分　数：	
评卷人：	

華中科技大學

研究生（数据中心技术）课程论文（报告）

题 目：云计算数据安全与隐私保护研究综述

学　　号 M202173868

姓　　名 何孝发

专　　业 电子信息

课程指导教师 施展 童薇

院（系、所） 计算机科学与技术学院

2022 年 1 月 7 日

云计算数据安全与隐私保护研究综述

何孝发 M202173868

摘　要　云计算作为一种新型的计算方式，已经受到了学术界和工业界的广泛认可。基于资源虚拟化技术，云平台能够以按需使用、按使用量收费的方式为用户提供数据存储、计算等服务。越来越多的企业和组织选择云平台来部署商业和科研应用。云服务提供商为云服务统一包装，极大简化了云服务的获取，促使越来越多的个人购买云服务，享受云计算带来的便利。用户数量的急剧增加，给云计算的安全性能提出了更高的要求，其中用户数据安全和隐私保护就是最重要的问题之一。本文首先首先给出了现有云计算模型，调研和分析云数据安全保护中存在的威胁。现在的云计算系统通常采用密码学技术保护数据安全和隐私。当前，云环境中较为有效的数据安全和隐私保护技术包括[4]：基于属性的加密、同态加密技术、代理重加密、零知识证明技术、多方密钥协商、群签名技术等。在此基础上，本文从云数据安全的访问控制、密钥协商、安全审计 3 个方面出发，对国内外云数据安全保护方案的最新研究成果进行分析概括。基于密码技术的数据安全查询、分享以及差分隐私保护是国内外当前的研究热点。其次，针对现有云数据安全保护方案存在访问控制过程中用户隐私易被泄露、密钥生成过程中开销难以控制、审计过程中动态操作效率低下、错误恢复较难实现、数据共享过程中恶意用户难以追踪等问题，进行调查研究．最后，探讨云数据安全保护当前面临的挑战和未来研究方向，以期推动更加完善的云数据保护体系的建立。

关键词　云计算、数据安全、隐私保护、密码技术、安全审计

Overview of cloud computing data security and privacy protection

Xiaofa He

Abstract　As a new computing method, cloud computing has been widely recognized by academia and industry. Based on resource virtualization technology, the cloud platform can provide users with data storage, computing and other services by using on-demand and charging according to usage. More and more enterprises and organizations choose cloud platform to deploy business and scientific research applications. Cloud service providers uniformly package cloud services, which greatly simplifies the acquisition of cloud services, and promotes more and more individuals to buy cloud services and enjoy the convenience brought by cloud computing. The rapid increase in the number of users puts forward higher requirements for the security performance of cloud computing, in which user data security and privacy protection are one of the most important issues. Firstly, this paper gives the existing cloud computing model, investigates and analyzes the threats in cloud data security protection. Today's cloud computing systems usually use cryptography technology to protect data security and privacy. At present, the more effective data security and privacy protection technologies in cloud environment include attribute based encryption, homomorphic encryption technology, proxy re encryption, zero knowledge proof technology, multi-party key agreement, group signature technology and so on. On this basis, this paper analyzes and summarizes the latest research results of cloud data security protection schemes at home and abroad from three aspects: access control, key agreement and security audit. Data security query, sharing and differential privacy protection based on cryptography are the current research hotspots at home and abroad. Secondly, the existing cloud data security protection schemes have some problems, such as easy disclosure of user privacy in the process of access control, difficult control of overhead in the process of key generation, low efficiency of dynamic operation in the audit process, difficult implementation of error recovery, and difficult tracking of malicious users in the process of data sharing. Finally, This paper discusses the current challenges and future research direction of cloud data security protection, in order to promote the establishment of a more perfect cloud data protection system.

Key words Cloud computing, data security, privacy protection, cryptography, security audit

1、引言

云 计 算（Cloud Computing）是分布式计算、并行计算、效用计算、虚拟化、负载均衡等传统计算技术和网络技术发展融合的产物。云计算是以按需付费的模式，通过互联网提供可配置计算资源共享池（资源包括网络、服务器、存储、应用软件、服务等）。总的来说，云计算可以概括为一个三层的体系架构：基础设置层（Infrastructure as a Service, IaaS）、平台层（Platform as a Service，PaaS）和软件服务层（Software as a Service，SaaS）。IaaS 层主要包括云计算基础架构及其硬件设备；PaaS 层可以看作云计算的操作系统，是云平台和应用软件的稳定良好运行的基础平台；SaaS 层提供软件服务，是一种基于互联网的云平台应用软件付费使用的新模式。

