BÖLÜM 3

KONUM TABANLI SERVİSLERDE MAHREMİYET

Şeyda DANYILDIZI[1]
Yavuz CANBAY[2]

GİRİŞ

Kablosuz iletişimin, mobil cihazların ve konumlandırma teknolojilerinin yaygınlaşmasıyla, konum tabanlı servisler son yıllarda çok yönlü ve kaynak açısından zengin hale gelmiştir (1). Mekân-zamansal verilerin toplanması, hizmet kalitelerini ve uygulama etkinliklerini artırmayı sağladığından konum hizmeti sağlayıcıları için oldukça faydalıdır. Akıllı telefonlar, tabletler ve akıllı giyilebilir cihazlar gibi çok sayıda internet bağlantılı mobil cihazlar sürekli konum verileri üretir (2-4). Ancak, bu veriler yapılan faaliyetler hakkında hassas bilgiler içerdiğinden, böylesi verilerin toplanması ve işlenmesi potansiyel olarak kullanıcılar hakkında kişisel bilgileri servis sağlayıcılara ya da üçüncü taraflara sızdırabilir.

Kullanıcıların kesin konumunun belirlenmesi ve izlenmesi, kullanıcıların mahremiyetini tehdit eder. Bu veriler, kullanıcıların sosyal alışkanlıklarını, günlük rutinlerini, dini düşüncelerini, işyerlerini, seyahat bilgilerini ve sağlık bilgilerini ortaya çıkarabilir. Kullanıcıların konum verilerinin ifşa edilmesi yalnızca kullanıcıların mahremiyet endişelerini artırmakla kalmaz, aynı zamanda birçok ülkede mevcut olan mevzuatlara da aykırıdır (2).

Özel hayatın gizliliği hakkı anayasa ile güvence altında iken Kişisel Verilerin Korunması Kanunu (KVKK) ile de veri mahremiyeti hakkının korunması gerektiği pekiştirilmiştir. Bu doğrultuda KVKK'nın hayatımıza girmesiyle beraber veri sorumluları, farklı çözümler ile değişen dünyaya ayak uydurmaya çalışmaktadırlar. Özellikle konum tabanlı uygulamaları kullanarak gerek hayatımızı kolaylaştıran gerekse analiz işlemi yaparak veri işleyen tarafların bu alanda yükümlülükleri bulunmaktadır. Bundan dolayı veri sorumlularının, verileri yayınlarken mahremiyet koruyucu önlemleri almaları gerekir.

[1] Kahramanmaraş Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Enformatik AD., seyda.danyildizi@istiklal.edu.tr

[2] Dr. Öğr. Üyesi Kahramanmaraş Sütçü İmam Üniversitesi, Mühendislik-Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, yavuzcanbay@ksu.edu.tr

lanmasından ve çeşitli eksikliklerinin olmasından dolayı diferansiyel mahremiyetin istenilen ihtiyaçları daha doğru karşılaması güvenilir bir model olmasını sağlamaktadır. Mahremiyeti sağlarken veri faydasına önem veren bir yöntemdir. Bu kapsamda son yıllarda, mahremiyetin sağlanmasında kademeli olarak diferansiyel mahremiyet yöntemi uygulanmaktadır.

Diferansiyel mahremiyet, verilerin yayınlanmasında ve analiz edilmesinde diğer koruma modellerine kıyasla fayda-mahremiyet açısından daha iyi bir performans sağlamaktadır. k-anonimlik, l-çeşitlilik ve t-yakınlık gibi modellerin arka plan bilgisi saldırılarında yetersiz olması diferansiyel mahremiyetin geliştirilmesi sürecini hızlandırmıştır. Diferansiyel mahremiyet mekanizmasının kullanıldığı yerlerde gerçek veri kümesi değerleri yerine gürültü eklenilen veri tabanlarının cevaplarına ulaşılabilmektedir. Bu da diferansiyel mahremiyete duyulan güveni destekler niteliktedir.

Bu kapsamda yapılan çalışmanın bir sonucu olarak, konum tabanlı servislerde veri mahremiyetini sağlama açısından genellikle diferansiyel mahremiyet yaklaşımından faydalanıldığı, fayda-mahremiyet dengesinin sağlandığı görülmüştür.

