DOI：10.16541/j.cnki.2095-8420.2018.50.153

浅析云环境下数据库安全的实现技术

陈芳

（宁夏职业技术学院软件学院，宁夏 银川）

摘　要：云技术在当前应用越来越广泛，发展速度也有着极大的提升，将私人数据外包于共有云数据库中，在极大程度上方便数据管理的同时也带来了数据安全和隐私隐患，这成为了影响云数据库发展的一个重要阻碍。对此，研究在云环境条件下数据库安全应当如何实现成为了如今亟待解决的重要问题。

关键词：云环境；数据库安全；数据安全保障

本文引用格式：陈芳 . 浅析云环境下数据库安全的实现技术 [J]. 教育现代化，2018，5（50）：356-357

云数据技术的高速发展为人们对计算机网络技术的使用提供了便利，因而当前越来越多的人们习惯于将个人数据上传到公有的云数据库系统进行管理。无论是企业还是个人，在使用云数据库系统时都是作为该系统的用户，其可以利用基础设施即服务提供的虚拟机来建立自己的数据库系统。云数据库是以云计算为基础的一种应用方式，因此其兼备了云计算技术的优点，但是我们也应该清晰的了解到，云数据库技术仍然存在着一系列的问题，诸如数据丢失、隐私泄露等问题屡见不鲜。如果想要让云数据库技术能够得到更好的应用，必须以此为依据对云数据库技术进行完善。

一　云数据库安全

（一）云计算安全

云计算安全是一个大范围的总称，其包括了与云计算有关的各个层面的安全，或存在的安全威胁的解决方案。云计算安全需要考虑的安全层面不仅包括传统意义上的网络安全，如有效防止服务攻击、域名系统攻击等，还需要考虑到物理层面的安全，如主机机房的消防安全、雷电天气防护等；存储层面的安全，如所储存数据的安全、加密防护措施、数据备份等；数据库层面的安全，如防止 SQL 注入攻击等；系统层面的安全，如虚拟机漏洞查补、操作系统存在漏洞的查补等。由此我们可以清楚的看出，所谓云计算安全并不是简单的某一层面的安全，而云数据库安全也仅仅是云计算安全的一个组成部分。

（二）云储存安全

所谓云储存是指以云计算技术为基础而衍生出来的数据云储存服务。为了保障云储存的安全，必须从如下几个方面来展开工作，包括：保障数据的隐秘性，避免数据泄露；保障数据的完整性，避免储存数据的丢失；保障数据的可用性，避免出现数据不能访问的问题发生。具体安全防护工作应当包括密文的检索工作、密钥的分发工作、对重复性密文的清理工作、对所储存数据完整性的审核工作、对所储存数据的加密工作等。

（三）云数据库安全

从上文所述可以看出，云数据库安全相较于云计算安全和云存储安全更加复杂，所包含的安全领域也更为广泛，因此目前对于云数据库安全的研究还并不足够完善。为了能够对云数据库安全进行研究，我们必须从云数据库的主要功能——数据安全领域进行分析。与云存储安全类似，云数据库安全需要满足数据库内储存数据的机密性、完整性和可用性。对于当前已有的云数据库而言，最为重要的便是数据的机密性，即保证所储存数据不被泄露或盗取。除此之外，想要完成云数据库的安全防护，不能指着眼于安全技术这一单一领域，而应该将云数据库所使用的技术、系统功能、运行特点等与安全技术相结合，从而使之能够更加紧密的贴合云数据库安全防护措施的实际应用 [1]。

二　云环境下数据库安全防护技术

随着云技术的不断发展，对于云计算领域的安全防护手段已经有了显著的进展，而云数据库的安全防护措施也同样取得了长足的进步。比如微软公司研发的 Always Encrypted 技术、Google 公司研发的 Encrypted Big Query 客户端等，都在一定程度上提高了云数据库对于数据的安全保护性能。可是我

