IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

IJARSCT
Impact Factor: 6.252

Volume 2, Issue 6, June 2022

Privacy Preservation of Location Data Publishing

Dr. M. L. Valarmathi[1], C. Devipriya[2], Saranya P[3], Banumathi S[4], Nathira Begum S[5]

Professor, Department of Computer Science and Engineering1

Assistant Professor, Department of Computer Science and Engineering2

UG Scholar, Department of Computer Science and Engineering3,4,5

Dr. Mahalingam College of Engineering and Technology, Pollachi, Tamil Nadu, India

Abstract: *Machine learning is important for future development and access for large detailed datasets. The privacy preserving machine learning enables maintaining of the data privacy and confidentiality. Machine learning enables new services in using sensitive data. This paper uses location trajectories and the application of this framework is the privacy preservation of location based data. Researchers had verified that publishing trajectories data would cause risk of user's privacy and also capable of identifying their locations, personal details and so on. Therefore, we have applied anonymization techniques and developed the data to preserve the privacy for the users. We propose a framework for Spatiotemporal datasets termed ML based anonymization (MLA). We use machine learning algorithms for clustering the dataset. To propose the trajectories we use k-means algorithm. The k-means is a type of clustering algorithm used in many real time applications, especially for analysis of data. Moreover, we improve alignment method for progressive sequence alignment of MLA. In this paper, we generate signature key for the public user and generate a digital signature for public users. Signature generation method use elliptic curve cryptography (ECC) algorithm. As a result on Spatiotemporal trajectory datasets indicate a high utility performance of ouranonymization based on MLA framework.*

Keywords: Machine learning, Location trajectories, Spatiotemporal dataset, k-means algorithm, Signature generation, Elliptic curve cryptography

REFERENCES

[1]. R. Agrawal, A. Evfimievski, and R. Srikant. Information sharing across private databases. In Proceedings of the ACM International Conference on Management of Data, 2003.

[2]. B. Barak, K. Chaudhuri, C. Dwork, S. Kale, F. McSherry, and K. Talwar. Privacy,accuracy, and consistency too: A holistic solutiontocontingencytablerelease. In Proceedingsofthe ACM Symposium on Principles of Database Systems (PODS),2007.

[3]. R. J. Bayardo and R. Agrawal. Data privacy through optimal k-anonymization. In Proceedings of the IEEE International Conference on Data Engineering (ICDE), 2005.

[4]. R.Bhaskar,S.Laxman,A.Smith,andA.Thakurta. Discovering frequent patterns in sensitive data. In Proceedings of the ACM International Conference on Knowledge Discovery and Data Mining (SIGKDD), 2010.

[5]. Blum, K. Ligett, and A. Roth. A learning theory approach to non-interactivedatabase privacy. In Proceedings of the ACM Symposium on Theory of Computing(STOC), 2008.

[6]. J. Brickell and V. Shmatikov. Privacy- preserving classifier learning. In Proceedings of the International Conference on Financial Cryptography andData Security, 2009.

[7]. P. Bunn and R. Ostrovsky. Secure two-party k-means clustering. In Proceedings ofthe ACM Conference on Computer and Communications Security (CCS), 2007.

[8]. K. Chaudhuri, C. Monteleoni, and A. Sarwate. Differentially private empirical risk minimization. Journal of Machine Learning Research (JMLR), 12:1069–1109, July 2011.

[9]. K. Chaudhuri, A. D. Sarwate, and K. Sinha. Near-optimal differentially private principal components. In Proceedings ofthe Conference on Neural Information Processing Systems, 2012.

[10]. C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu. Tools for privacy preserving distributed data mining. ACM InternationalConferenceonKnowledgeDiscoveryandDataMining (SIGKDD) Explorations Newsletter, 4(2):28–34, December 2002.

[11]. Dinur and K. Nissim. Revealing information while preserving privacy. In Proceedings of the ACM Symposium on Principles of Database Systems (PODS),2003.

[12]. C. Dwork. A firm foundation for private data analysis. Communications of the ACM, 54(1):86–95, 2011.

[13]. C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor. Our data, ourselves: Privacy via distributed noise generation. In Proceedings of the 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2006.

[14]. C. Dwork, F. McSherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In Proceedings of the Theory of CryptographyConference (TCC), 2006.

[15]. Frank and A. Asuncion. UCI machine learning repository, 2010.

[16]. Friedman and A. Schuster. Data mining with differential privacy. In Proceedings of the ACM International Conference on Knowledge Discovery and Data Mining (SIGKDD), 2010.

[17]. B. C. M. Fung, K. Wang, R. Chen, and P.S.Yu. Privacypreserving data publishing: A survey of recent developments. ACMComputing Surveys, 42(4):1–53, June 2010.

[18]. B. C. M. Fung, K. Wang, and P. S. Yu. Anonymizing classification data for privacy preservation. IEEE Transaction on Knowledge and Data Engineering (TKDE),19(5):711–725, May 2007.

[19]. S. R. Ganta, S. Kasiviswanathan, and A. Smith. Composition attacks and auxiliary information in data privacy. In Proceedings of the ACM International Conference on Knowledge Discovery and Data Mining (SIGKDD), 2008 Learning Research (JMLR), 12:1069–1109, July 2011.