KAYNAKLAR

1. N. Nisha, I. Natgunanathan, S. Gao, and Y. Xiang, A novel privacy protection scheme for location-based services using collaborative caching, *Computer Networks,* 213, 2022.
2. H. Navidan, V. Moghtadaiee, N. Nazaran, and M. Alishahi, Hide me behind the noise: local differential privacy for indoor location privacy, in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Genoa, Italy, 2022.
3. M. Douriez, H. Doraiswamy, J. Freire, and C. T. Silva, Anonymizing nyc taxi data: Does it matter?, in *2016 IEEE international conference on data science and advanced analytics (DSAA)*, Montreal, QC, Canada, 2016.
4. A. T. Hasan, Q. Jiang, C. Li, and L. Chen, An effective model for anonymizing personal location trajectory, in *Proceedings of the 6th International Conference on Communication and Network Security*, 39-35, 2016.
5. X. Kong *et al.*, Big trajectory data: A survey of applications and services, *IEEE Access,* 6, 58306-58295, 2018.
6. R. Talat, M. S. Obaidat, M. Muzammal, A. H. Sodhro, Z. Luo, and S. Pirbhulal, A decentralised approach to privacy preserving trajectory mining, *Future Generation Computer Systems,* 102, 392-382, 2020.
7. P. Canbay and H. Sever, The Effect of clustering on data privacy, in *2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA)*, Miami, FL, USA, 2015.
8. K. Gu, L. Yang, Y. Liu, and N. Liao, Trajectory data privacy protection based on differential privacy mechanism, in *IOP Conference Series: Materials Science and Engineering*, 351(1), 17-12, 2018.
9. R. Wazirali, A Review on Privacy Preservation of Location-Based Services in Internet of Things, *Intelligent Automation Soft Computing,* 31(2), 779-767, 2022.
10. A. Aloui, O. Kazar, S. Bourekkache, and A. Chikh, Protecting user privacy in location-based services over road networks, *Journal of Location Based Services,* 16(2), 118-77, 2022.

11. Kişisel Verileri Koruma Kurumu, 100 Soruda Kişisel Verilerin Korunması Kanunu, *ISBN : 978-975-19-6883-8, KVKK Yayınları,* 86, 2018.
12. Ş. Akkaya, Derin Öğrenme Yöntemi İle Diferansiyel Mahremiyetli Medikal Görüntü Sınıflandırma *Yüksek Lisans Tezi,* 77-1, 2021.
13. Y. Vural, Veri Mahremiyeti: Saldırılar, Korunma Ve Yeni Bir Çözüm Önerisi, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* 4(2), 34-21, 2018.
14. C. Mauger, G. Le Mahec, and G. Dequen, Modeling and evaluation of k-anonymization metrics, in *PrivacyPreserving Artificial Intelligence Workshop of AAAI*, 2020.
15. K. Zickuhr, Location-based services, *Pew Research,* 679-695, 2013.
16. X. Yin, Y. Zhu, and J. Hu, A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions, *ACM Computing Surveys,* 54(6), 36-1, 2021.
17. Z. Xu, J. Zhang, P.-w. Tsai, L. Lin, and C. Zhuo, Spatiotemporal mobility based trajectory privacy-preserving algorithm in location-based services, *Sensors,* 21(6), 21-20, 2021.
18. X. Zhao, D. Pi, and J. Chen, Novel trajectory privacy-preserving method based on clustering using differential privacy, *Expert Systems with Applications,* 149, 2020.
19. Kişisel Verileri Koruma Kurumu, *Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi*, Erişim tarihi: 23.09.2022, Web adresi: https://www.kvkk.gov.tr/.
20. A. İnan and E. Var, Sınıflandırma için diferansiyel mahremiyete dayalı öznitelik seçimi, *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi,* 33(1), 336-323, 2018.
21. P. Samarati and L. Sweeney, Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression, 1998.
22. S. Chang, C. Li, H. Zhu, T. Lu, and Q. Li, Revealing privacy vulnerabilities of anonymous trajectories, *IEEE Transactions on Vehicular Technology,* 67(12), 12071-12061, 2018.
23. S. Shaham, M. Ding, B. Liu, Z. Lin, and J. Li, Machine learning aided anonymization of spatiotemporal trajectory datasets, in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Paris, France, 2019.
24. J. Liu and S. Wang, All-dummy k-anonymous privacy protection algorithm based on location offset, *Computing,* 13-1, 2022.
25. T. Peng, Q. Liu, D. Meng, and G. Wang, Collaborative trajectory privacy preserving scheme in location-based services, *Information Sciences,* 387, 179-165, 2017.
26. O. Abul, F. Bonchi, and M. Nanni, Never walk alone: Uncertainty for anonymity in moving objects databases, in *2008 IEEE 24th international conference on data engineering*, Cancun, Mexico, 2008.
27. N. Rajesh, S. Abraham, and S. S. Das, Trajectory Anonymization Through Generalization of Significant Location Points, International Journal of Computer Sciences Engineering, 6(6), 62-58 2018.
28. C. Dwork, Differential privacy: A survey of results, in *International conference on theory and applications of models of computation*, 19-1, 2008.
29. X. Zhao, Y. Dong, and D. Pi, Novel trajectory data publishing method under differential privacy, *Expert Systems with Applications,* 138, 112791 2019.
30. J. P. Near and C. Abuah, Programming Differential Privacy, *open-source book,* 108-1, 2021.
31. N. Fernandes, A. McIver, and C. Morgan, The Laplace Mechanism has optimal utility for differential privacy over continuous queries, in *2021 36th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, Rome, Italy, 2021.
32. W. Cheng, R. Wen, H. Huang, W. Miao, and C. Wang, OPTDP: Towards optimal personalized trajectory differential privacy for trajectory data publishing, *Neurocomputing,* 472, 211-201, 2022.
33. D. Su, J. Cao, N. Li, E. Bertino, and H. Jin, Differentially private k-means clustering, in *Proceedings of the sixth ACM conference on data and application security and privacy*, 37-26, 2016.
34. Q. Han, Z. Xiong, and K. Zhang, Research on trajectory data releasing method via differential privacy based on spatial partition, *Security Communication Networks,* 2018, 2018.

