**简答题:**

**简析大数据生命周期中存在哪些安全风险，我们可以使用哪些技术手段实现安全目标？**

**安全风险**

一、存在大数据平台安全：比如大数据存储安全、大数据传输安全、大数据平台访问控制安全、大数据运行计算安全、大数据基础设施安全

二、存在大数据自身安全风险：比如数据源的真实可信性，源数据被伪造或刻意制造风险的存在，还有数据源是否可靠和完整，采集过程中由于人工干预带来的误差也会有安全风险。

三、存在大数据应用安全：如用户隐私问题，个人数据在平台上处理、流转过程中可能会被泄露，同时用户有时候没有权利决定自己的信息如何被使用，用户的隐私安全存在风险，还有数据治理和合规性风险: 大数据环境需要符合各种法规和标准，如GDPR或HIPAA，违反这些法规可能导致重大的财务和法律后果

**技术手段**

1.数据加密技术:加密和解密技术的运用，加密阶段将原始信息经过加密密钥及加密函数

转换，变成无意义的密文，实现信息隐蔽。解密阶段：接收方则将此密文经过解密函数、解

密密钥还原成明文。

2. 大数据真实性分析认证技术：保证大数据的真实可信性，对大数据的发布者进行认证检测。常用的方法有：数字签名、数字水印、基于数据挖掘的认证技术

3. 访问控制技术：基于角色的访问控制、基于属性加密的访问控制、基于风险的访问控制

4. 数据溯源技术：能够追踪和记录数据的来源和其在整个生命周期中的变化的技术，数据溯源对于保证数据质量、合规性和安全尤为重要。常用有标记法、反向查询法

5. 大数据安全审计技术：有基于规则的安全审计、基于统计的安全审计、基于机器学习的安全审计

6. APT攻击检测技术：通过异常行为分析，沙盒技术等及时发现APT攻击，提供必要的信息和工具来有效防御和应对高级威胁，保护组织的网络安全。

7. 数据脱敏技术: 对敏感信息进行脱敏处理，以防止在分析过程中暴露原始数据。这通常用于在保持数据实用性的同时，保护个人隐私。

8. 区块链技术: 用于增强数据的完整性和透明度，特别是在多方数据交互和处理的环境中。通过区块链，可以创建一个不可篡改的数据记录和验证日志,保护数据安全。

9.安全多方计算(SMC): 允许多方共同完成数据分析和处理任务，而无需暴露各自的数据。这是一种保护数据隐私的技术，特别适用于跨边界数据处理。

10.AI与机器学习在安全中的应用: 利用机器学习算法来识别和预防异常行为和安全威胁，提高安全事件的检测速度和准确性。

11.物理和网络安全措施的增强: 加强数据中心的物理安全措施，以及使用先进的网络安全技术，如入侵检测系统(IDS)和入侵防御系统(IPS)。