图 1.云计算体系架构

在使用云计算服务时，用户最为关心和担扰的问题是数据的安全和隐私是否得到了很好保护 . 当用户将数据外包给云服务提供商后，便失去了对数据的物理控制，数据的安全和隐私依赖于云服务提供商对数据采取的安全防护措施 . 如果安全措施被外部黑客或者云服务提供商内部人员破坏，用户的敏感数据有可能被泄露，数据的安全和隐私将被严重破坏。

在云平台上的数据的生存周期经历存储、使用、共享、归档直至最终销毁 6 个阶段. 在这过程中，数据安全主要面临数据泄露、数据丢失、数据损坏、密钥攻击等威胁。根据 云计算 安全公司 Elastica 的最新研究数据显示，云计算 允许移动员工方便地存储信息，并让他们可以广泛地与同事共享信息，但很多人没有考虑将敏感数据放在云计算中的安全性，这将产生数据泄露的风险。云计算的普及，让一些不法分子看到了有利可图，他们不满足于窃取具体数据，还热衷于窃取计算能力，即窃取数据加密的方式。他们专门针对企业公共云环境的加密器进行攻击，因为公共云环境是弹性计算环境。许多组织还没有成熟的云计算安全计划，使其云端容易受到攻击。云计算安全平台的不成熟以及比特币和以太网等加密货币的日益普及，这推动了云中加密劫持的兴起。这些因素都给云计算中的数据安全和用户隐私造成了很大的威胁。

云数据安全保护的安全需求以及为其提供保障的密码原语可概括如表 1 所示[4]。首先，不可伪造和合法访问指非法用户无法通过身份认证进而访问云上数据，该属性是云数据安全保护的关键环节。其次，数据的完整性和正确性是指外包存储在云上的数据没有出现错误，与用户上传的数据一致且完整，完整性和正确性是云服务发展的基础同时也是用户使用云的重要前提。再次，数据机密性和隐私保护是指存储数据安全，攻击者或者好奇的云在没有密钥的情况下无法获知数据所包含任何有价值信息，该属性是云数据安全的重要特征. 最后，隐私保护是指用户身份和数据隐私安全，目前，隐私保护越来越受到人们关注，同时大数据环境下驱动的各领域多方协作可极大推进科技的发展，但协作过程中的隐私保护是各方参与协作的必要前提，因此隐私保护已成为云进一步发展的关键瓶颈。

表 1 数据安全需求及相应密码原语

安全需求	功能	密码原语/协议
不可伪造性	用户身份无法伪造	签名、零知识证明
合法访问	非法用户无法获取数据	属性加密、密钥管理
数据完整性	存储数据完整	审计协议
数据正确性	存储数据正确	审计协议

数据机密性	存储数据安全	加密、密钥管理
隐私保护	确保身份/数据隐私	加密、同态存储

针对上述安全需求，密码学中的加密、签名、认证、密钥协商等密码原语作为保证数据机密性、身份合法性、数据完整性的技术具有重要作用．当前，云环境中较为有效的数据安全和隐私保护技术包括：基于属性的加密、同态加密技术、代理重加密、零知识证明技术、多方密钥协商、群签名技术等。

2. 加密技术原理

加密技术主要分为两种，一种是对称加密，一种是非对称加密[7]。对称加密技术使用同一个密钥对数据进行加密和解密，具有加密速度快、效率高等特点。对称加密 DES（Data Encryption Standard）算法的运算流程如图 2.

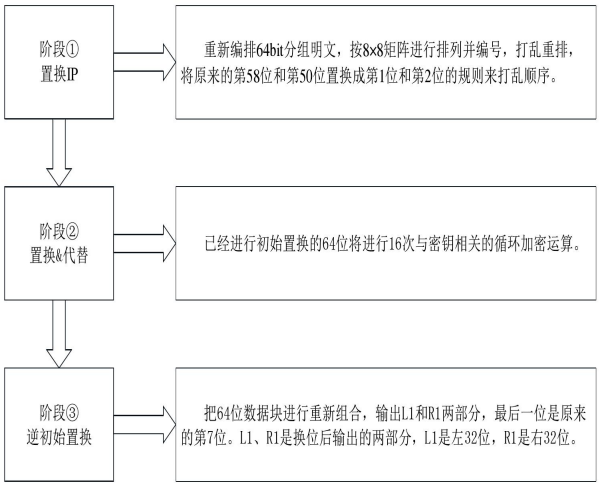


图 2. 对称加密流程

非对称加密算法中加密和解密的密钥是不同的，且两个密钥无法同过其中一个推导出另一个。RSA 算法是非对称加密最常用的算法，私钥存储在本地，传输的是密文，即使密文被截取了，按现有的手段一般很难破解。非对称加密在信息交换中的流程如图 3。公钥和私钥由可信的第三方认证中心生成，然后提供给请求访问的用户，可用于数据加密和数据认证[2]。

