**基于同态加密和多方计算的安全云计算算法**

计算机科学和信息系统系，比拉果阿校区，果阿-403726。电子邮件：[debasisd@goa.bits-pilani.ac.in](mailto:debasisd@goa.bits-pilani.ac.in)

**摘要：云计算是一种发展中的技术，它对许多安全问题还不清楚。不受信云中的数据可以使用加密算法进行加密。随机化这些数据提供了更多的安全性，这可以通过在云中填充的概念来实现。在本文中，用户的数据使用加密方案，称为最优非对称加密填充(OAEP)和基于RSA(即HE-RSA)的混合加密算法，以允许多方在保持完整性和机密性的同时计算其输入的函数。同态加密(HE)是对加密数据执行的，无需在计算强大的云中进行解密，安全多方计算(SMPC)，以确保用户的安全和隐私。在本文中，我们提出了一种将多方计算与同态加密相结合的方案，以允许加密数据的计算不需要解密。本文描述了我们在云模型中使用的加密技术，并将其管理费用与同态加密和多方计算进行了比较。**

**一、介绍**

需要一个适当的或更合适的大数据基础设施[1]来支持大规模的存储和处理。如今，世界以数据为中心，因此大数据处理和分析已经成为任何大型机构最重要的工作。云计算是一种提供方便的、按需的访问来共享计算资源的模型。组织可以简单地连接到云，并在适当使用的基础上使用可用的资源。云计算已经成为一种使用共享计算资源分析大数据的工具，同时可以轻松地处理数据[1]的量和种类上的变化。云提供了许多优点，如更多的容错能力和多因素身份验证，以保护云中的信息。然而，由于这些属性，云计算也带来了维护数据的机密性和完整性的风险。在过去的几年中，由于恶意和侵入性行为，云中数据泄露的数量不断增加。加密保持数据的安全，但如果我们丢失加密密钥。因此，为了防止对云的恶意攻击，有必要开发有效的加密技术[3]、[4]，以抵抗主动攻击，并不解密地对加密数据进行计算。基于云计算的解决方案在过去的几年中变得越来越流行。云计算平台从大数据云中进行分析和提取有用的信息。云计算的一个主要问题是云数据的隐私和机密性[5]、[6]、[7]。一种解决方案是将加密后的数据发送到云中。然而，我们仍然需要支持对加密数据的有用计算，而全同态加密(FHE)[8]，[9]，[10]，[11]是支持对加密数据进行计算的一种方法。我们注意到，虽然存在其他用来实现安全计算的机制，但它们通常需要不同的数据提供者来交换信息。因为FHE方案是公钥方案，所以FHE更适合于我们有许多数据源的场景。

安全多方计算(MPC)[12]，[13]保证每个人都学习联合计算的正确输出，但不学习其他人的输入，即使执行计算的一些用户可能是主动或被动恶意的。安全的MPC可以为任意的计算和任意数量的各方来完成。因此，我们可以将安全的MPC协议视为编译器，它将一个函数的规范作为输入，并输出一个安全地计算该函数的协议。因此，我们可以将安全的MPC协议视为编译器，它需要一个映射的规范作为输入，而输出是一种安全地计算函数的协议。安全的MPC[14]，[15]提供了保密性和完整性，这是比完全同态加密和可验证的计算要好得多。可以对云环境中的任意计算和任意数量的各方执行可靠的MPC。

我们的模式的好处是：将多方计算与同态加密相结合；提出了使用最优非对称加密填充(OAEP)-同态加密(HE)-RSA进行加密的方案。

在第二节中，我们描述了相关的工作。在第三节中，我们定义了安全云计算的问题声明。在第四节中，我们描述了目标。在第五节中，我们描述了我们的贡献。然后，在第五节和第七节中，我们描述了密码技术，并详细描述了我们的方案。在第八节中，我们将描述这些结果。最后，在第九节中，我们总结并描述了通过我们的方法所实现的目标。

