

# Scalable Privacy Preservation in Big Data

**Ankita Hatiskar**

Department of Information Technology

Sir Sitaram and Lady Shantabai Patkar College of Arts and Science, Mumbai, Maharashtra, India

**Abstract:** *In the realm of data analytics, big data has welcomed a revolution. Data that was abandoned a few years ago is now seen as a valuable resource. Big data is increasingly widely employed across all aspects of society for knowledge extraction. It is generated by practically all digitization, and it is saved and transmitted over the internet. This dependence on the web approach for massive data raises severe security problems. Due to its vast volume, diversity, and volume, traditional security measures cannot be used to big data. Privacy is also a huge security nightmare since a large dataset appears to contain confidential details. Traditional privacy preservation approaches are utilized to solve privacy difficulties in Big Data, and K-anonymity is the most often used strategy for protecting privacy for data disclosure.*

**Keywords:** Big data, Data privacy, Anonymization, K-Anonymization, Privacy, Scalable.

## REFERENCES

- [1]. AntorweepChakravorty, Tomasz Wlodarczyk, ChunmingRong, —Privacy Preserving Data Analytics for Smart Homes, IEEE Security and Privacy Workshops, pp. 1-5, 2013.
- [2]. Fung, B.C.M., Wang, K., Chen, R., Yu, P.S.: Privacy-preserving data publishing: A survey of recent developments. ACM Computing Surveys 42(4), 14 (2010)
- [3]. Jeff Sedayao, Rahul Bhardwaj and Nakul Gorade, —Making Big Data, Privacy, and Anonymization work together in the Enterprise: Experiences and Issues, IEEE International Congress on Big Data, pp.1-7, 2014.
- [4]. Linna Li, Michael F. Goodchild and Santa Barbara, — Is Privacy Still an Issue in the Era of Big Data —Location disclosure in spatial footprints, Proceedings of 21st International conference on Geoinformatics, IEEE, pp.1-4, 2013.
- [5]. Liu Y et al. A practical privacy-preserving data aggregation (3PDA) scheme for smart grid. IEEE Trans Ind Inf. 2018
- [6]. M. V. Dijk, A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing," Proceedings of the 5th USENIX conference on Hot topics in security, August 10, 2010, pp.1-8.
- [7]. N. Li, T. Li, S. Venkatasubramanian, "t-Closeness: Privacy Beyond k-Anonymity and l-Diversity, " IEEE 23rd International Conference on Data Engineering, 2007, pp. 106 - 115.
- [8]. Omar Hasan, Benjamin Habegger, Lionel Brunie, Nadia Bennani, Ernesto Damiani, —A Discussion of Privacy Challenges in User Profiling with Big Data Techniques: The EEXCESS Use Case, IEEE International Congress on Big Data , pp. 1-6, 2013.
- [9]. S. Sagioglu and D. Sinanc, "Big Data: A Review," Proc. International Conference on Collaboration Technologies and Systems, 2013, pp. 42- 47
- [10]. S.H. Kim, J. H. Eom, T. M. Chung, "Big Data Security Hardening Methodology Using Attributes Relationship," Proc. International Conference on Information Science and Applications (ICISA), 2013, pp. 1-2.
- [11]. S. H. Kim, N. U. Kim, T. M. Chung, "Attribute Relationship Evaluation Methodology for Big Data Security," Proc. International Conference on IT Convergence and Security (ICITCS), 2013, pp. 1-4.
- [12]. Wenyi Liu, A. SelcukUluagac, and RaheemBeyah, —MACA: A Privacy-Preserving Multi-factor Cloud Authentication System Utilizing Big Data, IEEE INFOCOM Workshops, pp. 518- 523, 2014.
- [13]. Y. Demchenko, P. Grzso, C. De Laat, P. Membrey, "Addressing Big Data Issues in Scientific Data Infrastructure," Proc. International Conference on Collaboration Technologies and Systems, 2013, pp. 48- 55.

