数据安全及保护

在当今信息爆炸的时代，数据的涵义已远远超出其原意数值的概念。一份文档，一张图片，一部电影、一个程序等等一切储存在各种存储介质里的信息都可以称为数据。数据涵盖范围极广，小至我们的一篇日记，大至跨国公司的全部客户资料，数据安全的重要性不言而喻。本文主要来简要讲述什么是数据安全，如何保护数据安全的问题。

1. 数据安全

“信息（Information）和数据（Data）是计算机的两个重要概念，一般认为信息是对数据进行处理后得到的……但在很多情况下，信息和数据这两个词被不加区分地使用着。”

数据是信息的承载者，信息是数据的内涵，人们通过解释、推理、归纳、分析、综合等方法，从数据中获得有意义的内容就是信息。对于人类的推理和计算来说，真正有用的不是数据本身，而是数据中携带的信息。为了达到保护信息安全的目的，我们必须保护数据安全。

数据安全主要分为物理安全和安全服务两部分。

数据的物理安全是指在物理介质上对存储和传输的数据的安全保护，是数据安全的最基本的保障。这一类的不安全因素主要有自然灾害、物理损坏、电磁辐射、操作失误等。提供这一类的安全保护主要通过采取各种安全措施、制定安全规章制度、状态检测、报警确认、数据备份、应急恢复等来完成。

数据的安全服务是指通过对数据的存储、传输和处理过程的监控和管理提供的安全保护。这一类安全保护通常是通过数据加密、用户身份认证、访问权限控制、互连设备与接口模块的状态监控、防火墙等手段来实现的。

数据安全或信息安全有两方面的含义：一是数据本身的安全，二是数据防护的安全。

信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。根据国际标准化组织（ISO）1的定义，信息安全性的含义主要是指信息的完整性、可用性、保密性和可靠性。

1.1 数据安全的重要性

信息一诞生就自动成为决策的基础，收集信息，是决策的前提。而在当今信息爆炸，竞争激烈的现代社会，信息的重要性更是被提到了一个前所未有的高度。信息，就是资源；信息，就是财富。

“今天的信息已经被认为是人类的重要资源，因此对信息资源的开发、运用也成为社会生活、经济活动的重要组成部分，并且成为衡量一个国家现代化程度的标志，有效地开发、运用和拥有信息资源已经被上升到国力的高度。”2

人们对信息、信息技术的依赖程度越来越高。一方面，信息已经成为一种崭新的资产，在政治、经济、军事、教育、科技和生活等方面发挥着重要的作用；另一方面，由此而带来的信息安全问题正变得日益突出。由于信息具有易传输、易扩散、易破损的特点，信息需要严格管理和妥善保护。

对于求职者来说，某些公司的招聘信息，对应聘者的要求，面试官的性格倾向，甚至更直接一点，笔试面试的题目等，都是相当宝贵的资源，影响到他的求

职生涯。对企业来说，人才的流动，市场的反应，竞争对手的变动，政府对市场的态度和措施，都是其在瞬息万变的商场上应对各类挑战，抓住各种机遇所必不可少的信息。对政府来说，市场的变动，人民的想法，国际局势的风吹草动，企业发展状况，都是其制定内外政策必须基于的数据。

个人、企业和政府基本上涵盖了现代社会的大部分主体，信息对于当代社会重要性毋庸置疑，数据安全的重要性可见一斑。

1.2 数据本身的安全

数据本身的安全即为数据内容的安全，保证数据内容的保密性，完整性和可用性是数据本身的安全的重要内容。

1.2.1 数据的保密性

保密性(Confidentiality)是指严密控制各个可能泄密的环节，使信息在产生、传输、处理和存储的各个环节中不泄漏给非授权的个人和实体。即信息只为授权用户使用。保密性是在可靠性3和可用性4基础之上，保障信息安全的重要手段。

数据的保密性是数据安全的核心内容。

在信息成为资源与财富的时候，人们更注意对信息的独家占有以保证自己在竞争中拥有足够的资本而不至于落败。信息资源的独家占有可以用来交换自己需要的其他信息，而一些珍稀的信息资源更是足以让己方占尽优势。数据的保密性在此便显得尤为重要。

