**Top 7 Big Data Security Issues and Their Solutions**

Today, Big Data is crucial for any business to succeed in the data-driven world. With several advanced infrastructures, organizations have streamlined the flow of data for real-time insights delivery and better decision-making. However, Big Data brings several security risks that could negatively impact organizations. Failing to incorporate security measures while storing and processing Big Data can lead to data breaches. While simplifying the accessibility of data is essential for companies, having control over Big Data is equally crucial for ensuring trust among its customers.

The ever-increasing data presents both opportunities and challenges. While the prospect of better analysis allows companies to make better decisions, there are certain disadvantages like it brings security issues that could get companies in the soup while working with sensitive information. Here are some of the Big Data Security challenges that companies should mitigate:

• Big Data Security Issues: Data Storage

• Big Data Security Issues: Fake Data

• Big Data Security Issues: Data Privacy

• Big Data Security Issues: Data Management

• Big Data Security Issues: Data Access Control

• Big Data Security Issues: Data Poisoning

• Big Data Security Issues: Employee Theft

**Big Data Security Issues: Data Storage**

Businesses are adopting Cloud Data Storage to move their data easily to expedite business operations. However, the risks involved are exponential with security issues. Even the slightest mistake in controlling the access of data can allow anyone to get a host of sensitive data. As a result, big tech companies embrace both on-premise and Cloud Data Storage to obtain security as well as flexibility.

While mission-critical information can be stored in on-premise databases, less sensitive data is kept in the cloud for ease of use. However, to implement security policies in on-premise databases, companies require cybersecurity experts. Although it increases the cost of managing data in on premise databases, companies must not take security risks for granted by storing every data in the cloud.

**Big Data Security Issues: Fake Data**

Fake Data generation poses a severe threat to businesses as it consumes time that otherwise could be spent to identify or solve other pressing issues. There is more scope for leveraging inaccurate information on a very large scale, as assessing individual data points can be a daunting task for companies.

False flags for fake Data can also drive unnecessary actions that can potentially lower production or other critical processes required for running businesses. One way to avoid this is to ensure that companies should be critical of the data they are working on for enhancing business processes. An ideal approach is to validate the data sources by periodic assessments and evaluate Machine Learning models with diverse test datasets to find anomalies.

**Big Data Security Issues: Data Privacy**

Data Privacy is a big challenge in this digital world. It aims to safeguard personal or sensitive information from cyberattacks, breaches, and intentional or unintentional data loss. Businesses must follow stricter Data Privacy principles with the help of access management services in the cloud, including very rigid privacy compliance, to strengthen Data Protection. It is best to follow a few rules alongside implementing one or more Data Security technologies. The general rules are knowing your data, having more grip over your data stores and backup, safeguarding your network against unauthorized access, conducting regular risk assessments, and training the users regularly about Data Privacy and Data Security.

**Big Data Security Issues: Data Management**

A security breach can have crushing consequences on businesses, including the vulnerability of critical business information to a completely compromised database. Deploying highly secured databases is vital to ensure data security at all levels. A superior Database Management System comes with various access controls. While it is advisable to follow rigid and rigorous physical security practices, it is even more essential to follow extensive software-based security measures to safeguard data storage. A few methods to effectively achieve this goal are—practicing data encryption, data segmenting and partitioning, securing on-the-move, and implementing a trusted server. Besides, a few security tools can integrate with databases to automatically monitor data sharing and notify businesses when data has been compromised.

**Big Data Security Issues: Data Access Control**

Controlling which data users can view or edit enables companies to ensure not only data integrity but also preserves its privacy. But managing access control is not straightforward, especially in larger companies that have thousands of employees. However, a shift from on-premise solutions to cloud-based services has simplified the process of working with Identity Access Management (IAM). IAM does the job of controlling data flow via identification, authentication, and authorization. Following relevant ISO standards is a good starting place to ensure organizations meet the best IAM practices.

**Big Data Security Issues: Data Poisoning**

Today, there are several Machine Learning solutions like chatbots that are trained on a colossal amount of data. The advantages of such solutions are that they keep on improving as users interact. However, this leads to Data Poisoning, a technique to attack Machine Learning models’ training data. It can be considered as an integrity attack as the tampered training data can affect the model’s ability to provide correct predictions. The results can be catastrophic, ranging from logic corruption to Data Manipulation and Data Injection. The best way to beat the evasion is through outlier detection, wherein the injected elements in the training pool can get separated from the existing data distribution.

**Big Data Security Issues: Employee Theft**

Advance data culture has allowed every employee to hold a certain level of critical business information. While it boosts data democratization, the risk of an employee leaking sensitive information, intentionally or unintentionally, is high. Employee Theft is prevalent not only in big tech companies but also in startups. To avoid Employee Theft, companies have to implement legal policies along with securing the network with a virtual private network. In addition, companies can use a Desktop as a Service (DaaS) to eliminate the functionalities of data stored in local drives.