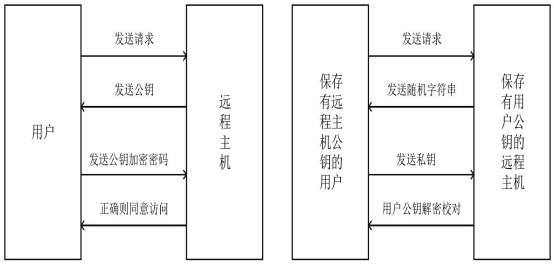


图 3. 非对称加密

云计算中数据安全保护涉及到的密码学原理主要包括：秘密共享、多方密钥协商、数据审计和代理重加密。

2.1. 秘密共享

秘密共享是一种将秘密分割的重要密码学原语．在秘密共享技术中，秘密持有者根据需求选取门限值 t 并基于特定技术将秘密值 S 分割为 n 个子秘密份额 $\{s1, s2, s3, \cdots, sn\}$。目前，用于成子秘密份额的技术主要包括一元 N 次多项式、中国剩余定理、多维向量空间等．当且仅当合作的用户数量大于门限值 t 时，恢复出秘密值 S．秘密共享包括 4 个算法：1）初始化．输入安全参数 l、门限值 t．输出子秘密份额生成函数 $Gen()$ 和秘密恢复函数 $\mathrm{Re}c()$。 2）秘密分割．输入秘密值 S、门限值 t，参与秘密共享的人数 n，子秘密份额生成函数 $Gen()$．输出 n 个子秘密份额 $\{s1, s2, s3, \cdots, sn\}$．3）秘密份额分发．在安全信道下或采用安全加密算法 $Enc()$ 将秘密份额分发给 n 个参与者。 4）秘密恢复．输入秘密份额 $\{s1, s2, s3, \cdots, sm\}$， $m \geq t$，秘密恢复函数 $\mathrm{Re}c()$。输出秘密值 S。

秘密共享的基本安全需求包括 2 方面：正确性和隐私性．正确性要求具有高效的算法能够根据满足门限要求的秘密份额 $\{s1, s2, s3, \cdots, sm\}$，$m \geq t$ 恢复出原始秘密值 S；隐私性要求任何不满足门限 t 要求的秘密份额组合 $\{s1, s2, s3, \cdots, sm\}$，$m < t$ 都无法恢复出秘密值 S，即秘密值 S 和任何不满足门限 t 要求的秘密份额组合是相互独立的。

2.2 多方密钥协商

多方密钥协商是保证公开网络下多方安全交互的基础密码原语，多方密钥协商主要包括 3 个算法： 1）初始化．输出系统安全参数 l，用户数量 n．输出子密钥生成函数 $SubGen()$，共享密钥生成函数 $SessionGen()$。 2）子密钥生成．每个用户选取随机数 r 和用户私钥 sk，根据子密钥生成函数 $SubGen()$ 计算子密钥 ki．3）共享

密钥生成．输入n个用户的子密钥，共享密钥生成函数$SessionGen()$，输出n个用户的共享密钥K．多方密钥协商的基本安全需求要求参与用户外的任何人都无法获知生成的共享密钥K。

2.3 数据审计

数据审计方案是保障云存储数据完整性的重要密码学原语。数据审计方案主要包括4个算法：1）初始化。输出系统安全参数l。输出用户公私钥对(pk,sk)。2）验证标签生成。输入公私钥对(pk,sk)和文件块f。输出验证标签Tf。3）证明生成。输入挑战chal，文件公钥pk，文件块f及其对应的验证标签Tf。输出被挑战块的持有性证明P． 4）证明验证。输入公私钥对(pk,sk)，挑战chal和证明P。数据审计方案的安全性要求以极大的概率检测出外包数据的损坏或丢失。

