人工智能的圣杯：全同态加密（FHE）

原文作者：Advait (Leo) Jayant

A 希望在 Netflix 和 Amazon 上获得高度个性化的推荐。B 不希望 Netflix 或 Amazon 了解他们的偏好。

在当今的数字时代，我们享受着亚马逊和 Netflix 等服务带来的个性化推荐便利，这些推荐精准地迎合了我们的趣味。然而，这些平台深入我们私人生活的行为正引发越来越多的不安。我们渴望在不牺牲隐私的前提下享受定制化服务。过去，这似乎是一个悖论：如何在不对基于云的人工智能系统分享大量个人数据的情况下实现个性化。全同态加密（FHE）提供了一个解决方案，使得我们能够兼得鱼与熊掌。

## 人工智能即服务（AIaaS）

人工智能（AI）如今在应对包括计算机视觉、自然语言处理（NLP）和推荐系统在内的多个领域的复杂挑战中扮演着关键角色。然而，这些 AI 模型的发展给普通用户带来了重大挑战：

1.数据量：构建精确模型往往需要庞大的数据集，有时甚至会达到千万亿字节的规模。

2.计算能力：像转换器这样的复杂模型需要数十个 GPU 的强大算力，通常连续运行数周。

3.领域专长：这些模型的微调需要深厚的专业知识。

这些障碍使得大多数用户难以独立开发强大的机器学习模型。

实际应用中的 AI 即服务流水线



进入 AI 即服务（AIaaS）时代，这一模式通过提供由科技巨头（包括 FAANG 成员）管理的云服务，让用户得以接触到最先进的神经网络模型，从而克服了上述障碍。用户只需将原始数据上传至这些平台，数据便会在平台上被处理，进而生成富有洞察力的推断结果。AIaaS 有效地普及了高质量机器学习模型的使用权，将先进的 AI 工具开放给更广泛的群体。然而，遗憾的是，当今的 AIaaS 在带来这些便利的同时，却牺牲了我们的隐私。

## 人工智能即服务中的数据隐私

目前，数据仅在从客户端传输到服务器的过程中进行加密。服务器能够访问输入数据以及基于这些数据所做的预测。

在 AI 即服务过程中，服务器能够访问输入和输出数据。这种情况使得普通用户共享敏感信息（如医疗和财务数据）变得复杂。诸如 GDPR 和 CCPA 之类的法规加剧了这些担忧，因为它们要求用户在数据被共享之前明确同意，并保证用户有权了解其数据如何被使用。GDPR 还进一步规定了传输过程中数据的加密和保护。这些法规设定了严格的标准，以确保用户的隐私和权利，倡导对个人信息有明确的透明度和控制。鉴于这些要求，我们必须在 AI 即服务（AIaaS）流程中开发强大的隐私机制，以维护信任和合规性。

## FHE 解决问题

通过对 a 和 b 进行加密，我们可以确保输入数据保持私密性。



全同态加密（FHE）为云计算中关联的数据隐私问题提供了解决方案。FHE 方案支持密文加法和乘法等操作。其概念简单明了：两个加密值之和等于这两个值之和的加密结果，乘法亦然。

实际操作中，其工作原理如下：用户在本地对明文值?和?执行加法运算。随后，用户加密?和?，并将密文发送至云服务器。服务器能够在加密值上（同态地）执行加法运算并返回结果。从服务器解密得到的结果将与?和?的本地明文加法结果一致。这一过程既保障了数据隐私，又允许在云端进行计算。

## 基于全同态加密的深度神经网络（DNN）



除了基本的加法和乘法运算外，在 AI 即服务流程中，利用全同态加密（FHE）进行神经网络处理的技术已取得显著进展。在此背景下，用户可以将原始输入数据加密成密文，并仅将这些加密数据传输至云服务器。服务器随后对这些密文进行同态计算，生成加密输出，并将其返回给用户。关键在于，只有用户持有私钥，使其能够解密并访问结果。这构建了一个端到端的 FHE 加密数据流，确保用户数据在整个过程中的隐私安全。

基于全同态加密的神经网络在 AI 即服务中为用户提供了显著的灵活性。一旦密文被发送到服务器，用户便可离线，因为客户端与服务器之间无需频繁通信。这一特性对物联网设备尤为有利，它们通常在限制条件下运行，频繁通信往往不切实际。

