

二维数据可视化	在数据可视化中, 二维数据是指由两种主要描述属性构成的数据, 如一个物体的宽度和高度、一个城市的平面地图、建筑物的楼层平面图等都是二维数据可视化的实例。最常见的二维数据可视化就是地理信息系统 (Geographic Information System, GIS)
三维数据可视化	三维数据比二维数据更进了一层, 它可以描述立体信息。三维数据可以表示实际的三维物体, 因此可视化的许多应用是三维可视化。物体通过三维可视化构成计算机模型, 供操作及试验, 因此预测真实物体的实际行为
多维数据可视化	在可视化环境中, 多维数据所描述事物的属性超过三维, 为了实现可视化, 往往需要降维
时态数据可视化	时态数据可视化实际上二维数据的一种特例, 即二维中有一维是时间轴。它以图形方式显示随着时间变化的数据, 是可视化信息最常见、最有用的方式之一
层次数据可视化	层次数据即树形数据, 其数据内在结构特征为: 每个节点都有一个父节点 (根节点除外)。节点分兄弟节点 (拥有同一个父节点) 和子节点 (从属该节点的节点)。拥有这种结构的数据很常见, 如商业组织、计算机文件系统和家谱图都是按树形结构排列的层次数据
网络数据可视化	网络数据指与任意数量的其他节点有关系的节点的数据。网络数据中节点不受与它有关系的其他节点数量的约束 (不同于层次节点有且只有一个父节点), 网络数据没有固有的层次结构, 两个节点之间可以有多条连接路径, 也就是说节点间关系的属性和数量是可变的

5、数据库安全 (了解)

数据库安全对策

安全对策	说明
防止非法的数据访问	数据库管理系统必须根据用户或应用的授权来检查访问请求, 以保证仅允许授权的用户访问数据库。
防止推导	指的是用户通过授权访问的数据, 经过推导得出机密信息, 而按照安全策略, 该用户是无权访问此机密信息的。
保证数据库的完整性	是保护数据库不受非授权的修改, 以及不会因为病毒、系统中的错误等导致的存储数据破坏。这种保护通过访问控制、备份/恢复以及一些专用的安全机制共同实现。
保证数据的操作完整性	定位于在并发事务中保证数据库中数据的逻辑一致性。由并发管理器子系统负责。
保证数据的语义完整性	在修改数据时, 保证新值在一定范围内符合逻辑上的完整性。对数据值的约束通过完整性约束来描述。
审计和日志	审计和日志是有效的威慑和事后追查、分析工具。
标识和认证	标识和认证是授权、审计等的前提条件是第一道安全防线。
机密数据管理	对于同时保存机密和公开数据的数据库而言, 访问控制主要保证机密数据的保密性, 仅允许授权用户的访问。这些用户被赋予对机密数据进行一系列操作的权限, 并且禁止传播这些权限。
多级保护	将数据划分不同保密级别, 用户只能访问拥有的权限所对应级别的数据
限界	限界的意义在于防止程序之间出现非授权的信息传递

数据库安全机制包括用户的身份认证、存取控制、数据库加密、数据审计、推理控制等内