作者简介：陈芳，女，江苏常州人，宁夏职业技术学院软件学院，教研室主任，副教授，硕士研究生。研究方向：计算机软件开发。

们也应当了解到，在这样广阔的发展前景背后，想要让云环境下数据库安全防护技术更加贴合实际需求、更加完善，当前还有许多技术问题需要我们去解决[2]。

（一） 密码学通用工具的特殊化

当前对加密语言的查询大多基于简单的密码学原语，如单向哈希函数、对称与非对称加密函数等。使用这类简单密码学语言的优点在于其可以提高密文查询的效率，让密文查询更加使用，用户操作得到简化。但是正由于加密语言的简单化，使得云数据库的安全性能上限无法再度提高。然而，如果为了提高数据库的安全性能而提高密码学原语的复杂程度，在目前的技术条件下也受到了相当的限制。如全同态加密、程序混淆等较为强大的密码学通用工具虽然可以提高密文的复杂程度，使之更难被破译，从而保证所存储数据的机密性。但是该类工具的实用性能较差，通用型构造相对较为复杂，为云数据库系统的建立提出了更多的要求。对此，需要对密码学通用工具的功能与实际需求以及技术水平进行协调，也就是所谓的特殊化。想要达到最好的安全性能时通用工具构造基本不能完成，则可以适当放宽对安全性能方面的需求，以提高该技术的实用性能[3]。

（二） 云数据库安全技术的实证化

由于云数据库的应用越来越广泛，技术人员对云数据库内数据内容的机密性保护已经做了大量的分析研究。通过分析可以看出，为了能够提高数据机密性安全防护措施的实用性，有时必须以牺牲部分安全性能作为代价。但需要考虑，在安全防护措施能够正式投入运用之后，其所具备的安全防护能力是否能够达到既定的要求？云数据库安全性能的主要评估手段便是外界攻击者获取到云数据库内部数据的便捷程度。攻击者获取数据越方便，则数据库的安全性能越差，反之亦然。因此在讨论云数据库安全防护性能时，必须站在外部攻击者的角度对其进行考量，并以此为实例对数据库的安全性进行证明。

（三） 提高安全技术与数据库技术的融合程度

当前云数据库系统最常使用的系统架构为CryptDB架构。主要原因是该架构为可信代理的系统架构，而且作为分离式架构在使用时无需对云数据库系统中的数据进行篡改。该架构在使用过程中与系统能够更好的相互兼容，进而可以更为方便的进行部署。可是该架构的应用仍然存在着较为明显的局限，即该架构之所以能够提高云数据库的安全性能主要是基于安全机制，而非云数据库技术。因此，该架构无法将安全技术与云数据库技术整合在一起，进而不能够从云数据库的层面来对数据库的安全性能进行改进和完善。为了改变这一情况，我们必须将安全技术与数据库系统进行融合，并将其作为未来研究的主要方向。在此面临的问题主要包括如下几个方面：首先，我们应当使用怎样的系统架构才能够将可信硬件进行有效整合？虽然已经有技术人员将FPGA融合了Cipherbase架构中，但是并没有能够研究清楚数据库架构应当怎样才能够兼备数据库系统和安全技术两者的优点。其次，云数据库系统的密文查询功能应当怎样添加？当前大多使用用户自定义函数对数据库进行扩展，但是该方式限制了用户与第三方之间的交流，如果强行要提供三方交互功能则极大程度上提高了云数据库建设的成本。最后，当采用安全性能更加优异的技术时，其对于整个云数据库系统的运行负荷也会进一步加大，在进行云环境下数据库安全的技术实现工作时必须有所取舍，进行协调[4]。

三 结论

随着云计算技术应用愈发广泛，以云环境为基础的数据库系统成为了当前人们进行数据存储的首选方案。但是云数据库的安全问题在没有得到充分解决时，是否可以将其作为一种可靠的数据保存手段仍然有待商榷。本文从云数据库的安全功能出发，对未来云数据库安全技术提出了探索和展望，并指出了一些研究方向。希望通过本文可以对云数据库安全性能的提升起到一定的促进作用，让云数据库系统在未来能够得到更加广泛的应用。

参考文献

[1] 林闯，苏文博，孟坤等．云计算安全：架构、机制与模型评价[J]．计算机学报，2013,36(9):1765-1784.DOI:10.3724/SP.J.1016.2013.01765.

[2] 刘冬兰，史方芳，刘新等．大数据环境下云数据库安全防护方法研究[J]．山东电力技术，2017,44(6):41-44,48.

[3] 洪澄．云数据库安全关键技术研究[D]．中国科学院研究生院，2012.

[4] 高明贺，申朝红，丁琪等．基于云计算服务的数据库安全与发展研究[J]．硅谷，2012,(8):80-81.DOI:10.3969/j.issn.1671-7597.2012.08.075.