**二、相关工作**

M.Tebba等人[2]提出了一种对云中的加密数据执行操作的技术，它将在计算后提供类似的结果，就像我们直接处理原始数据一样。Z.Wang等人[3]给出了移动云计算中身份管理中同态签名的新定义。S.Yakoubov等人[4]进行了一项关于保护云中大数据分析的加密方法的调查。C. Rong等人[5]对云计算中不同的安全挑战进行了一项调查。C. Gentry[6]计算了加密数据的任意函数，它描述了一种保持信息私有的完全同态加密技术，但这使得一个工人不拥有私有解密密钥来计算数据的任何结果，即使数据的目的真的很复杂。C. Wang等人[7]提出了一种具有两个显著特征的有效方案，以确保用户在云数据的正确性。Y.Yu等人[8]研究了云中共享数据的三种审计机制中的主动对手攻击，并提出了一种解决方案，在不牺牲这些机制的任何理想特性的情况下解决这个弱点。L.Wei等人[9]提出了一种隐私欺骗抑制和安全计算审计协议，或SecCloud，这是第一个连接云中安全存储和安全计算审计的协议。A. Lopez-Alt等人[10]展示了一种新的加密方案，他们称之为多密钥FHE。 F.F.Moghaddam等人[11]提出了一种基于RSASmall-e和高效RSA的云计算环境混合加密算法。E. Shen等人[13]利用安全多方计算的概念，提出了一种被称为云中加密安全计算[14]的方案。这是一种加密方法，它支持信息共享和分析，同时保持敏感输入保密，更快更容易为应用程序软件开发人员使用。M.Bellare等人[12]提出了基于RSA的最优不对称加密方法。这项工作旨在在云计算通信中使用密码学的概念，并提高安全性。

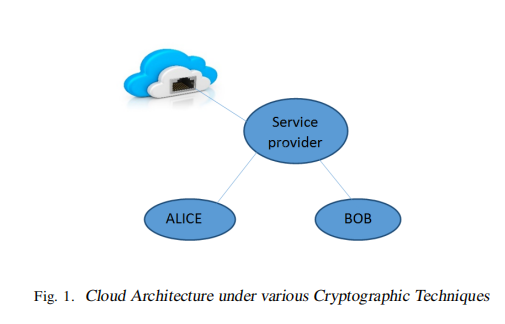
D. Zissis等人[18]解决了云计算安全问题的细节，他们提出了基于SSO和LDAP的公钥基础设施操作，以确保所涉及的数据和通信的身份验证、完整性和机密性。该解决方案提供了一个水平级别的服务，适用于所有牵连实体，实现了一个安全网格，在此网格中维护了基本的信任。C. Hongbing 等人[20]提出了一种替代方法，称为云环境的安全大数据存储和共享方案。该租户将大数据划分为已排序的部分，并将其存储在多个云存储服务提供商之间。该方案不是保护大数据本身，而是使用活板门功能保护各个数据元素映射到每个提供者。论文[15]介绍了所综述的云计算问题。在本文中，[15]的作者讨论了大数据与云计算、大数据存储系统和Hadoop技术[17]、[19]之间的关系。此外，还调查了研究挑战，重点是可伸缩性、可用性、数据完整性、数据转换、数据质量、数据异构性、隐私、法律和监管问题以及治理。最后，总结了需要大量研究努力的开放式研究问题。

J.Zhou等人[16]提出了一个方案称为安全和隐私保护协议基于云的车辆DTN解决抵抗层添加攻击的开放问题通过外包隐私保护聚合传输证据生成多个资源限制车辆云从执行任何单向活板门功能只有一次。车辆隐私很好地不受云和交通经理的保护。

