**隐私保护计算相关技术深入理解与启发**

邵华松 D21091100252 2022.5.16

**摘要:** 隐私保护计算在近年来被提出，主要指在保护隐私信息的前提下，对数据价值的分析与挖掘，其作为一套完整的技术体系，是数据在公共网络上实现安全的分布式计算与共享的有利支撑。最近，相关技术的发展使得传统隐私保护计算技术体系在面对欺诈攻击、串通攻击及推理攻击时无法有效的保护数据的“可用不可见性”。

讲座对多种数据保护技术的安全级别分类，并以差分隐私技术为重点，介绍了其在对抗推理攻击时的可行性与有效性，在此基础上以实例展现了差分隐私技术在数据共享安全性保护方向的实力，并进一步说明差分隐私技术在一些统计与组合优化问题的隐私保护解决方案的应用前景。

**介绍**

随着信息时代的发展，网络技术及相关硬件设施已经与当今人类社会深度融合。然而，网络在给社会带来便利的同时存在着被攻击的风险。网络攻击主要可分为以下三个方向：隐私窃取、软件无效化、硬件损害，即针对数据、软件、硬件的攻击。而隐私窃取攻击又可以分为三种类型：欺诈攻击、串通攻击、推理攻击，其中欺诈攻击与串通攻击可归类于推理攻击中的主动推理攻击。讲座重点阐述如何防御隐私窃取方向的推理攻击。

推理攻击存在被动推理攻击与主动推理攻击两种形式。两种攻击形式的区别主要在于数据获取手段的合规性，进一步解释即被动推理攻击所用数据均为公开共有数据，而主动推理攻击所用数据还有以不合规手段获取的非公开隐私数据。

被动推理攻击指攻击者在遵循相关协议的情况下，根据公开共有数据进行计算，推理出数据所包含的隐私，从而形成有效攻击。最典型的被动推理攻击即联动攻击：攻击者根据公开数据与不完全脱敏数据的交集，还原出原始隐私数据，形成有效攻击。

主动推理攻击指攻击者以各种手段获取数据，并据此进行计算，推理出数据所包含的隐私，从而形成有效攻击。主动推理攻击是串通攻击与欺诈攻击的集合，典型的串通攻击即K均值攻击：攻击者向信息获取系统 (如推荐系统) 中输入K数量的数据，根据系统的K数量的输出的均值对目标隐私数据进行推理，形成有效攻击。欺诈攻击则通过输入大量虚假信息来影响输出，使数据失真，形成攻击。

讲座从六个大部分对隐私保护计算本身、相关问题及相关研究贡献进行了系统性的介绍，在现有隐私保护技术的基础上对相关问题进行了深入研究，并就差分隐私技术在相关领域的应用进行了研究推进，佐以实例，论证了该技术在隐私保护计算领域内的高度可行性与高度有效性。

**研究问题**

隐私保护计算在近年来被提出，主要指在保护隐私信息的前提下，对数据价值的分析与挖掘，其作为一套完整的技术体系，是数据在公共网络上实现安全的分布式计算与共享的有利支撑。

要实现隐私保护计算，关键在于怎样保证云端数据的高度隐私性与高度性。同时云端数据的云端又分为公有云与私有云，相较于私有云，基于公有云的应用更需要重点防范推理攻击。

**研究理解**

随着隐私保护计算的发展，网络攻击手段也在不断变化改进，这对隐私保护计算的安全性提出了更高的要求，具体表现为对环境虚拟化、非对称数据保护方法云上安全数据交换通道、大数据脱敏等技术的要求。

差分隐私技术作为隐私保护计算领域内的重要数据保护手段，其目标在于限制输出数据的敏感性，即限制在结合假想最大先验知识下结合对输出数据的可分析性，其中心思想在于在计算中添加噪音以改变输出数据分布来防止基于输出数据的推理攻击。尽管差分隐私技术在理论上能够有效保护数据的安全性，但在实际应用中，该技术需要在效用与隐私性做出取舍。

在面对被动推理攻击时，不应偏向效用或隐私性任一边，对数据采取回环检测与同态加密即可保证数据的安全性；在面对主动推理攻击时，应更偏向隐私性，对数据采取额外的匿名化处理、几何变换和数据提炼才能更好的保证数据的安全性。

在发布经加密的敏感数据时，讲座提出通过构建布尔回环进行多阶段联合计算来实现回环检测；并允许对加密文本进行直接计算来实现同态加密。在平衡效用与隐私保证数据的安全性。

