New SQL 数据库技术在用户隐私数据安全保护中的应用

王怡婷 傅杰 林德威 肖传奇 吕智垒

（国网福建省电力有限公司信息通信分公司 福建省福州市 350013）

摘要：随着互联网普及，网络在日常生活方方面面扮演重要角色。在为大众提供便利服务和更多信息资料的同时，也面临隐私、安全问题挑战。尤其是互联网持续发展，全面保证用户隐私数据安全、营造安全应用环境成为大众关注重点。New SQL 数据库技术作为一种新兴的数据库管理范式，在应对传统 SQL 数据库在面对大规模数据和复杂查询时的局限性方面占据明显优势，其具备更好的灵活性和可拓展性，可以引入先进的加密、访问控制和审计机制，为用户隐私数据保护提供更为全面的保护。基于此，文章以 New SQL 数据库技术为基础，探究其在用户隐私数据安全保护中的应用价值，旨在为用户隐私数据安全保护提供更多参考。

关键词：数据库；New SQL 技术；用户安全隐私数据；安全保护；应用

引言：随着数字化时代的迅速发展，大数据的涌现以及信息科技的普及，用户个人隐私数据的安全问题日益引起广泛关注。在这个信息爆炸的时代，传统的数据库管理技术逐渐显露出其在用户隐私保护方面的薄弱性。隐私数据泄露和滥用不仅对个人权益构成潜在威胁，也对社会和企业造成了严峻挑战。因此，研究如何更好地保护用户隐私数据，成为数据库技术领域亟待解决的问题之一。在此背景下，相关研究持续开展，New SQL 数据库技术在研究支持下应运而生，作为传统 SQL 数据库的一种新兴范式，在用户隐私数据安全保护方面展现出独特的优势。因此，文章对该技术在用户隐私数据安全保护中的应用展开分析具有现实意义。

1 研究内容概述

现阶段，互联网技术的快速发展为人类发展提供助力，但网络作为一把“双刃剑”，也使得用户隐私数据暴露在危险中，严重的还面临经济损失。究其原因，与用户网络私密数据保护体系不完善有紧密联系。想要全方位提升用户隐私数据安全性，提升数据加密效果，营造稳定的应用环境是基础[1]。

此时，在研究成果支持下，New SQL 数据库技术被应用在用户隐私数据安全保护领域。文章以该技术为基础，对数据进行预处理提取隐私数据特征，然后构建等距加密保护结构，并在此基础上设置 New SQL 协同加密模型，将分布式动态的 New SQL 数据库引入数据防护程序之中，发挥 HTAP（Hybrid Transactional/Analytical Processing）优势，混合处理用户隐私数据。

2 实际应用分析

2.1 数据预处理

网络用户的个人信息和隐私数据常规是采取单向加密模式进行保护的。这种方法也可以起到预设保护效果，但随着网络环境日益复杂，以特定格式导出的数据很容易遭到泄露或者被恶意利用。为了有效缓解这一问题，提升用户数据隐私加密效果，采取定向转换模式对数据进行预处理，改变常规加密模式有积极作用。

数据预处理是首要步骤，在此过程中，需要结合数据具体规模，对加密权重进行设计，同时需要科学设定数据属性值。一般按照下表 1 进行设定。

表 1 数据预处理参照表

用户人数	加密权重范围	数据属性比值
20 人	1.02-1.42	0.21
35 人	1.29-1.56	0.33
55 人	1.32-1.67	0.38
80 人	1.46-1.85	0.42

结合表 1 相关参考值，可以对数据基础性指标做出预设。将此时系统平台中的用户隐私信息标定为权重同等状态，则可以按照如下公式设定加密临界值。

$$Q=2\sqrt{m^3\cdot\frac{m^3d_2}{md_1}}-\sum_{i=1}\left(id_2+n\right)$$

上述式子中：Q 代表加密临界值；m 代表特征值；n 代表临界加密范围；d_1 代表数据属性初始值；d_2 代表数据属性绝对值；i 代表归一系数。

按照如上公式计算得出实际的加密临界值，然后在应用 Min-max 定向规范法对用户隐私数据进行归一化转化，结合 NewSQL 数据库技术科学布设利群转换节点，此时可以得出修正加密均值[2]。计算公式用如下公式表示：

$$V'=\frac{V-\min_a}{\max_a-\min_a}\cdot\left(new\_\max_a-new\_\min_a\right)+new\_\min^{a-1}$$