1.2.2 数据的完整性

完整性（Integrity）是指存储在数据库中的所有数据值均正确的状态，主要是指数据的精确性（Accuracy） 和可靠性（Reliability）。数据在存储或传输过程中保持不被偶然或蓄意地修改、删除、伪造、乱序、重置等所破坏和丢失是数据完整性的特性。如果数据库中存储有不正确的数据值，则该数据库称为已丧失数据完整性。

数据库中的数据是从外界输入的，而数据的输入由于种种原因，会发生输入无效或错误信息。保证输入的数据符合规定，成为了数据库系统，尤其是多用户的关系数据库系统首要关注的问题。为了防止数据库中存在不符合语义规定的数据和防止因错误信息的输入输出造成无效操作或错误信息，提出数据完整性的概念。

数据往往不会孤立地存在，不同的数据之间会存在着一定的关联，很少有单一数据。所以通常各类数据根据某种分类依据被集中在一起管理，形成数据库。因此数据的完整性更多的是数据库的完整性。

1.2.3 数据的可用性

对于可用性，ISO9241/11 中的定义是：一个产品可以被特定的用户在特定的境况中，有效、高效并且满意得达成特定目标的程度。那么数据的可用性，顾名思义，就是数据在被人们使用的过程中对人们达成目标的帮助的效率有多高。数据在需要时可以被已授权的用户合法使用是数据可用性的特性。

表面上看来数据的可用性和数据安全并没有什么太大的关系，其实不然。在信息化社会，数据呈现出井喷式的增长。在信息爆炸中，无法避免地出现了很多

劣质数据，这大大地降低了数据的可用性。而劣质数据所导致的决策失误的后果可能要比数据外泄和数据完整性破坏可能导致的后果更为严重。

保证数据的可用性，保证数据使用的安全，也是保证数据安全的重要内容。

1.3 数据防护的安全

数据防护的安全即保护数据免受因存储介质损坏、人为过失、人为刻意窃取或破坏以及病毒等因素而导致数据的泄露、破坏和缺失。

数据防护的安全包括了数据的物理安全和安全服务这两个内容。与数据本身的安全注重对数据本身的保护不同，数据防护的安全更多地倾向于保护数据免受来自外部的影响或破坏。

可以说数据防护的安全是数据保护的重要内容。因为对数据本身的安全的保护大部分情况下依赖于对数据防护安全的保护。对数据本身的安全的保护，归根结底还是要回到对数据防护的安全的保护上。所以对数据防护的安全技术的研究，是数据安全保护研究的重要内容。

2. 2 数据保护

数据安全的重要性和现状要求我们必须重视对数据的保护，而与数据安全的两种分类相对应，亦有两种指向不同目的的数据的保护。

2.1 针对数据本身安全的数据保护

2.1.1 对数据保密性的保护

由数据访问和传播的完整路径出发，对数据保密性的保护可以从以下 3 方面着手：一，访问者；二，访问途径；三，数据源。

数据访问者是数据访问途径中的能动部分，欲使访问者不去破坏数据的保密性，就要使访问者对数据的内容守口如瓶，做好保密工作。而对于未获得允许而

想访问数据的访问者，要制定和完善相关的法律法规来阻止与惩戒这样的行为。要加强社会主义精神文明建设，构建社会主义核心价值体系，传播与弘扬社会主义价值观，使人们从内心自发地不去做破坏数据保密性的事。

而这毕竟是一个任重道远的过程，并且对一些具有巨大价值的数据的保密不能仅仅依靠人们的自觉性。对此，比较有保障的方法则是对访问者的身份的认证。

有效的身份识别是信息安全的保障，在对数据的访问或使用中，必须有严格的身份验证保证信息及信息系统的安全，保证授权用户的权利。

访问途径就是访问者到达数据源的途径。想要保护数据的保密性，可以对访问途径加以限制，这里或许可以借助访问控制技术。访问控制是在保障授权用户能获取所需资源的同时拒绝非授权用户的安全机制，是信息安全理论的重要组成部分。对限定范围的人开放访问权限，对有访问权限的人授予不同等级的管理权限。非授权用户没有访问权限，而授权用户有访问权限，但是授权用户中存在存取权限的差别，如读取、写入、执行、删除、追加等存取方式的组合。

数据源是数据保密性的基础部分。对数据源进行复杂的加密，使破译的难度上升。所谓数据加密（Data Encryption）技术是指将一个信息（或称明文，plain text）经过加密钥匙（Encryption key）及加密函数转换，变成无意义的密文（cipher text），而接收方则将此密文经过解密函数、解密钥匙（Decryption key）还原成明文。加密技术是网络安全技术的基石。

