsilon_i \tag{3}$$

考虑到跨平台文件型数据库往往涉及多个平台和数据源，数据在传输和存储过程中易受到篡改。因此为了进一步增强注册过程的安全性和可追溯性，机构节点会使用其完整的私钥对注册信息进行签名[5]。签名信息生成表达式为：

$$\psi_i = \mathrm{mod}\, q\left(u_i + \delta_i^{'} + \varepsilon_i \times \alpha_3\right) \tag{4}$$

式中：ψ_i 代表机构节点 i 的签名信息；u_i 代表机构节点选择的随机数；α_3 代表第三个全局参数。

当签名信息验证通过后，机构节点的注册信息和签名信息会被正式记录到区块链上，从而完成数据库用户访问认证节点的注册操作。

1.2 跨平台文件型数据库机构节点全局可信度计算

以跨平台文件型数据库用户访问认证节点注册过程中收集到的节点信息作为初始数据，通过构建信任关系网络，对机构节点的全局可信度进行计算。

将每个跨平台文件型数据库机构节点视为加权有向图

$G(V, E)$ 中的一个顶点 $v \in V$，若存在有向边 $e(u, v)$，则代表节点 u 向节点 v 存在请求资源操作。边的权重为节点 u 对节点 v 的推荐度 [6]，具体推荐度 R_{ij} 计算公式为：

$$R_{ij} = \frac{S_{ij} - F_{ij}}{\sum_{k} T_k S_{kj}} \tag{5}$$

式中：S_{ij} 和 F_{ij} 分别代表 t 时段内，跨平台文件型数据库组织或企业等机构节点 i 与节点 j 交易成功或失败的次数统计结果；k 代表已经与机构节点 j 产生过交易记录的节点；T_k 代表节点 k 对应的全局可信度。

结合上述推荐度，可以对跨平台文件型数据库中的组织机构节点的全局可信度进行计算，具体计算公式为：

$$T_i = \sum_{k=1}^{R_{ij}} T_k \times R_{ki} \tag{6}$$

上述计算得到的全局可信度 T_i 可以反映机构节点的最新信誉，用于后续的身份认证策略设计与调整。

1.3 跨平台文件型数据库用户访问多阶段身份认证流程设计

结合用户历史行为数据和机构节点全局可信度，计算用户综合认证可信度，并通过可信度阈值检查确定用户在各访问控制策略中的权限，从而实现多阶段身份认证。

在初始认证阶段，用户注册时收集用户身份信息和初始资源。用户提交身份凭证和资源行为数据至认证服务器。其中，身份认证包括用户名、密码以及数字证书等，资源行为数据包括用户对于跨平台文件数据的初始上传和下载量 [7]。假设 U_i 代表用户在机构节点 i 进行的跨平台文件型数据的资源上传量，D_i 代表对应的资源下载量，则可以对节点贡献值 AR_i 进行计算。具体计算公式为：

$$\mathrm{AR}_i = \xi \times \frac{U_i}{U_i + D_i} + (1 - \xi) \times \frac{I_i}{M_i} \tag{7}$$

式中：I_i 代表用户在机构节点 i 的推荐次数；M_i 代表总交易次数；ξ 代表权重因子。

在用户综合认证可信度评估阶段，将节点贡献值与节点全局可信度进行结合，对用户的综合认证可信度 Q_i 进行计算。具体计算公式为：

$$Q_i = \gamma_1 \times T_i + \gamma_2 \times \mathrm{AR}_i \tag{8}$$

式中：γ_1 和 γ_2 分别代表权重系数，用于衡量全局可信度以及节点贡献值之间的贡献程度。

通过设定综合阈值 θ，对用户访问权限进行分配。当用户的综合认证可信度高于设定阈值，则为其分配高可信度权限，允许其访问核心数据资源及执行关键操作；若综合认证可信度低于阈值但满足基础认证条件，则分配低可信度权限，限制其仅访问非敏感数据或执行普通操作。