**三、针对安全云计算的问题公式化**

考虑三方合作伙伴(如图所示1)：在云中存储数据的用户Alice；Alice希望与之共享数据的用户Bob；以及存储Alice数据的云服务提供商。要使用该服务，Alice和Bob首先下载一个由数据处理器、数据验证器和令牌生成器组成的客户端应用程序。在第一次执行时，Alice的应用程序会生成一个加密密钥。我们将把这个密钥称为主密钥，并假设它存储在Alice的系统上，并且对云服务提供商保密。云安全是根据可用性、完整性和机密性来衡量的，而加密技术很容易受到许多攻击，如：

1. 可用性；在这种情况下，云服务提供商有多个服务器。当一个服务器发生故障时，就没有安全问题，因为另一个服务器已准备好提供服务。
2. 完整性；数据的完整性是指数据的正确性和可信性。它确保了对敏感数据的计算是正确的。未经授权的用户不能更改这些数据。
3. 机密性；机密性是为了防止攻击者接触到敏感信息，同时确保授权用户能够访问这些信息。服务要求用户使用他们的数据来信任云。但在不受信任的云计算中，数据所有者并不信任云计算。因此，对用户侧的保护是必要的。用户在存储到云之前使用公钥对数据进行加密。
4. 循环攻击；在此攻击中，密码文本被反复加密，并计算迭代次数，直到原始文本出现。它可以解密任何密码文本。
5. 密码文本攻击在这种攻击中，明文和密码文本都是攻击者所知道的，他可以使用它来发现私有指数，一旦发现它就很容易找到。多方希望对其输入执行操作。这就需要解密他们的数据。这在不受信云的情况下带来了安全问题。



多方能否使用能够抵抗攻击的高效加密技术来存储其数据，并在不解密其数据的情况下执行计算？

**四、增值目标**

云环境需要用户数据的保护和机密性，同时直接利用云网络中实体的计算能力。本文关注一个吸引多种研究的问题，即云计算的数据加密。云环境要求用户数据的安全性和机密性，同时直接利用对加密数据的云网络中实体的计算能力。在本文中，我们提出了一种将多方计算与同态加密相结合的方案，以允许计算加密的数据而不需要解密。

**五、我们的贡献**

在本文中，我们提出了一种有效的加密技术，在多方数据加密。用户的数据使用填充方案最优非对称加密填充(OAEP)以及基于RSASmalle和高效RSA(HE-RSA)的混合加密算法进行加密。为了允许多方在其输入上计算一个函数，同时保持完整性和机密性。同态加密是对加密数据进行的，无需在计算强大的云中解密。该方案将多方计算与同态加密相结合，允许加密数据的计算无需解密。这种性质的输出允许在云环境中保持机密性和完整性。

1. **用于安全云计算的加密技术**
2. 初步和注意事项

1641222489(1)

G是一个基于由RFC3447定义的具有SHA1的哈希函数的掩码生成函数。G将r的K0位扩展到K-K0位。

1641222386(1)

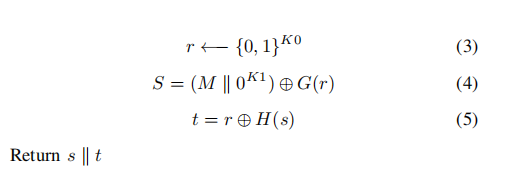
H是SHA-256哈希函数。H将K-K0位降低为K0位。r是一个大小为k0的随机种子。

1. OAEP密码系统

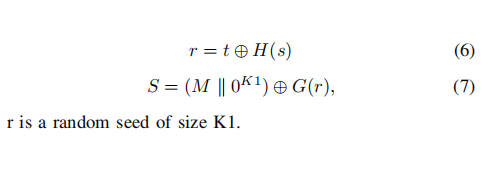
这是由贝拉雷和罗格威（[12]）提出的一种填充方案，它通过添加一个随机性元素来防止密文的部分解密。

