BÖLÜM 2

ÜRETKEN ÇEKİŞMELİ AĞLAR VE VERİ MAHREMİYETİ

Ali SAKMAK[1]
Yavuz CANBAY[2]

GİRİŞ

Günümüz sistemlerinde modern yapay zekâ teknolojilerinin kullanılmasına yönelik sürekli artan bir talep mevcuttur. Bu taleplerin çoğu, ilgili olduğu alana yönelik teknolojinin verimliliğini artırmak için kullanılabilecek doğru ve güçlü tahmine dayalı modeller oluşturmak esasına dayanır (1). Yapay zekâ sisteminin güçlü ve doğru tahminler yapabilmesi için yüksek oranda öğrenmesi gerekir. Öğrenmenin gerçekleşmesi doğru içerikli veri kümelerinin varlığıyla mümkün olmaktadır. Veri kümesinin doğru veriler içermesi, doğru etiketlenmesi ve içerdiği verinin miktarı, makine öğrenmesinin önemli unsurlarıdır.

Veri kümeleri, milyonlarca kayıt barındırabilmekle beraber bu verilerin toplanması ve etiketlenmesi işlemlerinin ilgili alan uzmanları tarafından yapılması şarttır. Gerçek verilere ulaşmakta etik, bürokratik ve operasyonel çeşitli zorluklar yaşanabilmektedir. Elektronik kişisel verilerin güvenliği ve kişisel veri mahremiyeti endişelerinden kaynaklanan veri paylaşım kısıtlamaları, yapay zekâ teknolojilerinin yeteri miktarda veri ile beslenmesinin önündeki en büyük engeldir (2). Bu problemin çözümü için veri mahremiyeti endişelerini gidererek daha az maliyetle daha hızlı şekilde orijinal veri kümelerindeki karmaşıklıkların (dağılımlar, doğrusal olmayan ilişkiler, gürültü vb.) çoğunu yakalayan, gerçek veriden herhangi bir ipucu içermeyen ve verinin tanımlanması riskinin en aza indirildiği yapay veri üretim yöntemi, makul bir çözüm olarak kabul edilmektedir (1).

Üretken çekişmeli ağ teknolojisi, kullanıcı mahremiyetinden ödün vermeden yapay veri üretmeyi sağlayan güncel bir teknolojidir. Bu çalışma da; üretken çekişmeli ağ teknolojileri açıklanmış, veri mahremiyeti ile ilişkisi irdelenmiş, bu tekno-

[1] Kahramanmaraş Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Bilişim Sistemleri AD., alisakmak@gmail.com

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

bu temel hak ve özgürlüklere yasal zemin oluşturan düzenlemelerdir. Bu düzenlemeler kapsamında, veri sahiplerinden bilgilendirilmiş onayı olmaksızın kişisel verilerin paylaşılması kullanılması yasal bir uygulama değildir. Giderek artan bir şekilde, veri mahremiyetiyle ilgili endişeleri önlemek için veri mahremiyeti sağlayan teknolojiler kullanarak veri mahremiyeti sorununu aşabilecek yaklaşımlara ihtiyaç duyulmaktadır.

Mahremiyet ve fayda arasındaki dengeyi sağlayabilmek amacıyla kullanılan yöntemlerden biride yapay veri üretmektir. Gerçek ile ayırt edilemeyecek kaliteli yapay veriler oluşturmak, veri mahremiyeti sorunu olmadan makine öğrenme modellerinin ihtiyacı olan verilere ulaşmanın bir yoludur.

Yapay veriler, gerçek olaylar tarafından üretilmek yerine yapay olarak oluşturulan veya simüle edilen verilerdir. Yapay veriler, orijinal veri setinin istatistiksel özelliklerini yansıtan gerçek veriler üzerinde modellenmiştir. Yapay veri oluşturmanın amacı, kurgusal ancak faydalı veri kümelerine daha hızlı erişim sağlamaktır. Yapay veriler, verilerin geniş çapta kullanımı ve paylaşımı için veri mahremiyetini koruyan bir mekanizma sağlar. Tanımlanabilir hiçbir bilgi içermeyen yapay bir veri kümesi oluşturduğu için hassas verilerin paylaşımı için güvenli bir yaklaşım olarak kabul edilir. Yapay verilerin popülaritesi, son yıllarda geliştirilen yapay veri üreteci modelleri ile gittikçe artmaktadır.