然而，值得注意的是全同态加密（FHE）的局限性。其计算开销巨大；FHE 方案本质上耗时、复杂且资源密集。此外，FHE 目前难以有效支持非线性操作，这对神经网络的实现构成了挑战。这一限制可能会影响基于 FHE 构建的神经网络的准确性，因为非线性操作对这类模型的性能至关重要。

K.-Y. Lam, X. Lu, L. Zhang, X. Wang, H. Wang, 和 S. Q. Goh 所著的 "基于高效全同态加密的隐私增强神经网络在 AI 即服务中的应用"，在南洋理工大学（新加坡）和中国科学院（中国）发表。



(Lam 等人，2024 年)描述了一种用于 AI 即服务的隐私增强神经网络协议。该协议首先通过使用误差学习(LWE)来定义输入层的参数。LWE 是一种加密原语，用于通过加密来保护数据，使得无需先解密即可对加密数据进行计算。对于隐藏输出层，参数则通过环 LWE(RLWE)和环 GSW(RGSW)来定义，这两种高级加密技术扩展了 LWE，以实现更高效的加密操作。

公共参数包括分解基?及???给定一个输入向量?长度为?, 一组?LWE 密文(??,??)为每个元素?[?]生成了使用 LWE 私钥?，关于?的评估密钥为索引生成?[?]>0及?[?]<0此外，还针对?设置了一组 LWE 切换密钥。这些密钥支持在不同加密方案间进行高效切换。

输入层被指定为第 0 层，输出层为第?层对于每一层?从 1 到?神经元数量为??在第 0 层已确定。权重矩阵??偏置向量??从第 0 层开始在第 0 层上叠加被定义。对于每个神经元ℎ从 0 到??−1来自第?−1层的 LWE 密文在同态加密下进行评估。这意味着计算是在加密数据上执行的，以计算ℎ中的线性函数。第?层中的第-th 个神经元，结合权重矩阵和偏置向量。随后，在ℎ中评估查找表（LUT）。-th 神经元，以及从?′的切换到较小的?执行操作后，接着对结果进行舍入和重新缩放。该结果被纳入第?层 LWE 密文集合中。

最后，协议将 LWE 密文返回给用户。用户随后可以使用私钥?解密所有密文。查找推理结果。

此协议通过利用全同态加密（FHE）技术，高效实现了隐私保护的神经网络推理。FHE 允许在加密数据上进行计算，而不向处理服务器泄露数据本身，确保了数据隐私的同时，提供了 AI 即服务的优势。

## AI 中全同态加密的应用

FHE（全同态加密）使得在加密数据上进行安全计算成为可能，不仅开拓了众多新的应用场景，同时确保了数据的隐私性和安全性。

广告中的消费者隐私：（Armknecht 等人，2013 年）提出了一种创新的推荐系统，该系统利用全同态加密（FHE）。此系统能够在向用户提供个性化推荐的同时，确保这些推荐内容对系统本身完全保密。这保证了用户偏好信息的私密性，有效解决了定向广告中的重大隐私问题。

医疗应用：（Naehrig 等人，2011 年）为医疗保健行业提出了一个引人注目的方案。他们建议使用全同态加密（FHE）持续将患者的医疗数据以加密形式上传至服务提供商。这一做法确保了敏感的医疗信息在其整个生命周期内保持机密性，既增强了患者隐私保护，又使得医疗机构能够无缝进行数据处理和分析。

数据挖掘：挖掘大型数据集能够产生重大洞见，但往往以用户隐私为代价。（Yang, Zhong, 和 Wright, 2006）通过在全同态加密（FHE）背景下应用函数加密解决了这一问题。这种方法使得从庞大的数据集中提取有价值的信息成为可能，同时不损害被挖掘数据个体隐私的安全性。

财务隐私：设想一个场景，一家公司拥有敏感数据和专有算法，必须保密。（Naehrig 等人，2011 年）建议采用同态加密来解决这一问题。通过应用全同态加密（FHE），公司能够在不暴露数据或算法的情况下，对加密数据进行必要的计算，从而确保财务隐私和知识产权的保护。

法医图像识别：（Bosch 等，2014）描述了一种利用全同态加密（FHE）外包法医图像识别的方法。这一技术对执法机构尤其有益。通过应用 FHE，警方及其他机构能够在不暴露图像内容的情况下，检测硬盘上的非法图像，从而保护调查中数据的完整性和机密性。

从广告和医疗保健到数据挖掘、金融安全和执法，全同态加密有望彻底改变我们在各个领域处理敏感信息的方式。随着我们不断发展和完善这些技术，在一个日益数据驱动的世界中保护隐私和安全的重要性再怎么强调也不为过。

