云环境下数据库机密性保护技术研究综述

苏　艳
文华学院，中国·湖北 武汉 430074

【摘　要】最近几年里,云计算以较快的速度不断发展,公有云数据库系统为企业和个人提供各种数据管理服务。但是,由于考虑到数据安全和隐私保护,云数据库的广泛应用在很大程度上受到限制。对于云数据库系统,安全需求越来越强烈,因此,对云数据库的机密性保护进行研究具有紧迫性,也是当前学术界重要的研究课题。本综述针对云数据库机密性保护提出五级安全模型,这样即使相关的安全技术是跨领域的也能进行统一讨论;接着,对3级-5级机密性威胁的保护技术进行总结和分析;并在此基础上,对当前最具先进性的安全云数据库系统进行介绍,并进行比较;最后,对后期的研究趋势做进一步展望,并指出相关的研究方向,希望在经过本文的分析之后,能为后期的研究学者提供更多有价值的参考。

【关键词】云计算；数据库系统；数据安全；密文查询；可信硬件

引言

最近几年里,云计算的发展速度是非常快的,公有云数据库系统为企业和个人提供各种数据管理服务。

用户对虚拟机可以进行租用,很好的实现数据资源的共享,成本也是进行摊销。同时,可以直接使用云服务商所提供的各种服务以及数据库,比如谷歌的Cloud sQL4就是很好的一例.采用上述方式即可实现云数据外包处理,并对云数据库系统进行充分有效的利用,云计算各种可靠、便捷、安全的优点,所有的用户都能享受到。

1　五级安全模型

1.1参与者

对于五级安全模型,三大参与者分别是用户、管理员、攻击者。对于用户,多数会采用数据外包服务,主要的目的是为了获得廉价而又高效的数据管理服务,而且数据的安全性可以得到很好的保障。管理员换句话也就是云服务的提供商,各种与云数据库系统相关的安装、配置等各类工作都由管理员进行负责,并对系统的安全性起到有效的保障作用。当遇到各种攻击时,就会及时采取措施进行防范,避免受到影响。对于攻击者,其来源具有不确定性,内部和外部的都有,也有可能是管理员。因此,攻击者可能享有一定的特权。前面已经提到,本文研究的重点是机密性。因此,在假设安全模型的时候,攻击者是消极的,他们会将各种数据进行盗取,这也可以说是他们的一种兴趣。各种数据的篡改破坏等属于恶意行为,本文对其不进行探讨[1]。

1.2系统

整个系统的构架是客户端-服务器式,借助数据库客户端之后,查询、指令等用户都可以向数据库系统进行发送，作描述时，将数据库系统看作是具有抽象的关系型数据库管理系统,包含查询和存储两个引擎,查询引擎管理内存数据,存储引擎则管理外存数据。特别要引起注意的是,在该系统中，包括硬件、软件等都是不可信的。但是,客户端则具有可信性,因为其是由用户进行完全控制的。

2　密文查询(3级)

密文查询,也就是一种数据库查询技术,建立在密码学方法的基础上。所使用的数据加密方法在经过特殊的设计之后,在不需要经过解密的情况下就能实现对密文的有效处理。由于数据不管是内存还是外存始终都是处于加密状态,因此,在很大程度上将2级机密性风险和3级机密性风险都降低。

数据库查询,其组成部分主要是选择、投影、连接等各种操作子,种类有限而且定义良好。以投影数据库操作来进行举例,其注重的只是所记录的字段。因此,要想执行投影操作,直接通过密文就可以。但是,在进行相关的操作之前,需要理解字段内容,确定好所选择的操作是否是合理的。在遇到连接操作的情况下,需要正确判断两条记录的匹配性。在遇到聚集操作的情况下,求和运算也是要做的。

3　可信硬件(4级)

对于可信硬件，其功能是非常多的，使用该硬件之后，会在很大程度上增强安全性，硬件内部的存储资源也会很好的进行隔离，以保证攻击者不能进行相关的窥探和篡改。因此,相关的密文如果被可信硬件接收，就可以很容易的进行解密处理，不会影响到机密性。硬件中的各个功能都能得到很好的保护。

站在逻辑的角度进行考虑,通过可信硬件,用户能享受到各种服务,换句话来说,可信硬件也就是用户的一种延伸。当用户数据具有一定的敏感性时,通过可信硬件可以进行很好的数据存储,各种程序的运行也会更具安全性。站在物理的角度进行考虑,可信硬件是服务器组件的一种,和服务器之间是可以直接相连的,通信延迟低、带宽高,而且具有共享性,数据之间是可以进行共享的,多个租户可以使用同一个可信硬件,并对成本进行摊销即可。由于这两个方面的特点,在对各种云安全问题进行解决时,可信硬件都具有较高的吸引力[2]。

但是,可信硬件是不能取代密文查询技术的,可信硬件和密文查询技术之间形成一种很好的互补关系,但是不会相互排斥。站在安全角度进行考虑,相比密文查询技术,可信硬件在安全保护方面更具有全面性。包括数据库中的数据、数据库执行状态的机密性、完整性都能进行很好的保护。但是,对于可信硬件,资源存储、计算等各方面的能力都存在不足,在进行数据查询时,如果只用可信硬件,而对不可信硬件不能有效利用,这样一来,要想实现整体性能最优化是非常困难的。

4　结束语

最近几年里,由于云计算的快速发展,公有云数据库系统为企业和个人提供各种数据管理服务。但是,由于考虑到数据安全和隐私保护,云数据库的广泛应用在很大程度上受到限制。对于云数据库系统,安全需求越来越强烈。本文首先对五级安全模型进行相关的介绍,这样就可以对数据进行很好的保护，这样一来,等研究中所涉及到的各种安全技术,即使是跨领域、跨问题,都能放在一起进行讨论，很具有统一性。接着,对3级-5级机密性威胁的保护技术做相关的总结和分析工作;在此基础上,对当前最具先进性的安全云数据库系统进行介绍和比较;在此基础上,对当前最具先进性的安全云数据库系统进行介绍和比较;最后,对后期的研究趋势做进一步展望,并指出相关的研究方向。

参考文献:

[1]王勉.云环境下数据库机密性保护技术研究综述[J].时代农机,2017,44(12):68.

[2]何淑娟.云环境下数据库机密性保护技术研究综述[J].科技经济市场,2017(12):176-178.

作者简介: 苏艳（1983.03-）女，湖北钟祥，研究生，研究方向：数据库、Java。