2.4 代理重加密

代理重加密是云环境下保证数据共享安全的有效密码原语。本质上来说，代理重加密是实现云环境下密文转换的一种技术，即将用户A可解密的加密数据转换成用户B可解密的加密数据。该特性可有效支持云环境用户动态变化情况下的高效密文更新．代理重加密包括5个算法：1）初始化．输出系统安全参数l。输出用户公私钥对(pk,sk)。2）初始加密．用户持有者A采用加密函数加密消息M，生成初始密文$C=Enc(M)$．3）转换密钥生成．用户持有者根据其意愿分享数据的接收方生成转换密钥$KA-B$．并将初始密文和转换密钥提交给代理．4）重加密．代理根据初始密文C和转换密钥$KA-B$对密文进行转换，生成转换密文CT。5）解密．符合用户A授权的用户在收到经过代理转换的密文后使用自己的解密密钥解密出明文M．代理重加密的安全性要求代理在转换的过程中无法获知明文的任何信息．

3 研究进展

当前，国内外的研究学者们已对各类云数据安全和隐私保护方案展开研究，取得了一系列研究成果。研究成果主要集中在访问控制、密钥协商、安全审计等方面

3.1 访问控制

访问控制机制可通过预先规定好的访问控制策略，来限制数据请求者行为，使得授权的合法用户可对数据进行访问，非授权用户被拒绝访问，通过合理的访问控制策略限制用户访问能力和范围，使数据资源被合法利用，对数据加强访问控制是保障数据安全的有效手段。合适的访问控制机制对提高云计算系统的安全性至关重要，是云环境下用户访问数据的重要前提，众多专家学者正在围绕访问控制展开研究，探寻适合当前云计算发展的方案。当前主要有基于身份认证的访问控制和基于属性加密的访问控制[6]。

3.1.1 基于身份认证的访问控制

基于身份认证的访问控制机制是在数据加密基础上引入一个可信的第三方认证中心，将服务器本身标识为证书颁发机构，对用户身份进行验证，通过身份认证确保公钥的正确性和安全性。数据属主利用对称加密把数据加密后发送到服务器，获得该数据属主的一个或多个私钥，通过数字签名来对尝试访问的用户进行身份验证任何想要访问数据的用户都需要取得可信第三方的证书，对该证书进行身份验证来确保该用户的真实身份。采用公钥证书来管理用户公钥密码，公钥和私钥可以由用户生成，或者是通过一个可靠的认证中心标识用户信息（例如用户的姓名、年龄、信用值）来生成，再分发给用户，为公钥加密后的数据安全性提供了保障，提供身份认证机制的云服务商能验证用户身份，对数据的安全性更有保障。

身份认证中使用的加密方式通常包括可重用密码、一次性密码、质询响应密码和组合密码。将用户身份作为标识公开，管理更加方便，相对而言基于身份的密码体制私钥的维护与管理比较简单，可以进行简单快捷的保密通信。使用基于身份的密码体制对用户进行认证时，系统为保障安全性要建立专门的通道向不同用户分发私钥，缺点在于如果私钥中心遭受攻击，会直接影响到用户身份信息的安全性能，这种访问控制没有全然解决当前云环境存在的数据安全问题，无法实现细粒度访问，在密文更新时权限撤销方面还存在欠缺。

3.1.2 基于属性加密的访问控制

当下云环境访问控制更多的是基于属性加密，是保护用户数据安全的主要方法之一，在基于角色

的访问控制机制中，将角色与权限绑定修改为属性与权限相结合，只有属性满足控制策略时，才可以访问数据资源，由此专家们提出了属性加密方案。与传统的访问控制方案相比较，基于属性加密的访问控制方案可以改善访问控制机制中不够细粒度的问题，符合云环境下一对多的要求。通过属性与权限的结合，用户可以根据自身属性获得相应的密钥，解密、读取与该属性相关的数据。对于数据属主来说，数据上云之后希望自己掌控数据，自己指定可访问数据的用户，根据这些属性对数据加密，能解密的用户即可访问，保障数据在云端发挥最大价值。

在 CP-ABE(ciphertext Policy Attribute Based Encryption) 密文策略属性基加密方案中，用户解密密钥由用户的属性集合进行描述，数据密文则使用数据属主定义的访问结构进行描述，加密者根据数据文件的机密性对数据制定不同的访问结构，密文属性匹配访问控制属性，抗合谋攻击。如图 4 所示，用户从云服务提供商处下载加密过的数据，只需要符合相应属性条件便可解密，简化操作，减少运算量，比其它方案更加灵活，适合用户众多、数据量庞大的云环境。尽管 CP-ABE 方案已经比其他方案更适合云环境，但是仍然存在一些遗留问题没有解决，比如属性撤销问题、密钥泄露问题。