2 实验论证

2.1 实验准备

实验通过部署多台服务器模拟跨平台数据库节点，并配置不同网络带宽和延迟，以此搭建出网络测试结构。对此，实验采用了 10 台服务器，其中 1 台作为中心认证服务器，9 台作为边缘数据库节点。为实现跨平台覆盖，9 台边缘数据库节点分别采用 3 台 Linux 服务器（Ubuntu 20.04 LTS）、3 台 Windows 服务器（Windows Server 2019）以及 3 台 macOS 服务器（macOS Big Sur）。由此搭建出的星型网络拓扑结构如图 2 所示。

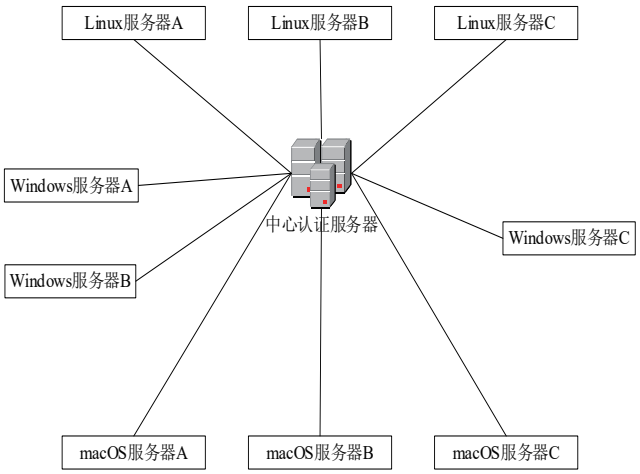

图 2 星型网络拓扑结构

实验选取的跨平台文件型数据库采用分布式架构设计，覆盖 3 个主要地理区域（北美、欧洲、亚洲），每个节点部署独立的数据存储与计算模块。数据库总存储容量为 500 TB，日均文件访问量达 200 万次。实验对用户行为进行模拟，模拟出 3 种不同的用户，分别为高贡献用户、普通用户以及恶意用户。并分别模拟出两种不同的安全事件，即 DDoS 攻击以及 SQL 注入攻击。日均跨节点文件访问量占比 35%，其中高贡献用户发起的跨节点访问占比 80%。机构节点间日均数据共享请求达 1 200 次。具体模拟参数如表 1 所示。

表 1 用户行为模拟参数

用户	用户数量	每日上传数据量 /GB	每日推荐次数 / 次	每日下载数据量 /GB	非法访问次数 / 次	模拟时间周期 / 天
高贡献用户	200	10±2%	50±5%	2±15%	0	30
普通用户	4 500	1±10%	5±10%	3±10%	0	30
恶意用户	300	0.5±5%	0（恶意用户不推荐）	20 ±5%（模拟高下载需求）	50±10%	30

设定 DDoS 攻击的攻击频率为每周一次，峰值为 500 Mbit/s，SQL 注入的模拟频率为每日随机 10 用户，成功率 1%。过去 30 天内检测到 2 500 次异常访问尝试，其中 SQL 注入攻击占比 40%，DDoS 攻击占比 30%。在上述用户行为模拟的基础上，分别采用本文方法以及两种常规方法进行模拟用户身份认证。同时记录不同认证方法下，非法访问尝试总次数以及非法访问成功次数，从而计算出跨平台文件型数据的隐私保护率，实现认证安全性的对比。实验选取的认证方法分别为连接场景下基于国密算法的身份认证方法以及基于区块链的去中心化动态身份认证方法。

