

大数据时代下云存储信息安全的防护技术

秦 璐

(江西医学高等专科学校, 江西 上饶 334000)

摘 要 数据以爆炸式的方式增长, 传统的数据存储方式已经很难在管理方面发挥稳定作用, 各类企业开始寻找更加有效的数据管理维护方法。而云存储作为近年来发展迅速的一项技术, 特别适用于大量数据的维护和管理, 从而解决本地存储空间不足的缺陷。用户也可以使用存储资源来存放有关的数据信息, 信息分布在不同的服务器主机之上, 在安全防护方面作用突出。

关键词 大数据 云存储 信息安全防护

中图分类号: G20

文献标识码: A

文章编号: 1007-0745(2021)05-0009-02

按照 IDC 的预测数据, 全球数据量将从 2016 年的 16ZB 增长至 2025 年的 160ZB 以上, 年复合增长率大约为 30%, 这说明大数据时代下, 人类正处于一个前所未有的信息爆炸时代, 互联网业务所产生的庞大数据量呈现出几何增长的态势, 不断挑战着原有的传统存储方法, 以大量数据存储为基础服务的云存储价值将在信息时代更加显著地得到社会认同。

1 云存储的有关内容

1.1 云存储的基本特征

云存储本身是云计算技术的代表, 应用也是一种新型的线上存储方案, 通过分布式文件系统和网络技术将散落在网络中的不同类型存储设备进行协同集合工作, 对外提供信息存储和业务访问的基本功能需求。通过云存储能够让存储设备和服务各自发挥职能, 按照用户的喜好借助传输设备将信息提前存储在云端, 并且还可以随时进行访问和下载, 有效地突破了数据管理的时间和空间限制。与此同时, 云存储的模型结构划分为访问层、应用层、基础管理层和存储层等四个部分, 访问层是云服务商直接授权用户登录系统的公用接口, 应用层则是实现云基础服务的功能接口, 基础层承担了存储协同工作和数据访问的基本要求, 而存储层则负责将不同类型的存储器进行连接和融合保障数据的集中管理。和传统的数据存储方法相比, 云存储技术在使用模式上更加高效率、便捷化, 不受到物理条件的限制, 可以直接在云服务器上采取集中性管理对数据进行备份, 以应对数据损坏或数据窃取等安全问题, 所以实现了智能化管控并大幅减少了人工机械化操作比例。

1.2 云存储的划分

一般情况下, 我们按照云存储的部署方式进行类别划分, 可以划分为私有云、公有云和混合云等几个部分, 其中私有云指的是用户内部访问管理和私有网络空间当中的存储服务与基础结构这些信息不与其他用户进行共享, 极大地强化了对于信息的安全管控, 而且私密性变得更加突

出。而公有云则指的是用户通过互联网的方式获取存储服务, 在云服务商区域获取他们想要的资源。混合原则将两者的功能和特性进行了综合管控, 不但实现了信息和数据的来回管理, 同时还获得了良好的信息部署功能^[1]。

2 大数据时代下云存储信息安全防护技术——以同态加密算法为例

同态加密算法本身是基于数学困难问题计算理论的密码, 学技术能够体现出密文和明文之间的对应关系, 让云存储系统当中可以完成对信息的检索与统计操作, 不需要进行解密就能直接对敏感数据进行调节。而同态加密技术的核心要求在于将系统当中用户上传的数据使用全同态加密算法进行加密, 然后密文可以被执行各项系统操作。

2.1 安全防护应用

由于加密技术是安全方案当中的首选技术, 其已经被广泛应用于金融市场和信息管理等领域当中, 这些领域一般拥有多个信息参与者, 参与者可能是可信方, 也可能是没有经过认证的不可信方, 而全同态加密技术正是在不可信方当中进行应用。

为了能够妥善保护好用户的隐私数据, 通常情况下用户会自行加密数据信息, 然后将这些加密后的信息上传至云存储当中, 如果要进行数据检索分析和处理时, 那么传统的加密方案可能无法适应此类要求, 在这种情况下就可以采用全同态加密算法完成数据检索。随着越来越多的企业开始使用云计算技术, 企业在云端存储的加密数据信息同样也会呈现出增长的趋势, 所以现阶段所使用的数据检索算法应完成检索信息的客观要求, 同时确保信息质量。实际上数据检索也有许多种不同的方法, 在云计算中加密信息的处理和加密信息的检索方法比较接近, 需要对待操作的关键数据进行加密并标记让其和普通的加密数据做好区分之后再上传至云端, 要严格根据用户的实际需求对密文数据展开处理, 最后将这部分数据重新传回给用户, 从而完成数据循环过程。现代用户都不希望泄露自己的私人

