A study on Adaptive and Robust Privacy-Enhancing Technologies for Spatio-Temporal Data Aggregation

氏　　名　笹田　大翔

研 究 室 名　サイバーレジリエンス構成学研究室

主指導教員名　門林　雄基

内 容 梗 概

Spatio-temporal data is utilized for various purposes such as epidemiology, natural disaster management, urban planning, and more. However, there is a risk of individuals' residential locations or workplaces, from the accumulated data on datastore. Data collection based on Local Differential Privacy LDP is a promising approach to protect sensitive information. By modifying (e.g. adding noise to data) each data point in a way that the adversary cannot distinguish it from others, privacy can be preserved. However, we argue that there are three fundamental defects in LDP for utilizing spatio-temporal data. In LDP, we should determine the strength of privacy protection based on the distribution of the entire dataset, but spatio-temporal data are distributed differently at different places and times, and the characteristics of the data change over time. Moreover, if we combine LDP-data with data from different domains, the cartesian product provides incorrect analysis results. Furthermore, LDP cannot indicate whether the distortion is due to noise or to an attack. Client have diverse privacy preferences for their own data, making it difficult to utilize LDP, which requires uniform protection strength. Current research assumes identical data volume and privacy preferences, and different volumes of data and protection strength cannot be set. To tackle these problems, we propose three approaches. First, we design novel privacy model which assigns protection strength to similar client groups, maintains correlations, and controls protection strength dynamically. Second, we collect statistical features exclusively by combining LDP with the Oblivious Transfer (OT) protocol, addressing perturbation and data volume issues. Third, we combine LDP with homomorphic encryption for secure analysis across organizations while keeping data encrypted. we achieve adaptive and robust privacy-enhancing technologies for spatio-temporal data aggregation through these approaches.

業績リスト

氏　　名

査読付学術論文（著者[本人の氏名に下線]，題目，掲載雑誌名，巻，号，ページ，年月，博士論文対応箇所）

１．Taisho Sasada, Yuzo Taenaka, Youki Kadobayashi.“Oblivious Statistic Collection With Local Differential Privacy in Mutual Distrust”, IEEE Access, vol.11, 2023, pp.21374—21386.

査読付国際会議発表（著者[本人に下線]，題目，掲載論文集名または会議名，（あれば巻,号,ページ），年月，博士論文対応箇所）

１．Masashi Yoshimura, Taisho Sasada, Yuzo Taenaka,Youki Kadobayashi.“Enabling Memory Efficient Encrypted Database Utilizing Secure_Unsecured Area of Intel SGX”,The Proceedings of 15th International Conference on Advances in Databases, Knowledge, and Data Applications (In press)

２．Taisho Sasada, Yuzo Taenaka, Youki Kadobayashi.“DPSD: Dynamic Private Spatial Decomposition Based on Spatial and Temporal Correlations”, The 7th International Conference on Smart Computing and Communication, vol. 13828, pp.188—202.

３．Taisho Sasada, Yuzo Taenaka, Youki Kadobayashi.“Decoupling Statistical Trends from Data Volume on LDP-Based Spatio-Temporal Data Collection”, 2022 IEEE Future Networks World Forum, 2022, pp.262—269.

４．Taisho Sasada, Yuto Masuda, Yuzo Taenaka, Youki Kadobayashi, Doudou Fall.“Zero-Trust Access Control Focusing on Imbalanced Distribution in Browser Clickstreams“, In Proceedings of the 8th International Conference on Software Defined Systems, 2021,pp.1--8.

５．Taisho Sasada, Masataka Kawai, Doudou Fall, Yuzo Taenaka, Youki Kadobayashi, “Differentially-Private Text Generation via Text Preprocessing to Reduce Utility Loss”, In Proceedings of the 3rd International Conference on Artificial Intelligence in Information and Communication, 2021, pp.042—047.

６．Taisho Sasada, Yuzo Taenaka, Youki Kadobayashi, “Anonymizing Location Information in Unstructured Text Using Knowledge Graph”, In Proceedings of the 22nd International Conference on Information Integration and Web-based Applications & Services, 2020,pp.163—pp.167.

７．Taisho Sasada, Zhaoyu Liu, Tokiya Baba, Kenji Hatano, Yusuke Kimura.“A resampling method for imbalanced datasets considering noise and overlap”, 24th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, 2020,pp.420—pp.429

他　国内研究会１３件