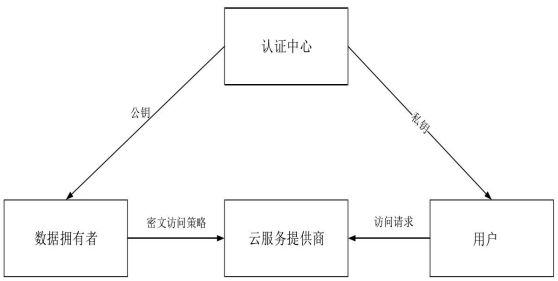


图 4.基于属性加密的访问控制

3.2 密钥协商

密钥的协商协议是当前云计算环境下普遍采用的保证网络 安全的加密模式，密钥协商是指双方或多方实体通过协商，建 立的一种密钥加密方式，而密钥协商协议是指对每个用户密钥 参数的计算方法，当前云计算环境下通常使用的协议是 IKE 协议。密钥协商协议的实施过程为：首先用户与云计算平台产生相互服务的密钥，即密钥协商，再通过密码技术也就是密钥 协议对密钥进行传输，传输过程中使用一定的加密技术将密钥 转换成相应代码，云端服务方接收代码，并破译形成服务方密钥。当前的应用主要有双方密钥协商协议和群密钥协商协议。

3.2.1 双方密钥协商协议

双方会话密钥协商协议，要求通信双方在公开网络中传递信息，协商出会话密钥。一般基于双线性对的密钥协商协议交互轮数和信息量较小，具有较高的效率和很好的安全性，并且不需要建立和维护代价高昂的公钥基础设施，易于实现和应用;而不基于双线性对的协议计算量小，在资源受限的网络中尤其是计算资源受限的网络中比较适用，但安全性相对而言较弱。

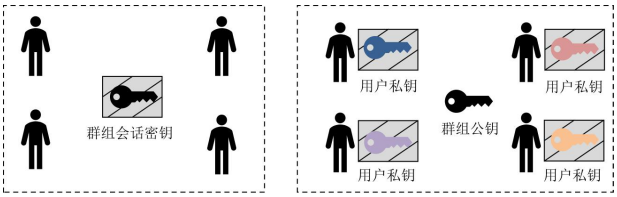
Diffie-Hellman 协议是最早的一轮双方密钥协商协议，该协议的安全性直接作为密码学中的标准假设性问题，即 CDH(Computational Diffie-Hellman) 问题和 DDH(Decisional Diffie-Hellman)问题。但是该协议只能抵抗被动攻击，并不能有效地抵抗主动攻击，一旦攻击者具有篡改双方的交换信息的能力，则没有相应的认证机制来避免或者检测到该情况，协议设计过于简单。为了避免中间人攻击这一漏洞，近年来，许多研究者根据 DH 协议设计了认证密钥协商协议来保证除了合法参与者外其他人无法获取本次密钥协商相关信息。2010 年，Cao 等利用基于身份思想提出一种不使用双线性映射的认证密钥协商协议，在密钥提取阶段，通信双方会相互验证长期私钥的有效性，进而互相验证双方的身份以防攻击者的主动攻击。在 cNR-mBR游戏 (Computational No Reveal-modified Bellare-Rogaway game)模型下基于 CDH 假设证明协议的安全性，能够抵抗密钥泄露伪装攻击，达到完美前向安全性和主密钥前向安全性。并且该协议只需要一轮的信息交换，计算量较少。但该模型是一种简化的 mBR(Modified Bellare-Rogaway model)模型，并不能进行Reveal查询，因此安全性较弱。Islam 等指出 Cao 等提出的协议既不能抵挡密钥偏移攻击，可能产生错误的会话密钥；也不能够抵挡已知特定会话暂时信息攻击。针对缺点改进了 Cao 等的协议，采用消息认证码 MAC 来抵抗密钥值偏移攻击;加入新的参数，利用 CDH 问题来抵抗已知特定会话暂时消息攻击。同时，该协议与 Cao 等的协议相比计算量

更少，但是 Islam 协议需要会话参与双方进行信息交互，并且 Islam 等并没有形式化的对协议进行安全性证明。

3.2.2 群密钥协商协议

群组密钥协商协议能够使参与会话的用户在一个安全的信道中进行通信，保证交互信息的机密性、真实性认证和完整性。群组密钥协商协议可以分为对称群组密钥协商协议和非对称群组密钥协商协议。对称群组密钥协商协议就是组内的用户通过协商，计算出一个相同的会话密钥来进行消息的加解密;而非对称群组密钥协商协议采用公钥密码体制，参与者协商出个加密密钥，各自拥有的解密密钥可以对消息进行解密。对称群组会话密钥协商协议只允许组内成员间广播信息，非对称协议允许构建广播加密系统，群组成员协商出公钥，保留各自的私钥，这样任何知道协商出的公钥的用户都可以发送消息。完成协商过程，基于随机预言模型在 k-BDHE 假设下可证安全。

