FCS 文章精要：基于先加密后索引方法的云中加密数据高效安全k近邻查询方案

作者：writer 来源：科学网

本文原地址：https://www.iikx.com/news/progress/26030.html

FCS
文章精要：基于先加密后索引方法的云中加密数据高效安全k近邻查询方案。论文标题：Indexing dynamic encrypted database in cloud for efficient secure k-nearest neighbor query（云中的FPGA共享：综合分析）

期刊：Frontiers of Computer Science

作者：Xingxin LI, Youwen ZHU, Rui XU, Jian WANG, Yushu ZHANG

发表时间：15 Feb 2024

DOI：10.1007/s11704-022-2401-1

微信链接：点击此处阅读微信文章

导读

安全k近邻查询(k-NN)旨在不泄漏隐私信息给云服务器的同时从云服务器存储的加密数据集中发现k个距离查询最近的数据条目，在许多领域都有着广泛的应用，例如：隐私保护机器学习和安全生物特征识别。研究者已经提出了许多方案来解决这一挑战性问题。然而现有方案在效率和灵活性方面仍然存在着各种局限性。本文提出了面向安全 k-近邻查询的先加密后索引方法，在云服务器端对加密数据进行转换并构建高维空间索引比如：R树，实现了具有亚线性查询复杂度并且支持加密数据动态更新的安全k-近邻查询机制。这是目前第一个同时实现上述两个性质的安全k-近邻查询方案。通过理论分析和模拟实验，本文分别证明了提出方案的安全性和高效性。

文章精要

Indexing Dynamic Encrypted Database in Cloud for Efficient Secure k-Nearest Neighbor Query

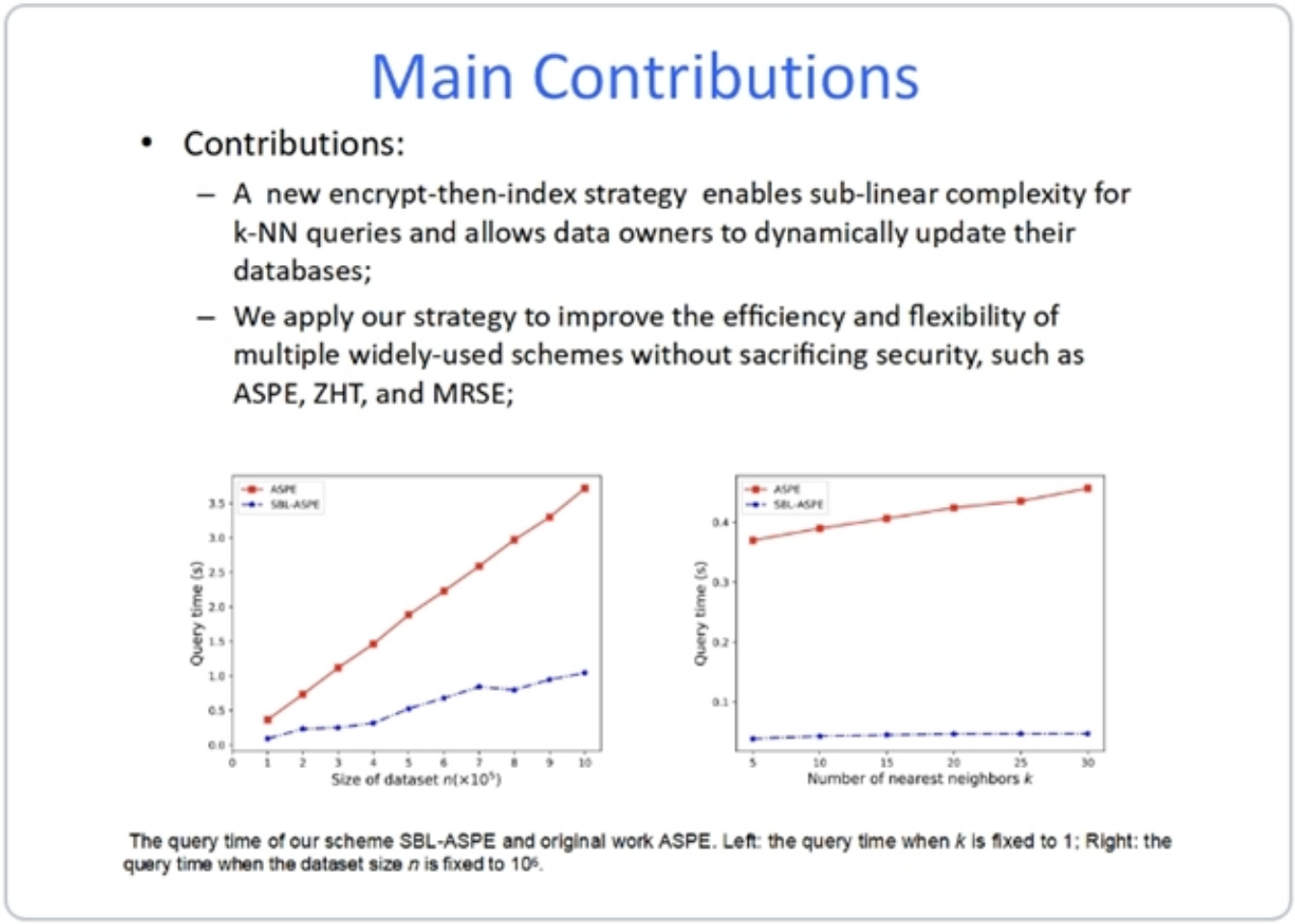
Xingxin LI, Youwen ZHU (✉), Rui XU, Jian WANG, Yushu ZHANG