上述式子中：V' 代表修正加密权值；V 代表定向属性值；$\max_a$ 表示离群转换最大值；$\min_a$ 表示离群转换的最小值；a 表示加密次数。

通过上述两个公式计算，准确得出修正加密均值，此时便可以依据数值构建数据预处理层，为稳定的数据防护环境营造奠定基础。

2.2 隐私数据特征提取

隐私数据特征提取是从大量的隐私数据中抽取关键信息或特征，而不暴露个体的敏感信息。这是在保护隐私的同时进行数据分析和挖掘的重要步骤。结合文章提出的数据安全保护思路来看，完成数据预处理之后，隐私数据特征提取是重点环节。其主要目的是结合文章提出的用户隐私数据安全保护方法，提出符合需求的数据特征提取策略。

具体来看，提取过程如下：依据标定系统功能，以采用的加密评估标准为参照，发挥安全防护指令筛选功能，确定最有特征子集的特点。此过程中，New SQL 技术发挥重要作用，将隐私数据按照相对应的模块模式，科学分布在数据库之中，并以计算所得的平均值为参考，确定加密范围。为了对信息加密等级做出区分，设定同类标准和不同类标准两类参考，以便在数据中确定核心加密信息，最后，获得的权值按照顺序进行排列，此时数据特征提取过程完成[3]。

2.3 等距加密保护结构构建

等距加密保护结构是一种基于等距加密（Homomorphic Encryption）技术的安全结构，旨在在保障数据隐私的同时，允许在加密状态下进行计算和分析。其构建主要步骤如下：首先选择等距加密算法，然后确定密钥管理方式，对数据做好分类，并有序做出标记，最后，对标记的数据进行等距加密操作，结合最终结果确定该结构能否按照预期完成加密操作。并进行数据传输验证，确定在数据传输中，该加密保护结构可以正常运行，防止数据被窃取或者篡改。

2.4 New SQL 协同加密模型设计

New SQL 协同加密模型的设计旨在为数据库系统引入高效而安全的加密机制，以确保在数据存储和传输过程中的隐私保护。完成上述步骤后，以用户信息和数据为基础，验证模型的动态调整灵活性，并发挥混沌处理方法优势，确保数据状态变量精准得到确定，为安全网络环境奠定基础。

一旦用户隐私数据遭受攻击，构建的模型关联的协同加密模块会做出预警，立即做出响应，采取科学措施提升数据库安全防护等级[4]。

依托 New SQL 技术构建协同加密程序，可以依据如下公式计算二次加密系数：

$$\omega_{\mu}=M(p)-\frac{C=\{C_1,C_2,\cdots,C_N\}\times p_1}{p=\{p_1,p_2,\cdots,p_n\}}$$

上述式子中：ω_{μ} 代表二次加密系数；μ 代表加密次数；$M(p)$ 代表协同差值；C 代表加密排序；C_1-C_N 代表动态加密距离；p 代 表数据库覆盖 排序；p_1-p_n 代表覆盖距离。

按照上述公式得出加密系数后，所得信息作为加密标准，为模型加密功能发挥提供支撑。

2.5 分布式动态 Ne w SQL 数据库引入

继上述步骤后，科学引入分布式动态数据库，以期提升加密安全性。主要步骤如下：确定需求，然后评估分布式动态数据库技术特性，针对数据库功能需求，科学搭建基础环境，并安装、配置相关系统，为其运行奠定基础。最后需要进行性能测试，确保引入数据库之后，整体运行良好，可以达到预期需求。建设完成之后，需要对混沌加密方式进行优化，并增设加密识别模块，以确保充分发挥 New SQL 数据库优势，有效避免信息泄密事故发生。

2.6 HTAP 混合处理完成用户隐私数据保护

HTAP（混合事务/分析处理）具备支持实时事务处理和复杂分析查询能力，因此，经过科学设计，也具备一定保护用户隐私数据的作用。文章完成上述步骤后，发挥 HTAP 优势，与构建的加密模型进行关联，从而确保模型充分发挥作用。此时 HTAP 在模型获取数据基础上，可以借助科学方法构建动态矩阵，从而按照预设的范围对数据进行调整，且可以促使密钥覆盖范围按照预期发挥效用，实现双重加密[5]。

3 测试分析

为了验证上文提出的基于 New SQL 数据库技术的用户隐私数据安全保护体系应用效果，在此采取试验，对其性能进行检验。

3.1 准备工作

文章选择 100 名用户信息数据作为测试对象，比较传统的蜜罐数据加密方法、大数据加密方法和本文方法的优越性，以结果为依据加以验证。在验证之前需要科学搭设测试环境。

在搭建测试平台时，CPU 选择 NVIDIA GeForce RTX 3080，显存选择 16GB GDDR6，固态硬盘为 1TB 的系统作为基础环境。在该条件下，使用 Hyper-V 数据虚拟化软件，建立多个虚拟机，构建数据安全环境。虚拟机与大数据处理平台建立关联，确保 100 名用户数据按照规定格式成功导入[6]。