2016 年，陈勇等人基于零知识证明技术，设计了一种可否认群密钥协商协议，实现了 密钥协商过程中的隐私保护. Teng 等人在密钥协商协议中引入矩阵论，有效支持协商过程中用户动态变化问题，然而，该协议交互信息量较多，计算 和 通 信开 销 较 大. 方 亮 等 人基于 秘密共享技术，提出了无需在线可信第三方的密钥协商协 议. 然而，该协议需要较大的计算和通信开销. 邓淑华等人基于 ElGamal 体制，提出了一种安全组播密钥管理方案，提升了组密钥管理的可扩展性，然而，该协议基于集中式模型，存在单点失效以及成员贡献失衡问 题. 为了平衡多方密钥协商协议所需的通信 开 销、交互次数和协议功能性. 2009 年，Wu 等人在欧密 会 上 提出了一 种 非 对 称 群 组 密 钥 协商协议(asymmetric group key agreement, ASGKA)，平衡了非交互式密钥协商难以实现以及交互式密钥协商轮数偏高，安全性不足等问题. 该协议基于可聚合签名广播密码原语实现了多方单轮群组密钥协商，该协议执行效率高且在 n-BDHE(n-bilinear diffice-hellman exponention, n-BDHE)假设下是 可证明安全的. ASGKA 密钥协商模型和传统一多方密钥协商模型如图 5 所示，在传统多方密钥协商协议中，每个群组成 员 协商 完 成 后 将 生成一个群组会话密钥，该密钥需要保密以保证后续通信安全，ASGKA 协议中，协商完成后每个群组成员将生成各自的用户私钥（群组私钥）和一个群组公钥，每个成员所持有的不相同的用户私钥可以解密群组公钥加密的信息. ASGKA 协议 相 较于传统群组密钥协商协议具备无需 管 理 员 参 与（dealer-free）、自 认 证（keyself-confirmation）、恶意 参 与 方 识 别（identification of disruptive principals)等优势. 然而，通过该协议得到的群组公私钥需要基于公钥加密实现安全通信，其运行效率将低于传统群组密钥协商得到的对称密钥. 此外，该协 议 具 备 密 钥同 态 的 特 性，若 存 在 恶 意参与者，则 会导 致 协 议 受 到 共 谋 攻 击. 谢 涛 等 人研究了 ASGKA 协议中的共谋攻击问题，定义了非对称群组密钥交换的叛逆追踪性，并严格证明了具备密钥同态性质的非对称密钥协商协议中合谋者构成的集合满足非模糊性导致合谋者是不可追踪的.



(a) 传统密钥协商模型　(b) ASGKA密钥协商模型

图 5.ASGKA 密钥协商模型和传统密钥协商模型

3.3 安全审计

传统的 I T 安全审计技术已经非常成熟，安全审计是对计算机系统和计算机网络中的各种信息进行实时采集、分析，以查证是否发生安全事件的一种安全技术。尽管传统 IT 安全审计和云计算安全审计在定义和安全观念上存在相同的观点，但是它并不能直接迁移至云计算环境。云 计 算 环 境特 有的数据和服务外包、虚拟化、多租户和跨域共享等特征都给安全审计带来了一些非常具有挑战性的难题。云计算中的安全审计主要有日志审计、云存储审计和配置审计[1]。

3.3.1 日志审计

日志在信息系统运行管理中发挥着重要的作用，尤 其 在安全领域，日志记录了用户涉及安全操作的所有活动的过程，以备有违反安全规则的事件发生后能够有效地追查事件发生的时间、地点及过程，是安全事件追溯、取证分析的重要依据。但

是当前关于云计算日志审计的研究成果比较少，因为云服务提供商的内部操作细节并不为用户所知，并且其限制提供日志记录和实施监控数据，审计日志所能获得的部分审计日志不足以对云计算安全审计进行全面的研究。

