|  |
| --- |
|  |
| BIG DATA PRIVACY |
| ASSIGNMENT 2 |

|  |
| --- |
| Sukhdeep Kaur  Submitted to Dr. Read |

**BIG DATA PRIVACY AND SECURITY**

Nowadays, big data is a common word in big industries and it usually refers to a huge amount of data. Big data can bring benefits on a large scale such as advertisement really focused on which you really want to buy, can offer wearable devices that can monitor your health.

Huge amount of data also leads to big data privacy concerns. People generate data on large scale which is in the hands of big organizations and their employees. Data generated by people contains some sensitive information, hence data privacy is a main concept which should be taken in concern. Todays, companies face too many challenges related to privacy.

**CHALLENGES FACED BY COMPANIES**

1. **Secure data storage and transactions logs**

Data and transaction logs are stored in multi-tiered storage media. As the size of data growing exponentially, auto-tiering is recommended. However, auto-tiering solutions do not keep track of where the data is stored, which leads to new challenges to secure stored data in the presence of unauthorized access.

1. **Software used for big data**

Software commonly used for the storage big data such as Hadoop doesn’t always come with user authentication by default. This makes a problem of access control because a default installation open to unauthorized users.

1. **Anonymization becomes impossible**

With so much data and powerful analytics it becomes impossible to completely remove the ability to identify an individual if there are some poor rules established for the use of anonymized data files.

1. **Encryption of sensitive data**

Sensitive data is routinely stored unencrypted in the cloud. The main problem is to encrypt data, especially large data sets, disallowing people to easily perform fine grained actions such as sharing searches to secure the sensitive data.

**Equifax hack**

Equifax hack is a common example of poor handling of the breach. Equifax compromised 143 million records. These records contains credit numbers, social security numbers. This sensitive data is now in the hands of criminals. The flaw is the result of mishandling files uploaded to web server, allowing hackers to remotely run code.

**SECURITY ASPECTS USED BY ORGANIZTIONS**

1. **Safeguard distributed programming frameworks**

The CSA recommends that organizations first establish trust by using methods such as kerberas authentication while ensuring conforming to predefined security policies.

1. **Secure non-relational data**

Organizations uses layers to secure non-relational data such data tagging layer and object oriented security, also it can be secured using pluggable authentication models.

1. **Endpoint filtering and validation**

Endpoint is a paramount and your organization can start by using trusted certification, doing resource testing and connecting only trusted devices to your networks by using a mobile device management solution.

1. **Big data cryptography**

Mathematical cryptography has not gone out of style, infact it’s gotten for more advance. The CSA recommends a variety of cryptographic techniques such as identified-based encryption and attribute based encryption to secure most of sensitive data.

1. **Audit**

Auditing is must in big data security, particularly after an attack on your system. Organization should create a cohesive audit view following any attack in order to cut down incident response time.

**GOOGLE USES PROTECTION METHODS**

Encryption keeps the data of user private while data in transit. Encryption brings a higher level of security and privacy to google services. When users do things like send an email, share a video, visit a website, or store photos, the data that users create and move from their devices to google services. Google uses some leading encryption layers such as transport layer security and HTTPS.

Apart from this, google have privacy policies that are based on rules which helps to protect user’s data.

**CONCLUSION**

**Privacy concern is the main concept today which needs to be taken effectively to provide security. There are many security methods and technologies available in the market, however, these are not enough to secure a huge amount of data.**