Abstract

Big data has brought a revolution in the world of data analytics. Data that was discarded a few years back is now considered a powerful asset. Big data is now being extensively used for knowledge discovery by all sectors of society. It is produced by almost all digital processes and is stored, shared on web. This reliance of big data on web model poses serious security concerns. Traditional security methods cannot be applied to big data due to its large volume, variety and volume. Also since big data contains person specific information, privacy is a major security concern. The three important privacy preservation methods are: data anonymization, notice and consent and differential privacy. In this paper we discuss these privacy preservation methods for big data and how differential privacy is a better solution for big data privacy.

References

- M. V. Dijk, A. Juels, "On the impossibility of cryptography alone for
- L. Sweeney, "k-anonymity: A model for protecting privacy,
- N. Li, T. Li, S. Venkatasubramanian, "t-Closeness: Privacy Beyond k-Anonymity and l-Diversity,
- F. H. Cate, V. M. Schönberger, "Notice and Consent in a World of Big Data,

Index Terms

Computer Science

Security

Keywords
Big data  Data privacy  Anonymization  Differential privacy  Notice and consent