Bu çalışmada, yapay zekânın ihtiyacı olan verilere mahremiyet sorunu yaşamadan yapay veri üreterek çözüm sağlayan üretken çekişmeli ağ teknolojisi anlatılmış, üretken çekişmeli ağların algoritma, teori, uygulamaları, kullanım alanları ve literatürdeki çalışmaları irdelenmiştir.

Üretken çekişmeli ağlar, büyük miktarda etiketlenmemiş verilerden yararlanma yeteneği nedeniyle ilgi odağının arttığı bir çalışma alanıdır. Üretken çekişmeli ağ eğitiminin incelikleri içinde, teori ve algoritmalardaki gelişmeler için birçok fırsat vardır ve derin ağların gücü ile yeni uygulamalar için çok büyük potansiyel barındırır. Üretken çekişmeli ağların kişisel verilerin korunması ve yapay zekânın ihtiyacı olan verilerin üretilmesine önemli katkı sağlayacağı değerlendirilmektedir.

KAYNAKLAR

1. A. Tucker, Z. Wang, Y. Rotalinti, P. Myles, Generating high-fidelity synthetic patient data for assessing machine learning healthcare software, *Npj Digital Medicine,* 3(2), 147-157, 2020.
2. A. Deveci, M. F. Esen, Medikal Sentetik Veri Üretimiyle Veri Dengelemesi, *İstatistik ve Uygulamalı Bilimler Dergisi,* 1(5), 17-28, 2022.
3. H. Yılmaz, TS ISO/IEC 27001 Bilgi güvenliği yönetimi standardı kapsamında bilgi güvenliği yönetim sisteminin kurulması ve bilgi güvenliği risk analizi, *Denetişim,* 1(15), 45-59, 2014.