35. R. Chen, B. Fung, and B. C. Desai, Differentially private trajectory data publication, arXiv cs arXiv:1112.2020*,* 2011.
36. H. Li, Y. Guo, and X. Ren, An Efficient Location Privacy Protection Method for Location-Based Services based on Differential Privacy, *Research Square,* 26, 2022.
37. Y. Yan, Z. Sun, A. Mahmood, F. Xu, Z. Dong, and Q. Z. Sheng, Achieving Differential Privacy Publishing of Location-Based Statistical Data Using Grid Clustering, *ISPRS International Journal of Geo-Information,* 11(7), 404, 2022.
38. F. Tian, S. Zhang, L. Lu, H. Liu, and X. Gui, A novel personalized differential privacy mechanism for trajectory data publication, in *2017 International Conference on Networking and Network Applications (NaNA)*, Kathmandu, Nepal, 2017.
39. M. Akın, Y. Canbay, and Ş. Sağıroğlu, Yörünge Verisi Yayınlamada Mahremiyet Duyarlı Yeni Bir Model Önerisi ve Uygulaması, *Politeknik Dergisi*, 24(3), 1286-1275, 2021.
40. C. Bayrak, Konum tabanlı uygulamalarda konum ve konum örüntü mahremiyetinin sağlanması, TOBB ETÜ Fen Bilimleri Enstitüsü, 2016.
41. D. E. Seidl, P. Jankowski, and M.-H. Tsou, Privacy and spatial pattern preservation in masked GPS trajectory data, *International Journal of Geographical Information Science,* 30(4), 800-785, 2016.
42. S. B. Avaghade and S. S. Patil, Privacy preserving for spatio-temporal data publishing ensuring location diversity using K-anonymity technique, in *2015 International Conference on Computer, Communication and Control (IC4)*, Indore, India, 2015.
43. Z. Tu, K. Zhao, F. Xu, Y. Li, L. Su, and D. Jin, Protecting Trajectory From Semantic Attack Considering k-Anonymity, l-Diversity, and t-Closeness, *IEEE Transactions on Network Service Management,* 16(1), 278-264, 2018.
44. L. Yao, Z. Chen, H. Hu, G. Wu, and B. Wu, Sensitive attribute privacy preservation of trajectory data publishing based on l-diversity, *Distributed parallel databases,* 39(3), 811-785, 2021.