Frontiers of Computer Science, 2024, 18(1): 181803
DOI:10.1007/s11704-022-2401-1

Problems & Ideas

- Problems of secure k-Nearest Neighbor (kNN)Query:
  - Most secure kNN query schemes have linear search complexity regarding to dataset sizes.
  - Existing index strategy for secure kNN query cannot support dynamic update over encrypted datasets.
- Ideas: A new encrypt-then-index strategy that transforms encrypted databases and then builds index on the transformed data.

Figure shows the main algorithms of our kNN query scheme which simultaneously achieves sub-linear complexity for kNN queries and allows data owners to dynamically update their databases. The correctness can be guaranteed because $dis(p_i, q) \leq dis(p_j, q) \Leftrightarrow dis(p_i^*, q^*) \leq dis(p_j^*, q^*)$.



相关内容推荐：

文章精要 SEOT：安全的动态可搜索加密所有权转移 2023 17(5): 175812

文章精要 DPPS：用于增强连续位置查询隐私的双重隐私保护方案 2023 17(5): 175814

文章精要 基于动态滑动窗口的差分隐私直方图发布方法 2023 17(4): 174809

文章精要 通用可调Even-Mansour密码及其应用 2023 17(4): 174807

文章精要 衡阳师范学院李浪教授团队：DBST: 一种基于动态S盒的轻量级分组密码 2023 17(3): 173805

文章精要 VenomAttack: Android系统中自动化和自适应的活动劫持攻击 2023 17(1): 171801

NTRU问题的困难性 2022 16(6): 166822

一种基于云模型的LDoS攻击检测方法 2022 16(6): 166821

本地化差分隐私技术下主要项值识别的有效方法 2022 16(5): 165825

Frontiers of Computer Science

Frontiers of Computer Science
（FCS）是由教育部主管、高等教育出版社和北京航空航天大学共同主办、SpringerNature
公司海外发行的英文学术期刊。本刊于 2007 年创刊，双月刊，全球发行。主要刊登计算机科学领域具有创新性的综述论文、研究论文等。本刊主编为周志华教授，共同主编为熊璋教授。编委会及青年 AE 团队由国内外知名学者及优秀青年学者组成。本刊被
SCI、Ei、DBLP、INSPEC、SCOPUS 和中国科学引文数据库（CSCD）核心库等收录，为 CCF 推荐期刊；两次入选中国科技期刊国际影响力提升计划；入选第4届中国国际化精品科技期刊；入选中国科技期刊卓越行动计划项目。

《前沿》系列英文学术期刊

由教育部主管、高等教育出版社主办的《前沿》（Frontiers）系列英文学术期刊，于2006年正式创刊，以网络版和印刷版向全球发行。系列期刊包括基础科学、生命科学、工程技术和人文社会科学四个主题，是我国覆盖学科最广泛的英文学术期刊群，其中12种被SCI收录，其他也被AHCI、Ei、MEDLINE或相应学科国际权威检索系统收录，具有一定的国际学术影响力。系列期刊采用在线优先出版方式，保证文章以最快速度发表。

中国学术前沿期刊网

http://journal.hep.com.cn

来源：Frontiers of Computer Science

更多 科学进展 请访问 https://www.iikx.com/news/progress/