Shetty 等人提出了一种审计恶意云租户的技术，通过 IP 定位和路由器 IP 分析技术，结合网络度量（平均时延、标准方差时延、跳数）和社会特征（城市人口密度）等因素能够确定云租户的真实地理位置。Shetty 等人开了基于机器学习和控制理论模型的数据挖掘技术，能够自适应地调整检测阈值，实时分析云日志以发现云环境的异常事件。Wang 等人设计并实现了一个云数据中心审计系统 CDCAS（Cloud DataCenter Auditing System)，能够满足云数据中心可扩展性和有效性的需求。这个系统中设计了一个分布式自治代理模型来收集各种多源异构日志，利用基于特征的方法和相关性分析算法比较审计日志和预配置或预定义的事件模式，从而发现非法行为，提取攻击、误用和错误事件。最后在真实的和仿真环境中评估、证实了该系统的有效性。

3.3.2 云存储审计

云存储审计是指数据拥有者验证存储在云中数据的完整性和可用性的过程。为了提供可信、公平的审计结果，使数据所有者和云服务提供商都信服，第三方审计是比较合适的选择。第三方审计方案的设计面临诸多挑战：1）支持动态审计，即审计方案支持数据动态更新操作；2）支持批量审计，即审计方案支持多个审计任务进行合并处理，以提高审计效率；3）支持盲审计，即数据需要对第三方审计保密。

Ateniese 等人首次提出了“可证明数据持有”PDP 方案，该方案只支持静态审计，将 RSA 密码与同态可验证标签结合起来。所有者先将数据分成块并加密，然后为每个数据块计算标签，并与加密后的数据一起保存在服务器上。审计者向服务器发出对数据块子集的质询而不需要检索整个文件。在后续的工作中，Ateniese 又设计了一种部分动态可证明（DPDP）的数据持有协议，在开始阶段预先计算一些元数据，其中每个元数据对应一个更新，其缺点是更新和验证次数有限且是预先固定的，不支持数据插入操作。由于采用耗时的 RSA 算法，PDP 方案中数据完整性证据的生成和验证效率很低。同年，Juels 等人提出了“检索的证明”POR 方案，在云存储服务器中利用抽样和纠错码来确保数据文件的持有性和可检索性，该方案只支持有限次的验证。这两种方案中验证数据完整性的算法基本相同，主要区别是 POR 方案在验证数据完整性的基础上加入了纠错码技术，以便恢复原始数据。Wang 等人采用双线性配对技术基于离散对数问题提出了一种支持第三方验证的 PDP 协议，该协议利用随机屏蔽方法实现了盲审计，并利用同态标签的思想将数据标签聚合实现了批量审计。Wang 在另一个研究中基于默克尔哈希树构造了一个允许数据动态变化的第三方审计 POR 协议，同时基于纠错码支持数据动态更新。Zhu 等人基于双线性配对技术和索引表设计了一种支持数据动态变化的第三方审计 PDP 协议，该协议允许无限次验证并支持盲审计。He 和 Yang 等分别提出了支持多所有者多云服务器的批量审计方法，这些批量审计方法都是假设数据所有者只有一份文件。之后，He 等人又提出了一种聚合盲审计方法，利用双线性对映射的性质在云端服务器将数据证据和标签证据加密后再合并，实现审计者在不知数据内容的情况下进行盲审计。在此基础上设计高效的索引机制来支持数据更新，同时实现了动态审计。针对多个审计请求，设计将不同的证据聚合的方法，以支持对多所有者多云服务器多文件的批量审计。表 2 从动态审计、批量审计、盲审计等方面对上述方案进行了对比分析。可以看出，现有方案或多或少存在一些问题：有些方案不支持盲审计，有些方案不支持动态审计，而有些方案不支持多文件批量审计；计算开销和通信开销过高。但鉴于 POR 方案具有数据恢复功能，比 PDP 方案具有更高的实用价值，因此设计支持盲审计、动态审计和批量审计的 POR 协议是云存储审计研究的一个重要方向。

表 2 存储审计中各方案对比分析

方案	动态审计	批量审计			盲审计
		多所有者	多服务器	多文件	
PDP	-	-	-	-	-
POR	-	-	-	-	-
Wang	√	√	-	-	√
Zhu	√	-	√	-	√

Yang	√	√	√	-	√
He	√	√	√	√	√

3.3.3 配置审计

配置审计主要用来验证云基础设施的安全机制和静态结构配置是否与标准、用户期望或安全策略一致。比如，在多租户共享资源的云基础设施中，防火墙配置的正确性非常重要，一旦防火墙配置出现问题，很可能导致数据的泄露或服务的非法使用。同样，在多租户环境下网络结构要素没有进行有效隔离也将导致数据被窃取。