基于测试主要内容分析，构建的平台主要是对其身份验证环节性能展开测试。同时，此过程中需要验证数

据筛选、数据审核和数据过滤等功能使用效果。一般情况下，常用的身份验证方式包括人脸验证识别、指纹验证等，文章为了便于测试，统一设定研究的 100 名用户均采用密码验证方式通过身份验证。并且借助 MAP 格式将所有信息数据划分为默认防护模块。为了全方位收集测试结果信息，在每一模块均设置监测节点，负责监测和获取数据。但需要注意，如果发现异常，节点则作为定向保护结构发挥作用，此时监测和获取数据不再是唯一功能。测试中搭建的密钥防护模块的应用如下图 1 所示。

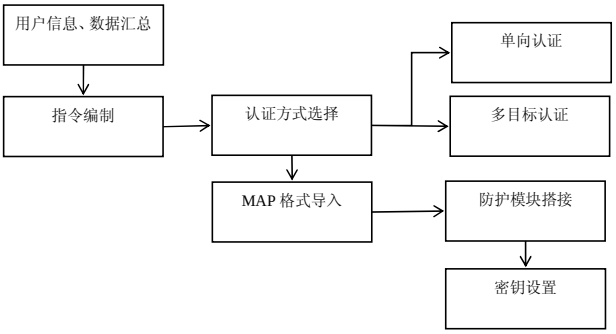

图 1　密钥防护模块应用环节示意图

结合图 1 来看，完成密钥防护模块应用设定后，便可以增设数据分类层级，调整密钥长度，此时需要参考下表 2 各项基础参数进行思考。

表 2　密钥基础指标参数预设表

测定指标	一级密钥	二级密钥
状态变量	+10.73	+11.72
密钥长度	452bit	581bit
合并比率	89	94
密钥精度	1.4	2.64

结合表 2 来看，完成密钥基础指标参数预设后，便可以确定密钥长度，进而营造动态的密钥空间，此条件下，测试环境搭设完成，通过调试确定无误后便可以进行测试。

3.2 测试结果分析

测试环境搭设完成后，正式进行检测。测试流程如下：将选定的 100 名测试用户隐私数据作为研究基础，规范导入平台数据库之中，按照预设模拟指令，营造测试环境。在测试过程中，为了保证测试结果具备参考意义，按照如下公式计算安全系数[7]。

$$H = 0.5u_1 - \left(\frac{ku_1 \cdot a^3}{f^2 \cdot af} + (u_1 - u_2) \right)$$

上述公式中：H 代表安全系数；u_1 代表加密差值；u_2 代表极限加密差值；k 代表导入距离；a 代表混沌系数；f 代表数据集。

最终得出如下表 3 所示的结果。

表 3　测试结果总结表

用户组	传统蜜罐数据加密方法安全系数	传统大数据加密方法安全系数	文章提出的 New SQL 数据库技术加密方法安全系数
10 人	1.02	1.22	1.42
20 人	1.21	1.13	1.54
30 人	1.28	1.37	1.59
40 人	1.17	1.26	1.49

结合表 3 来看，文章提出的方法安全系数处于最高水平。基于此，可以证明相较传统的蜜罐数据加密方法和大数据加密方法，应用 New SQL 数据库技术对用户隐私数据进行保护更具有优势。

结语

综上所述，文章研究了 New SQL 数据库技术在用户隐私数据安全保护中的应用。New SQL 通过引入先进的加密、身份验证和权限管理机制，为用户隐私数据提供了更全面、可控的安全保护。为了验证提出方法的安全性和实用性，通过搭建测试环境，以传统的蜜罐数据加密方法、大数据加密方法作为对照组，通过对 100 名用户身份信息和隐私数据进行加密测试，最终结果证明，科学应用 New SQL 数据库技术可以显著提升用户隐私数据安全加密效果。

参考文献：

[1]季焕淑.试谈 SQL 数据库优化技术在信息管理系统中的应用[J].电脑编程技巧与维护,2022，29(11):82-85.

[2]邵麒,李亚鹏,佟文朋.基于分布式系统设计中 NewSQL 数据库技术分析[J].电子制作,2021,29(24):66-67+46.

[3]奚军庆,李绍俊,李波.分布式系统设计中 NewSQL 数据库技术的应用[J].长江信息通信,2021,34(5):64-67.

[4]郝小凤.基于 C/S 架构的 SQL 数据库技术研究[J].电脑编程技巧与维护,2021，28(2):104-106.

[5]方阿丽.My SQL 数据库技术课程中创新能力培养的教学研究[J].电脑知识与技术,2020,16(27):28-29+42.

[6]张皓.SQL 数据库优化技术在计算机信息管理系统中的应用研究[J].电子元器件与信息技术,2020,4(5):36-37.

[7]黄卓洲.浅谈 SQL 数据库优化技术在信息管理系统中的应用[J].中国新通信,2020,22(2):104.