## 全同态加密（FHE）的局限性

尽管具有潜力，我们仍需解决一些关键限制

多用户支持：全同态加密（FHE）允许对加密数据进行计算，但在涉及多个用户的场景中，复杂性成倍增加。通常，每个用户的数据会使用唯一的公钥进行加密。管理这些不同的数据集，尤其是在大规模环境中考虑到 FHE 的计算需求，变得不切实际。为此，研究人员如 Lopez-Alt 等人于 2013 年提出多密钥 FHE 框架，允许对使用不同密钥加密的数据集进行同时操作。这种方法虽然前景看好，但引入了额外的复杂层级，并需要在密钥管理和系统架构方面进行精细协调，以确保隐私和效率。

大规模计算开销：全同态加密（FHE）的核心在于其能够在加密数据上执行计算。然而，这一能力伴随着巨大的代价。与传统的未加密计算相比，FHE 操作的计算开销显著增加。这种开销通常表现为多项式形式，但涉及高次多项式，加剧了运行时间，使其不适用于实时应用。针对 FHE 的硬件加速代表了巨大的市场机遇，旨在降低计算复杂性并提高执行速度。

有限操作：近期进展确实拓宽了全同态加密的应用范围，使其能支持更多种类的运算。然而，它主要仍适用于线性和多项式计算，这对涉及复杂非线性模型（如深度神经网络）的人工智能应用而言，是一个重大限制。这些 AI 模型所需的操作在当前全同态加密框架下实现高效执行颇具挑战。尽管我们正取得进展，但全同态加密的操作能力与先进 AI 算法需求之间的差距，仍是亟待突破的关键障碍。

## 加密与人工智能背景下的全同态加密

以下是一些致力于在加密领域利用全同态加密（FHE）进行 AI 应用的公司：

Zama 提供 Concrete ML，这是一套开源工具，旨在简化数据科学家使用全同态加密（FHE）的过程。Concrete ML 能够将机器学习模型转换为其同态等价形式，从而实现对加密数据的保密计算。Zama 的方法使得数据科学家无需深入的密码学知识就能利用 FHE，这在医疗和金融等对数据隐私至关重要的领域尤为有用。Zama 的工具在保持敏感信息加密的同时，促进了安全的数据分析和机器学习。

Privasee 专注于构建一个安全的 AI 计算网络。他们的平台利用全同态加密（FHE）技术，使得多方能够在不泄露敏感信息的情况下进行协作。通过使用 FHE，Privasee 确保用户数据在整个 AI 计算过程中保持加密状态，从而保护隐私并遵守如 GDPR 等严格的数据保护法规。他们的系统支持多种 AI 模型，为安全数据处理提供了一个多功能的解决方案。

Octra 将加密货币与人工智能相结合，以提升数字交易安全性和数据管理效率。通过融合全同态加密（FHE）与机器学习技术，Octra 致力于增强去中心化云存储的安全性与隐私保护。其平台通过运用区块链、密码学及人工智能技术，确保用户数据始终处于加密且安全的状态。这一策略为去中心化经济中的数字交易安全与数据隐私构建了坚实的框架。

Mind Network 将全同态加密（FHE）与人工智能结合，实现人工智能处理过程中的安全加密计算，无需解密。这促进了隐私保护的、去中心化的人工智能环境，无缝融合了加密安全与人工智能功能。这种方法不仅保护了数据的机密性，还实现了无需信任、去中心化的环境，其中人工智能操作可以在不依赖中央权威或暴露敏感信息的情况下进行，有效结合了 FHE 的加密强度与人工智能系统的操作需求。

在全同态加密（FHE）、人工智能（AI）和加密货币领域前沿运营的公司数量仍然有限。这主要是因为有效实施 FHE 需要巨大的计算开销，要求强大的处理能力以高效执行加密计算。

## 结语

全同态加密（FHE）通过允许在未解密的情况下对加密数据进行计算，为增强 AI 中的隐私提供了一种有前景的方法。这一能力在医疗和金融等对数据隐私至关重要的敏感领域尤为宝贵。然而，FHE 面临重大挑战，包括高计算开销以及在处理深度学习所必需的非线性操作方面的局限性。尽管存在这些障碍，FHE 算法和硬件加速的进步正在为 AI 中更实用的应用铺平道路。该领域的持续发展有望极大提升安全、保护隐私的 AI 服务，平衡计算效率与强大的数据保护。