**编码操作**

选择随机整数r，使其为1<r<n。

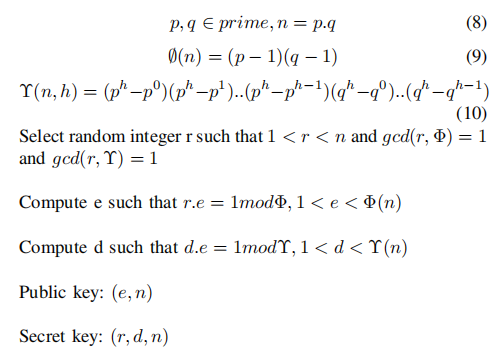


**译码操作**

****

1. **赫尔萨**

基于RSASmalle和高效RSA(HE-RSA)[11]的混合加密算法。引入了有效的RSA方案，采用一般的h阶线性群，有意从整数mod环中随机选择值。n.n被用作公钥和私钥的模量。它的长度，通常以位表示，是键的长度。



1. **同构加密**

可以使用同态加密[2]，[11]，[20]对加密数据执行操作。当使用密钥解密时，这些操作的结果与我们对原始数据执行的操作相同。乘法同态加密，它只允许在原始数据上的产品。

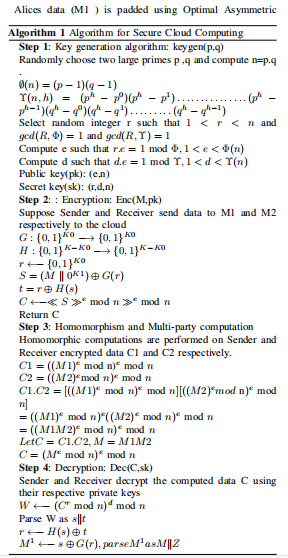
1641223267(1)

1. **提出的安全云计算算法**

所提出的安全云计算算法保证了云中单个数据的安全和隐私性[21]、[22]，并增强了同态加密和多方计算(MPC)等安全机制。

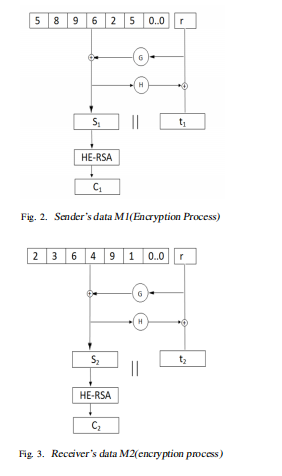
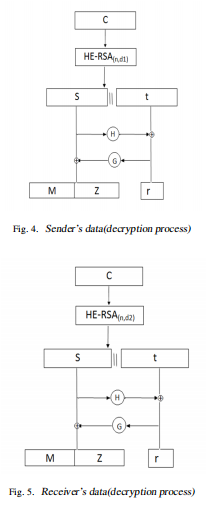
该算法主要基于密钥生成、加密、同态加密(HE)、多方计算(MPC)和欺骗等四个阶段。其主要目标是在这四个阶段中最小化运行时间、成本和开销。在所提出的算法中，与现有的一些算法(即RSA)相比，密钥生成过程中的指数数（在第1步中）得到了扩大。此外，该算法还实现了一个双重加密过程（在步骤2中），以防止对一些现有技术的一般攻击。在步骤3中，我们集成了完全同态加密和多方计算，允许在云中不解密地计算加密数据（在步骤4中）。

要与云中的各种服务交互并存储由这些服务生成/处理的数据，需要多种安全功能。假设Alice和Bob分别将数据发送到M1和M2到云中，在使用HE-RSA加密之前，使用最优不对称加密填充(OAEP)方案对爱丽丝的数据(M1)进行填充，得到密文C1，如图所示 2。



加密填充（OAEP）在使用HE-RSA加密之前的填充方案，产生密文C1（如图2所示）。在使用HE-RSA加密之前，使用最佳非对称加密填充（OAEP）方案对接收器的数据（M2）进行填充，从而生成密文C2（如图3所示）。同态加密产生的数据C使用发送方的私钥解密，然后使用OAEP解码（如图4所示）。