信息,因此使用该类加密算法对数据进行加密之后,就可以将加密的内容上传至服务器端,在不泄露身份信息的前提下完成数据交换^[2]。

2.2 物联网加密

物联网中同样存储着海量的信息。物联网发展本身要解决数据存储和数据信息等方面的问题。保存在物联网中的用户机密隐私数据不断增多的背景之下,无论是企业的商务资料还是用户的隐私信息等都有着泄露的风险,且某些非安全的应用程序端口和黑客的恶意攻击,也会导致数据加密出现系统化问题,让用户无法获取相应的保障服务。在此背景之下全同态加密技术可以解决数据操作和隐私保护的相关矛盾,用户可以直接将已经加密过的数据信息传递给服务商,服务商不需要对数据进行解密就可以直接进行操作,将结果返还给用户之后,从而完成数据循环过程,所获取的结果等同于对明文数据执行的操作。这样一来,用户在使用互联网时既能保护自己的隐私信息,又可以让服务器端处理加密过的数据,在一定程度上还可以增加互联网的用户群体数量。

2.3 加密云存储方案设计

一个完整的加密云存储方案,包括服务器端、云端和管理系统三个组成部分。用户在使用电脑或手机等设备进入系统后,就会产生相应的信息,客户端持续负责和云端之间的信息交互过程,当客户端完成对数据存储和数据加密之后,就能进一步实现对秘文数据的上传和下载。而云端则负责数据的基本存储工作,将用户的相关信息存储在资源池当中。对于用户而言,他们并不需要考虑数据究竟存储在哪个具体的地方,因为云存储系统会直接帮用户选择最佳的存储位置。管理系统则负责云端数据的综合管理完成数据检索等全同态操作步骤。

具体来看,用户会在客户端先将数据存入临时区域,再使用全同态加密模块,对数据加密后,将加密后的数据上传至云端,管理系统将云端所获取的数据按照相应的规则存储到云系统当中。如果用户需要使用这些数据,那么会向管理系统提出合理请求,管理系统接收到请求之后,从系统当中提取出数据下载至用户端内,然后在完成解密过程之后,最终将数据传递给用户。值得一提的是,如果用户需要进行数据检索或其他操作时,管理系统可以直接对云端数据进行操作而不影响数据的本身完整性,不仅节约了操作时间,同时也避免了信息泄露的可能性。前文提到加密云存储系统包括服务器端、云端和管理系统三个组成部分,每个部分有着对应的设计方法和职责^[3]。

服务器端即客户端方面,用户使用客户端能够完成数据的上传和下载,并且这一系统也是用户使用频率最高的系统,对于他们而言客户端的功能设计至关重要。如果能够在任何时间和任何区域进行系统访问,那么数据管理过程会更加简便。客户端系统当中,用户注册登录有关信息

之后,会将上传的文件存入临时存储区域,使用用户独有的加密密钥进行全同态加密,最终在加密过后上传至云端。如果要下载这些文件,那么用户会向云存储管理系统发出数据下载请求,客户端使用保存在本地的解密密钥进行解密,并将解密后的数据存入计算机系统当中,并且文件进入云端之前会自动调用解密模块或加密模块。

云端则是整个加密存储系统的核心组成部分,包括存储硬件设备和虚拟软件两个部分,其中存储硬件设备会借用大量的存储硬件来支持数据存储要求,而虚拟软件则可以将硬件设备虚拟为逻辑存储单元,提供给用户虚拟化的资源^[4]。

管理系统则用于进行客户端和云端之间的交互,并且维护用户的账号信息和云端资源管理等,按照资源存储信息的特性,方便定位数据位置,并将信息传递给用户。

在未来的研究工作当中,应该基于安全技术体系的要求做好更新和管理,着重从防护技术和审计监督技术角度进行系统构建,加强对外部风险的抵御能力,严格防止用户信息被窃取等类似问题的产生。这样一来也能让不同的用户对云存储平台更加信任。

3 结语

云计算技术在现代社会的各个领域当中扮演了重要的角色,而云存储必然成为今后数据存储的优先选择方案,基于网络安全层面展开研究工作具有明确的现实意义。对于云存储数据管理而言,数据的完整性、可用性与机密性、数据共享和数据迁移问题是重点环节。本次研究所分析的全同态加密算法是当前信息安全防护技术的一项案例,诸如此类的信息安全防护措施,可以为今后的用户隐私保护和信息安全管理提供关键的技术支持,也需要相关工作者做好技术保障。

参考文献:

- [1] 高洁.大数据时代下云存储信息安全的防护——评《云存储安全——大数据分析计算的基石》[J].中国安全生产科学技术,2019,15(10):191.
- [2] 张俊玲.大数据时代计算机网络信息安全与防护措施研究[J].信息技术与信息化,2019,229(04):135-137.
- [3] 张丽.基于大数据时代下的计算机网络信息安全与防护对策分析[J].数字通信世界,2020,185(05):42-43.
- [4] 席亚军.大数据时代下云技术在图书馆数据存储中的应用[J].农业图书情报学刊,2015,27(11):5-8.