OPEN ACCESS Freely available online

Journal of Information Technology & Software Engineering

ISSN: 2165-7866

Commentary

Evolutionary Implementation of a Security Breaches in Big Data Privacy

Fargana Camtepe*

Department of Computer Science and Software Engineering, Ghent University, Ghent, Belgium

DESCRIPTION

When performing analytics or training machine learning algorithms, big data sets might quickly exceed the RAM on a desktop or laptop computer. The coefficient of determination from the regression analysis is also recomputed after removing each sample observation. The goal is to avoid including all observations (especially in large datasets) when these statistics are recomputed. The real-world datasets we use today are highly correlated, as our reliance on data continues to grow as it becomes a commodity of choice around the world. For years, researchers have paid attention to this aspect of data protection, but have found that existing data protection guarantees cannot be guaranteed by existing data protection algorithms when there is a correlation between the data. The data protection guarantees of existing algorithms were sufficient when there were no relationships between the data in the dataset. Therefore, given the existence of data correlation, there is an urgent need to rethink data protection algorithms. Some research explores using well-known machine learning concepts. The amount of research on correlated privacy, though less numerous, is still substantial. However, the related big data privacy has not been fully explored. Often, the real-world datasets we work with are large (technically called big data) and contain a large amount of data correlation. Therefore, there is an urgent need to understand and propose solutions for data protection of correlated big data.

Big data should be stored in the cloud, but companies are not relying on it for security and privacy reasons. When choosing the cloud for data storage, users worry about issues such as leakage of personal information, unauthorized user access and modification of data, and malicious behavior while accessing cloud data. Privacy leaks should be avoided when analyzing data. Data integrity must be maintained to avoid data modification. We also need machine learning models to detect malicious activity patterns of users in the cloud to ensure data security. Big data requires technology that protects privacy and security with minimal investment of time and space. An approach using anonymization, integrity, and machine learning techniques is proposed. The top three privacy risks are misuse of personal data, data security, and data quality. Misuse of personal data can lead to loss of control and transparency. Data breaches are a major challenge as they can expose personal data to potential misuse.

Cloud computing provides applications, platforms, infrastructure, and storage services over the Internet in a consumption-based model. This reduces setup and maintenance costs for the IT industry. Before adopting or using the cloud, there are a number of risks that must be eliminated. Big data requires the cloud to store and share data, raising security and privacy concerns. Research is needed that focuses on finding solutions to security challenges such as data theft, information corruption, unauthorized intrusion, and disclosure of personal information leading to loss of privacy. Real-time services rely on data from the internet and sensors. Analyzing this fast-generated data is challenging, and big data technology handles this situation quickly without introducing bottlenecks.

Data from different sources in different formats need to be classified before being processed. Insights provided by big data include customer details. Unfortunately, these details are often private and can fall into the wrong hands. When that happens, customers lose trust in this organization. Therefore, companies should take measures to prevent the compromise of confidential information. Big data ethics, also called simple data ethics, refers to the systematization, defense, and recommendation of the concept of right and wrong actions regarding data, especially personal data. Big data repositories are often too large to be analyzed using traditional data analytics. But if big data is analyzed correctly, many interesting conclusions can be drawn.

Correspondence to: Fargana Camtepe, Department of Computer Science and Software Engineering, Ghent University, Ghent, Belgium, E-mail: camfar@vb.sv.be

Received: 02-Jan-2023, Manuscript No. JITSE-23-22509; **Editor assigned:** 05-Jan-2023, PreQC No. JITSE-23-22509 (PQ); **Reviewed:** 19-Jan-2023, QC No. JITSE-23-22509; **Revised:** 26-Jan-2023, Manuscript No. JITSE-23-22509 (R); **Published:** 02-Feb-2023, DOI: 10.35248/2165-7866.23.13.319

Citation: Camtepe F (2023) Evolutionary Implementation of a Security Breaches in Big Data Privacy. J Inform Tech Softw Eng. 13:319.