4. Y. Canbay, Ş. Sağıroğlu, Derin Öğrenmede Diferansiyel Mahremiyet, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* 6(1), 1-16, 2020.
5. P. Jain, M. Gyanchandani, N. Khare, Big data privacy: a technological perspective and review, *Journal of Big Data,* 3(1), 1-25, 2016.
6. Y. Canbay, Aykırı veri yönelimli fayda temelli büyük veri anonimleştirme modeli, Doktora, Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Ana Bilim Dalı, 2019.
7. P. Canbay, H. Sever, The Effect of clustering on data privacy, *2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA)*, Florida, USA, 2015.
8. E. Aktan, Büyük veri: Uygulama alanları, analitiği ve güvenlik boyutu, *Bilgi Yönetimi,* 1(1), 1-22, 2018.
9. Y. Vural, Veri mahremiyeti: Saldırılar, korunma ve yeni bir çözüm önerisi, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi,* 4(2), 21-34, 2018.
10. Ş. Sağıroğlu, Bölüm 5: Büyük veri güvenliği ve mahremiyeti, *Büyük veri analitiği, güvenliği ve mahremiyeti*, ISBN: 978-605-86904-4-8 , Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü Büyük Veri Analitiği Ve Güvenliği (Bidisec) Araştırma Gurubu, 32-37, 2016.
11. A. N. Akıncı, Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti, *T.C. Cumhurbaşkanliği strateji ve bütçe başkanliği,* 1(1), 1-20, 2019.
12. G. Yiğit, K. Ayşe, Derin Öğrenme Modellerinde Mahremiyet ve Güvenlik Üzerine Bir Derleme Çalışması, *Düzce Üniversitesi Bilim ve Teknoloji Dergisi,* 9(5), 1843-1859, 2021.
13. C. Dwork, Differential privacy: A survey of results, *International conference on theory and applications of models of computation*, Xi'an, China, 2008.
14. P. Kairouz *et al.*, Advances and open problems in federated learning, *Foundations and Trends® in Machine Learning,* 14(1,2), 1-210, 2021.
15. S. AbdulRahman, H. Tout, H. Ould-Slimane, A. Mourad, C. Talhi, M. Guizani, A survey on federated learning: The journey from centralized to distributed on-site learning and beyond, *IEEE Internet of Things Journal,* 8(7), 5476-5497, 2020.
16. Q. Yang, Y. Liu, Y. Cheng, Y. Kang, T. Chen, H. Yu, Federated learning, *Synthesis Lectures on Artificial Intelligence and Machine Learning,* 13(3), 1-207, 2019.
17. K. G. Hartmann, R. T. Schirrmeister, T. Ball, EEG-GAN: Generative adversarial networks for electroencephalograhic (EEG) brain signals, *arXiv preprint arXiv:1806.01875,* 2018.
18. I. Goodfellow *et al.*, Generative adversarial nets, *Advances in neural information processing systems,* 27(1), 2672-2680, 2014.
19. J. Gui, Z. Sun, Y. Wen, D. Tao, J. Ye, A review on generative adversarial networks: Algorithms, theory, and applications, *arXiv preprint arXiv:2001.06937,* 2020.
20. A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, A. A. Bharath, Generative adversarial networks: An overview, *IEEE Signal Processing Magazine,* 35(1), 53-65, 2018.
21. S.-W. Park, J.-S. Ko, J.-H. Huh, J.-C. Kim, Review on Generative Adversarial Networks: Focusing on Computer Vision and Its Applications, *Electronics,* 10(10), 1192-1216, 2021.
22. I. Goodfellow, Nips 2016 tutorial: Generative adversarial networks, *arXiv preprint arXiv:1701.00160,* 2016.
23. M. A. Atıcı, Ş. Sağıroğlu, "Beyin Tümörlerinin Derin Öğrenme Yaklaşımlarıyla Tespiti, Doktora, Gazi Üniversitesi Fen Bilimleri Enstitüsü / Bilgisayar Mühendisliği Ana Bilim Dalı, 2020.
24. A. Öcal, L. Özbakır, Supervised deep convolutional generative adversarial networks, *Neurocomputing,* 449(2), 389-398, 2021.
25. A. Dash, J. Ye, and G. Wang, A review of Generative Adversarial Networks (GANs) and its applications in a wide variety of disciplines--From Medical to Remote Sensing, *arXiv preprint arXiv:2110.01442,* 2021.
26. J. Brownlee, *Generative Adversarial Networks with Python: Deep Learning Generative Models for Image Synthesis and Image Translation*, Machine Learning Mastery, 2(1), 25-37, 2019.

27. Y. Liu, J. Peng, J. James, Y. Wu, PPGAN: Privacy-preserving generative adversarial network, *2019 IEEE 25Th international conference on parallel and distributed systems (ICPADS)*, Tianjin, China, 2019.
28. L. Xie, K. Lin, S. Wang, F. Wang, J. Zhou, Differentially private generative adversarial network, *arXiv preprint arXiv:1802.06739,* 2018.
29. R. Torkzadehmahani, P. Kairouz, B. Paten, Dp-cgan: Differentially private synthetic data and label generation, *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, CA, USA, 2019.
30. J. Jordon, J. Yoon, M. Van Der Schaar, PATE-GAN: Generating synthetic data with differential privacy guarantees, *International conference on learning representations*, Vancouver, Canada, 2018.
31. P. Isola, J.-Y. Zhu, T. Zhou, A. A. Efros, Image-to-image translation with conditional adversarial networks, *Proceedings of the IEEE conference on computer vision and pattern recognition*, Hanolulu, Hawaii, 2017.
32. O. Mogren, C-RNN-GAN: Continuous recurrent neural networks with adversarial training, *arXiv preprint arXiv:1611.09904,* 2016.
33. H. Zhang *et al.*, Stackgan: Text to photo-realistic image synthesis with stacked generative adversarial networks, *Proceedings of the IEEE international conference on computer vision*, Venice, Italy, 2017.