由同态加密产生的数据C使用接收器的私钥进行解密，然后使用OAEP进行解码(如图所示5)。例如，同态加密要求所有用户和结果的最终接收者共享一个密钥来加密输入和解密结果，如果他们属于不同的组织，这可能很难安排。此外，同态加密不允许对使用不同密钥加密的数据进行计算（而不会产生额外的重大开销），因此用户不可能允许对他们参与计算的数据进行不同的访问。

安全多方计算(MPC)适合于利用半可信的云设置。MPC杠杆是诚实的政党的存在，而不必要知道哪些各方是诚实的，以实现数据和计算的机密性和完整性。多方计算提供的安全保证比FHE更弱，但效率可以更高。在MPC中，没有一方了解到关于数据的任何信息，但如果有足够多的一方被对手破坏并汇集他们的信息，他们就可以破坏机密性。MPC的相对效率，以及半可信云模型在现实世界中的适用性，使其成为更实际的安全云计算的一个很有前途的候选者。

1. **结果**

将同态加密和多方计算（HE+MPC）相结合后，数据的机密性和完整性得到了维护，其开销小于同态加密，但大于多方计算。因此，我们收到了基于同态加密和多方计算的中等开销（如表1所示）。图6总结了各种计算中每种技术的近似效率和成本，描绘了在不安全计算中产生的乘法性能开销。除了效率低下之外，同态加密还有其他局限性。

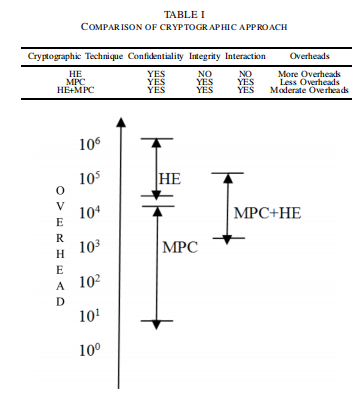


图 6.由同态加密(HE)、多方计算(MPC)和同态加密+多方计算(HE+MPC)引起的不安全计算的乘法性能开销的图形描述。

1. **结论**

在本文中，我们提出了一种安全的云计算模型，利用基于同态加密(HE)和多方计算(MPC)的高效加密技术加密用户数据，然后对用户数据进行操作，同时保持完整性和机密性。输出与对原始数据进行的操作相同。一方可以共同执行计算，而不向另一方透露其数据。在这里，我们设计并开发了专门为私有半可信云设置而设计的安全同态加密和多方计算技术。此设置允许开发人员将私有云与保护它所需的加密技术(即HE+MPC)一起设计。

1. **致谢**

这项工作得到了美国政府科技部(DST)科学与工程研究委员会(SERB)颁发的早期职业研究奖的部分支持。印度新德里(项目编号：ECR/2015/000256)和2017-bilpianiK.KBirlaGoa校园研究启动基金(RIG)奖。

**参考文献**

[1]Mcll P Gracc T. The NIST definition of cloud computing,NIST Special Publication,2009, pp. 800-145.

[2]Tebaa M,Haiji S.E,Ghazi A.E. Homomorphic Encryption Applied to the Cloud Computing Security,Proceedings of the world Congress on Enginecring,London,U.K.，Vol.1,No.1，2014,Pp.4-6.

[3]Wang z,Sun G,Chcn D.A new defininion of homomorphic signarure for idenfiry management in mobile cloud compuring, Journal of Computerand Systcm Scicnccs,Vo1. 80,NO.3,2014,pp. 546-553.

[4]Yakoubov s,Gadepally v, SchearN, Shen E，Yerukhimovich A.A Survey of Cryptographic Approaches to Seauring Big-Data Analyricsin the Cloud,IEEE High Performance Extreme Computing Confcrcnce(HPEC),2014, pp. l-6.

[5] Rong C ,NguyenST，Jaatun MG.Beyond lighrning: Asurvey on security challenges in cloud compufing，Computers and ElectricalEng inecring，Vol.39,No.1，2013,Pp.47-54.