2.2 认证安全性对比

3 种认证方法下的数据隐私保护率对比结果如图 3 所示。

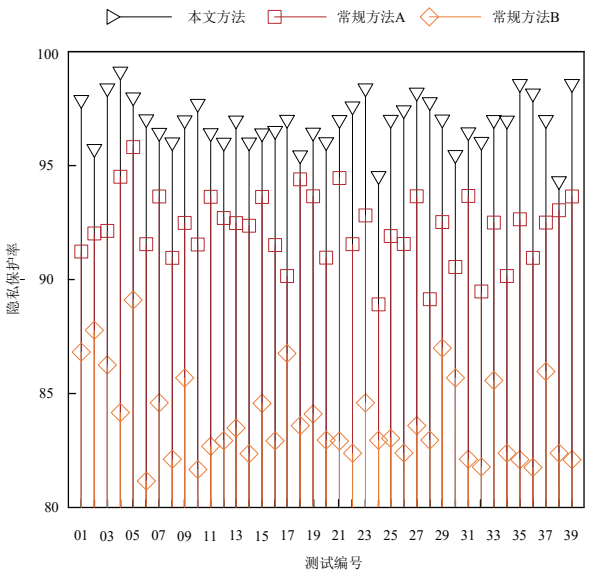

图 3 数据隐私保护率对比结果

通过上述实验结果可以看出，相较于两种常规的用户身份认证方法，本文所提出的多阶段身份认证算法表现出更为优越的安全性，平均数据隐私保护率达到 96%，以此可以证明本文方法能够有效抵御跨平台环境下的复杂攻击。

3 结论

在当今数字化时代，跨平台文件型数据库的复杂应用场景日益增多，其中用户身份认证的安全性以及动态信任管理成为保护数据资产的关键挑战。本文提出了一种创新的多阶段身份认证方法，该方法通过引入权威节点信任锚点，并结合先进的椭圆曲线加密技术，实现了对节点全局可信度的评估以及贡献值的动态计算。这种方法有效地突破了传统单因素或双因素认证方法所固有的静态信任局限性。通过一系列的实验验证，发现该方法在跨平台兼容性、数据隐私保护率（达到 96% 以上）以及抗攻击能力方面都表现出了显著的优势。这些成果不仅为构建细粒度的动态信任体系提供了坚实的理论基础，同时也为实践操作提供了可行的范式。展望未来，进一步研究基于实时行为分析的动态信任更新模型，探索将零知识证明等隐私增强技术与之融合的可能性，并考虑利用区块链技术实现去中心化的信任锚点管理。这些努力将推动跨平台认证体系朝着更加智能、自适应的方向发展，将极大地提升在多机构协作场景下的数据安全治理能力，为构建数字时代可信数据生态提供关键技术保障。

参考文献：

[1] 王宏，赵雨昕 . 无连接场景下基于国密算法的身份认证方法 [J]. 计算机与现代化，2025(1):120-126.

[2] 朱金涛，魏银珍，尚晓晓 . 基于区块链的去中心化动态身份认证系统 [J]. 计算机应用与软件，2025,42(1):333-337.

[3] 张朝阳，王建祥，侯乃明，等 . 基于大数据与区块链的智能平台身份认证技术 [J]. 高技术通讯 ,2024,34(12):1279-1285.

[4] 宋岍龙 . 基于 SPEA-II 算法的网络多层次安全访问控制方法 [J]. 计算机测量与控制，2024,32(6):173-179.

[5] 赵一霈，谭海波，张中贤，等 . 基于区块链和密码累加器的自我主权身份认证方案 [J]. 计算机应用研究，2022, 39(6): 1633-1637.

[6] 王家峰 . 基于混合算法的互联网访问用户身份认证方法 [J]. 齐齐哈尔大学学报 (自然科学版), 2024, 40(3): 5-10.

[7] 刘鹏飞，宫志强，韩佳乐 . 基于 SSL VPN 的智慧校园统一身份认证平台建设 [J]. 网络安全技术与应用，2023(6): 91-93.

【作者简介】

薛婷婷（1990—），女，甘肃秦安人，硕士研究生，中级经济师，研究方向：招投标管理、数据分析与管理、数据安全。

王静武（1985—），男，甘肃兰州人，本科，工程师，研究方向：招投标管理、数据安全。

张静（1984—），女，甘肃武威人，专科，研究方向：招投标管理、数据分析与挖掘。

戴欣彤（1981—），女，天津人，专科，研究方向：招投标管理、数据安全。

呼鑫（1971—），男，河北海兴人，本科，高级工程师，研究方向：系统集成与测试、招投标管理、数据安全。

（收稿日期：2025-04-07 修回日期：2025-09-08）