在发布包含噪音的敏感数据时，讲座提出在尽量少做修改的情况下对集合中的元素进行匿名化实现数据匿名化；向输入数据中添加随机噪声实现输入随机化；保留距离的情况下对数据向量进行旋转实现几何变换；通过最小化样本本征向量实现对数据的凝结。在更偏向隐私的思想下保证数据的安全性。

在发布不敏感数据时，讲座提出向输出数据中添加随机噪音，并最小化计算正输入与负输入的输出间的敏感性实现对输出数据的安全保护。

**研究理解**

讲座针对隐私保护计算领域快速发展所带来的数据安全问题，提出并实现了基于差分隐私技术的数据保护手段，采用了对比分析与实验论证的方法，从不同的角度证明了差分隐私技术在隐私保护计算领域的可行性与有效性，并就隐私保护计算的不同应用场景提出了适应数据敏感度的多强度安全保护以平衡隐私性与效用。

讲座通过大量使用“总结工作-提出问题-解决问题的”的论述模式与研究方法，逻辑清晰地阐述了差分隐私技术在隐私保护计算领域的应用潜力；同时与传统方法进行对比，凸显出差分隐私技术的优势。有理有据，令人信服。

**结论**

关于理论研究与实验实现的关系。理论研究应先于实验实现，而理论研究的前期应重点关注现有相关工作搜集与探讨，在此基础上结合新思想、新技术进行创新性研究，避免陷入闭门造车的情况。

关于实验方法。实验方法应紧紧围绕实验创新点进行展开，对比实验先行，进一步探究实验，在确保新方法相比其他方法具备足够的优越性后，再在此基础上继续实验探究方法的更深层次的发展可能性。

关于文章写作。文章写作应在具备足够的知识储备、足够的相关领域前沿论文储备与足够的实验结果支撑的条件下进行。首先需要确定的是文章结构，文章结构应清晰明了使读者能够了解作者整体写作方向；其次是文章内容，文章内容方面应注重遣词造句的易读性与图表的简洁性，即文章为内容服务。

**参考文献**

Zhigang Lu and Hong Shen, Differentially Private k-Means Clustering with Convergence Guarantee, IEEE Transactions on Dependable and Secure Computing8(4): 1541-1552 (2021)

Songyuan Li , Hong Shen, Yingpeng Sang, Hui Tian: An efficient method for privacy-preserving trajectory data publishing based on data partitioning. J. Supercomput. 76(7): 5276-5300 (2020)

Hui Tian, Jingtian Liu, Hong Shen, ?Diffusion Wavelet-based Privacy Preserving in social networks?, Computers & Electrical Engineering, 67: 415-424, 2018

Ruoxuan Wei, Hui Tian, Hong Shen: Improving k-anonymity based privacy preservation for collaborative filtering, Computer & Electrical Engineering, 67: 509-519, 2018

Zhigang Lu and Hong Shen, Secured Privacy-preserving Data Aggregation with Semi-honest Servers, PAKDD-2017

Zhigang Lu and Hong Shen, A New Lower Bound of Privacy Budget for Distributed Differential Privacy, PDCAT-2017

Yingpeng Sang, Hong Shen, Hui Tian, Zonghua Zhang: Achieving Probabilistic Anonymity in a Linear and Hybrid Randomization Model, IEEE Trans. Info. Forensics & Security, 11(10): 2187-2202, 2016

Zhigang Lu and Hong Shen, A Security-assured Accuracy-maximised Privacy Preserving Collaborative Filtering Recommendation Algorithm, 19th International Database Engineering & Applications Symposium, IDEAS’15, Yokohama, Japan, 2015. ACM

Zhigang Lu and Hong Shen, An Accuracy-Assured Privacy-Preserving Recommender System for Internet Commerce, ComSIS 2015

Yidong Li and Hong Shen. On Identity Disclosure Control for Hypergraph based Data Publishing, IEEE Trans. Info. Forensics & Security, 8(8): 1384-1396, 2013

Yingpeng Sang, Hong Shen, Hui Tian: Effective Reconstruction of Data Perturbed by Random Projections. IEEE Trans. Computers 61(1): 101-117 (2012)

Yingpeng Sang, Hong Shen, Hui Tian: Privacy-Preserving Tuple Matching in Distributed Databases. IEEE Trans. Knowl. Data Eng. 21(12): 1767-1782 (2009)

Yingpeng Sang, Hong Shen: Efficient and secure protocols for privacy-Preserving set operations. ACM Trans. Inf. Syst. Secur. 13(1): (2009)