[6]Gentry C.Compuring Arbitrary Foncions of Encrypted Data, Commu-nications of the ACM,vo1. 53,No. 3,2010,pp. 97-105.

[7]WngC, Wang Q.Rcn K,Lou W. Ensuring Data Storage Security inCloud Compufing, Quality of Service, 2009,Pp. 1-9.

[ 8]YuY. Niua L, Yang,G, Mu 'Y,Susilow.On the security of auudiring mechanisms for secuwre coud storage，Future GcncrationComputcr Systcms,Vol. 30,2014 Pp.127-132.

[9]wei'L,Zhu H,CaoZ, Dong x,JiaW, Chen Y,Vasilakos AV. Securiry and privncy for storage and computation in cloud computing,Information Scicnccs, Vol. 258,2014, Pp. 371-386.

[10]Lopez-Alt A,Tromer V,VaikuntanathanE.On-the-Fly Multiparty Computation on the Cloud via Mulrikey Fully Homomorplic Encryption,Proceaiings of the forty-fourth annual ACM symposiuim on Theory of computing, 2012,pp. 1219-1234.

[11] Brakerski Zand VaikuntanathanE.Efficient fiually homomorphic encryption from(s tandard )LWE,SIAM Joumal on Computing,Vol.43,No.2,2011, Pp. 831-871.

[ 12] Bellarc M. and Rogawayy P. Optimal Asymmetric Encryprion How to Encrypr with RSA，Advances in Cryptology Eurocrypt 94 Proceedings，vol.950,1995, Pp.1-19.

[13] Shen E,Varia M.Cunningham RK, Vesey WK. Cryptog raphically Secure Computation，IEEE Computcr Socicty，Vol.48,No.4，2015,pp.78-81.

[14] Zissis D, Lckkas D.Addressing cloudl computing security issues, FutureGencration Computer Systcms,Vol.28, No. 3,2012,pp. 583-592.[15] Hashem IAT,Yaqoob L,AnuRr NB,Mokhtar N, Gani A, Khan S.U.

[15]The rise of 'big data’on cloudi computing: Review and open res earchis sues,Infomation Systcms,2015,Vol.47,pp. 98-1 15.

[16] ZhouJ,Dong x,Co. z，VasilakosAv. Secure and Privacy Pres erving Protocol for Cloud-based Vehicular DTNs,IEEE Transactionson Information Forensics and Security,In formation Systems,Vo. 10， No.6,2015,Pp. 1299 -13 14.

[17] Zhao J, Wang L, Tao J, Chen J, Sun w, Ranjan R, Kolodziej J, Strcit A,Gcorgakopoulos D.A securiry framework in G-Hadoop for big datacompuring across distributed Cloud data cenires，Journai of Compuerand System Sciences,Vol.80, No.5,2014,Pp. 994-1007.

[18] Zucch R, Khoshgoftaar TM,Wald R.lntrusion detection and Big Heteogeneous Dafa: a Survey，Joumal of Big Data，Springer，Vol.2,No. 3,2015, pp.1-40.

[19]Hongbing ℃,Chunming R,Kai H,Weihongw, Yanyan L. Secure Big Data Storage aund Sharing Scheme for Cloud Teanis,ChinaCommunications,2015, pp. 106-115.

[20]Jajodia\_S, Kant K,Samarati ,Singhal \_A, Swarup v, WangC. Secure Cloud Compuring, Springer Scicnce+-Business Media,2014, pp.1-350.

[21] D. Das, R. Mism, A Raj Approximating Geographic Routing using Coverage Tree Heuristis for Wireless Network, Wireless Networks (WINE),Springer Us, Vol. 21. No. 4, 2015, pp.1 109-1118.

[22] T Limbasiya, D. Das, Secure Message Transmission Algoritlon for Vehide to Vehicle (V2V) Comunication, IEEE Region 10 Conference (TENCON)201 6, Technologies for Smart Nation, Singapore, 22-25 Now. 2016, Singapore, pp. 2507-2512.