Commentary
Volume 16:3, 2023

Journal of Computer Science & Systems Biology

ISSN: 0974-7230 Open Access

Privacy-Preserving Techniques for Big Data Analytics in the Age of Digital Surveillance

Mark Daniel*

Department of Business Information Systems, Pantheon-Sorbonne University, 12 Pl. du Panthéon, 75231 Paris, France

Description

The rapid growth of digital technologies and the proliferation of data collection have given rise to concerns regarding privacy, especially in the context of big data analytics. With increasing instances of digital surveillance, individuals and organizations face the challenge of balancing the benefits of data analysis with the need to protect sensitive information. This research article provides an overview of privacy-preserving techniques that address these concerns in the realm of big data analytics. We explore various methods such as encryption, anonymization, and differential privacy, highlighting their strengths and limitations. The article also discusses the potential impact of these techniques on data utility and the evolving landscape of privacy regulations. By understanding and implementing these privacy-preserving techniques, stakeholders can strike a balance between data analysis and safeguarding individual privacy [1-3].

The age of digital surveillance has ushered in a new era of privacy concerns. As data collection and analysis become ubiquitous in various domains, including healthcare, finance, and social media, there is an urgent need to protect sensitive information from unauthorized access. This article examines the privacy-preserving techniques that enable the extraction of valuable insights from big data while ensuring the privacy of individuals. Privacy-preserving techniques have become essential in mitigating the risks associated with big data analytics and digital surveillance. These techniques aim to enable data analysis while ensuring the confidentiality and anonymity of individuals' personal information. By applying privacy-preserving techniques, organizations can extract valuable insights from data without compromising the privacy rights of individuals.

This research article provides an overview of privacy-preserving techniques that address the concerns surrounding big data analytics in the age of digital surveillance. It explores various methods, such as encryption, anonymization, and differential privacy, which have proven effective in safeguarding privacy while allowing for meaningful analysis. By understanding and implementing these techniques, stakeholders can navigate the intricate landscape of data privacy, fostering a responsible and ethical approach to data analytics.

Privacy-Preserving Techniques

Encryption

Encryption techniques, such as homomorphic encryption and secure multi-party computation, enable data analysis on encrypted data without revealing the raw information. These methods allow computations to be performed on encrypted data, ensuring privacy during the analytical process. However, encryption can introduce computational overhead and pose challenges in performing certain types of computations efficiently.

***Address for Correspondence:** Mark Daniel, Department of Business Information Systems, Pantheon-Sorbonne University, 12 Pl. du Panthéon, 75231 Paris, France, E-mail: MarkDaniel21@gmail.com*

Received: 17 April, 2023, Manuscript No. jcsb-23-99622; **Editor Assigned:** 19 April, 2023, Pre QC No. P-99622; **Reviewed:** 03 May, 2023, QC No. Q-99622; **Revised:** 09 May, 2023, Manuscript No. R-99622; **Published:** 17 May, 2023, DOI:10.37421/0974-7230.2023.16.470

Anonymization

Anonymization techniques, such as k-anonymity and l-diversity, de-identify datasets by removing or obfuscating personally identifiable information. By achieving a level of indistinguishability among individuals, anonymization protects privacy while allowing data analysis. However, re-identification attacks and the risk of attribute disclosure pose challenges to the effectiveness of these techniques [4,5].

Differential privacy

Differential privacy provides a rigorous framework for privacy guarantees in data analysis. By injecting controlled noise into queries or statistical computations, differential privacy ensures that individual contributions to the dataset cannot be distinguished. This technique balances privacy and data utility, but careful parameter tuning is required to strike an appropriate balance.

Impact on data utility

While privacy-preserving techniques are essential for safeguarding sensitive information, they can impact data utility. Encryption and anonymization can introduce noise or distortion, potentially reducing the accuracy of analysis results. Differential privacy can limit the granularity of queries to protect privacy, leading to a trade-off between privacy guarantees and analytical precision. Striking a balance between privacy and data utility is a crucial consideration for practitioners.

Evolving landscape of privacy regulations

The growing awareness of privacy concerns has led to the development of privacy regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). These regulations impose legal obligations on organizations to protect individual privacy and provide transparency in data handling practices. Privacy-preserving techniques play a pivotal role in enabling compliance with these regulations and fostering a privacy-centric culture. As the digital landscape continues to evolve, privacy-preserving techniques are crucial for ensuring the responsible use of big data analytics in the face of digital surveillance. Encryption, anonymization, and differential privacy offer viable approaches to strike a balance between data analysis and privacy protection. However, it is essential to evaluate the trade-offs between privacy and data utility while considering the evolving landscape of privacy regulations. By embracing these techniques, stakeholders can navigate the challenges posed by digital surveillance and preserve individual privacy in the era of big data analytics.

Acknowledgement

None.

Conflict of Interest

Authors declare no conflict of interest.

References

1. Guo, Yulan, Mohammed Bennamoun, Ferdous Sohel and Min Lu, et al. "3D object recognition in cluttered scenes with local surface features: A survey." *IEEE Trans Pattern Anal Mach Intell* 36 (2014): 2270-2287.

2. Schmidhuber, Jürgen and Sepp Hochreiter. "Long short-term memory." Neural Comput 9 (1997): 1735-1780.

3. Al Badawi, Ahmad, Louie Hoang, Chan Fook Mun and Kim Laine, et al. "Privft: Private and fast text classification with homomorphic encryption." *IEEE Access* 8 (2020): 226544-226556.

4. Jung, Wonkyung, Sangpyo Kim, Jung Ho Ahn and Jung Hee Cheon, et al. "Over 100x faster bootstrapping in fully homomorphic encryption through memory-centric optimization with gpus." *IACR Trans Cryptogr Hardw Embed Syst* (2021): 114-148.

5. Eltayieb, Nabeil, Rashad Elhabob, Alzubair Hassan and Fagen Li. "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud." *J Syst Archit* 102 (2020): 101653.

How to cite this article: Daniel, Mark. "Privacy-Preserving Techniques for Big Data Analytics in the Age of Digital Surveillance." *J Comput Sci Syst Biol* 16 (2023): 470.