Bleikertz 等人提出了一种利用可达性图对虚拟机防火墙配置进行审计的方案。该方案根据多个虚拟机之间以及虚拟机与外界之间的可达性构建出整体的可达性图，Bleikertz 等人设计了两个算法，分别够对任意的访问模式进行审计和验证可达性图是否包含某个可达性策略。对于给定的可达性策略集合，通过周期性地调用验证算法进行审计，能够保证所有的可达性策略都被满足。Bleikertz 在文献中又延伸了先前的工作，提出了基于增量图的计算方法（如增加／删除结点和边），能够近实时地检测影响安全的配置变化，通过在云基础设施中部署探测器来保持图模型的变化和实际的配置变化同步。Doelitzscher 等人提出了一个基于自治代理的云计算安全审计系统，通过利用自治代理能够自动检测虚拟基础设施、VMs 的变化（例如新的 VMs 的打开／关闭和虚拟机迁移）和评估云环境的安全状态。该系统基于底层的业务流程模型还能够检测滥用云计算资源和租户账户、分布式拒绝服务攻击以及 ＶＭ 突破等攻击行为，克服了传统审计、入侵检测系统ＩＤＳ和入侵防御系统ＩＰＳ在频繁变化 的云环境下的不足。

4 总结与展望

4.1 总结

本文围绕云计算的数据安全和隐私保护，介绍了云计算的基本架构，列出了云计算中数据安全面临的基本问题。现今对于数据保护的技术主要还是基于数据加密的方法。对云计算系统的数据安全保护主要有访问控制、密钥协商、安全审计等方法。访问控制从软件层面制定用户访问规则，是对于数据安全保护的第一道屏障。会话密钥协商协议是在不可信网络中实现安全的信息交换的有效解决方法。通过对会话密钥协商协议相关的安全属性、可证明安全理论及协议分类进行说明。本文阐述双方会话密钥协商协议与群密钥协商协议的研究现状。安全审计安全审计是对计算机系统和计算机网络中的各种信息进行实时采集、分析，以查证是否发生安全事件的一种安全技术，在云计算中的安全审计面临新的挑战，如多层服务模式带来的挑战、数据外包存储带来的挑战、虚拟化多租户特性带来的挑战等，这些挑战都给安全审计带来了新的问题。

4.2 展望

立足于国家“建设国家数据统一共享开放平台，保障国家数据安全，加强个人信息保护”的战略需求，云数据安全保护方案的未来发展方向主要包括 3 个分支．首先是可信认证模式的统一，尽管现阶段云数据访问控制在隐私保护、可信评估和来源认证等方面已经积累了一定的经验和基础，取得了一定的研究成果，然而目前成果缺乏针对数据复杂异构场景的特殊化模式设计．因此，为了云数据安全访问控制，推动云技术的进一步应用，迫切需要实现不同来源、不同类型数据认证模式的统一。其次是安全传输技术的创新，现有的密钥协商、数字签名的加密技术虽然发展比较成熟，但是面对日益复杂的系统这些传统技术在交互性、灵活性和效率方面稍显不足，需要在加密技术上有新的创新。最后是安全共享组件的创新，实现数据安全共享是云数据的重要应用．当前云数据应用在目标选取、公共审计、数据聚合等重要组件方面已经积累了一定的经验和基础，然而这些组件多依附于全球先进的安全算法进行设计，且缺乏云数据安全共享场景下实际急需的隐私匹配、数据恢复、同态分析以及容错共享等特性．因此，目前云数据现行的共享组件如何实现功能性跃迁是具备应用前景的发展方向。

参 考 文 献

[1] 王文娟,杜学绘,王娜,单棣斌.云计算安全审计技术研究综述[J].计算机科学,2017,44(07):16-20+30.

[2] 胡志言,杜学绘,曹利峰.会话密钥协商协议研究进展[J].计算机应用与软件,2018,35(05):1-9+72.

[3] 蔡苏瑾.云计算环境下密钥协商协议的应用与改进[J].计算机产品与流通,2018(04):26-27.

[4] 沈剑,周天祺,曹珍富.云数据安全保护方法综述[J].计算机研究与发

展,2021,58(10):2079-2098.

[5] 邓桦,宋甫元,付玲,欧露,尹辉,高毅,秦拯.云计算环境下数据安全与隐私保护研究综述[J/OL].湖南大学学报(自然科学版):1-11[2022-01-06].http://kns.cnki.net/kcms/detail/43.1061.N.20211214.1140.002.html.

[6] 魏玉. 云计算数据安全访问控制机制研究[D].山东师范大学,2020.DOI:10.27280/d.cnki.gsdsu.2020.002073.

[7] 牛淑佳.基于云计算的密码技术综述[J].电子技术与软件工程,2021(09):227-230.