我们所能常见到的主要就是磁盘加密和驱动级解密技术：

全盘加密技术是主要是对磁盘进行全盘加密，并且采用主机监控、防水墙等其他防护手段进行整体防护，磁盘加密主要为用户提供一个安全的运行环境，数

据自身未进行加密 ,操作系统一旦启动完毕 ,数据自身在硬盘上以明文形式存在，主要靠防水墙的围追堵截等方式进行保护。

驱动级技术是信息加密的主流技术，采用进程+后缀的方式进行安全防护，用户可以根据企事业单位的实际情况灵活配置，对重要的数据进行强制加密，大大提高了系统的运行效率。驱动级加密技术与磁盘加密技术的最大区别就是驱动级技术会对用户的数据自身进行保护，驱动级加密采用透明加解密技术，用户感觉不到系统的存在，不改变用户的原有操作，数据一旦脱离安全环境，用户将无法使用，有效提高了数据的安全性；另外驱动级加密技术比磁盘加密技术管理可以更加细粒度，有效实现数据的全生命周期管理，可以控制文件的使用时间、次数、复制、截屏、录像等操作，并且可以对文件的内部进行细粒度的授权管理和数据的外出访问控制，做到数据的全方位管理。

或许还可以设定自毁程序，在遭到暴力破解的情况下自动销毁数据。这可能造成数据的丢失，但对数据保密性的保证却是比较有利的。

2.1.2 对数据完整性的保护

上文已经提到，数据的完整性更多地体现在数据库的完整性上。数据完整性分为四类：实体完整性（Entity Integrity）、域完整性（Domain Integrity）、参照完整性(Referential Integrity)、用户自定义完整性(User-definedIntegrity)。数据库采用多种方法来保证数据完整性，包括外键、约束、规则和触发器。系统很好地处理了这四者的关系，并针对不同的具体情况用不同的方法进行，相互交叉使用，相补缺点。

数据库通常使用数据库管理系统5（DataBase Management System，DBMS）来管理。目前使用的数据库管理软件很多，大型的数据库管理软件有IBM的DB2，Oracle公司的Oracle，微软公司的SQL Server，还有Sybase公司的Sybase等。中小型公司的数据库软件有微软的FoxPro、Access等。

数据库管理系统对完整性约束6主要有实体完整性约束、参照完整性约束、函数依赖约束、统计约束四类。而实现完整性约束的方法依类别不同而不同。完整性约束可以分为两大类：静态约束和动态约束。这里不作详细的展开。

2.1.3 对数据可用性的保护

如果说数据保密性，数据完整性的保护倾向于保护数据本身，那么数据可用性的保护着更着重于数据的使用。数据可用性的保护核心在于如何排除冗余的低质信息，获取收集高质量的有效信息。

或者可以通过在数据筛选时的一系列限定排除掉一些重复的和过时的数据，又或者直接搜索我们需要的数据，但是又该如何保证排除掉的那些重复的和过时的数据就不包含我们需要的信息？应该有相关方面的专家学者正在研究这一方面的问题。毕竟在大数据时代如何提炼有效数据，排除冗余数据的干扰，保证决策及工作的高效，是一个时代性的问题。

2.2 针对数据防护安全的数据保护

数据防护安全的数据保护途径相对来说比较简单，一些具体内容在针对数据自身的安全的数据保护中已经比较详细地提到。针对任何原因造成的数据丢失有两种办法。一是及时做好重要数据的备份，二是进行数据恢复。当然数据恢复有一定失败的几率，数据备份这是最保险的方法。而针对人为刻意窃取和破坏则可

以加强防御系统的建设，阻挡黑客和病毒的攻击。还可以对核心数据的访问进行严格的审批，防止对数据的恶意破坏。

2.3 数据保护的意义

数据保护的意义不言自明，对企业和国家来说数据保护关系到自身的安全、利益甚至生死存亡。而对大学生来说，数据保护更多的是提高我们工作的效率，避免我们因意外原因导致的数据丢失而耗费太多的不必要的时间和精力，以及带来不必要的麻烦。我们能做的或许就是及时备份比较重要的数据，保护好自己的私人信息，同时尊重他人的数据安全，维护国家的安全和利益。