



(21) 申请号 202411055747.7

G06F 16/27 (2019.01)

(22) 申请日 2024.08.02

G06F 21/60 (2013.01)

(65) 同一申请的已公布的文献号

G06F 21/62 (2013.01)

申请公布号 CN 118568359 A

G06F 16/22 (2019.01)

G06F 16/215 (2019.01)

(43) 申请公布日 2024.08.30

(56) 对比文件

(73) 专利权人 合肥理微大数据有限公司

CN 117609642 A, 2024.02.27

地址 230000 安徽省合肥市高新区云飞路5

CN 118132845 A, 2024.06.04

号合肥新宇创谷科技园A座2层213室

CN 116128607 A, 2023.05.16

(72) 发明人 张清云 李昕 张淑娟 宋雨

审查员 张培

宋力 李秀丽 姚玉海

(74) 专利代理机构 安徽华晟智恒知识产权代理

事务所(普通合伙) 34193

专利代理师 陈宇

(51) Int. Cl.

G06F 16/9535 (2019.01)

权利要求书4页 说明书9页 附图1页

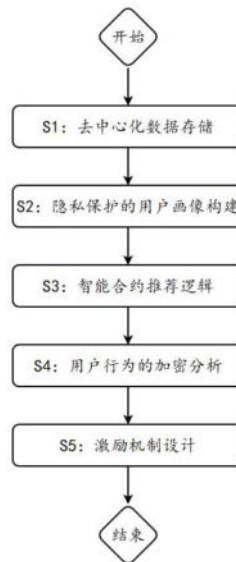
(54) 发明名称

基于用户行为和偏好的个性化内容推荐方

法

(57) 摘要

本发明公开了基于用户行为和偏好的个性化内容推荐方法,涉及内容推荐技术领域,本发明,包括以下步骤:去中心化数据存储:将用户数据存储在区块链上,确保数据的不可篡改性和透明性;首先对即将存储的数据进行初步筛选;本发明,通过采用去中心化的数据存储方式,将用户数据存储在区块链上,利用区块链的不可篡改性和透明性,显著提高了数据的安全性,结合零知识证明等隐私保护技术,确保了用户在区块链上的匿名性,增强了用户对系统的信任度,这种信任是基于数据的加密处理和安全存储,以及智能合约的公正性与透明性,为用户提供了一个安全可靠的个性化推荐环境。



1. 基于用户行为和偏好的个性化内容推荐方法,其特征在于,包括以下步骤:

S1:去中心化数据存储:将用户数据存储在区块链上,确保数据的不可篡改性和透明性;

S2:隐私保护的用户画像构建:通过零知识证明密码学技术,构建不泄露用户具体信息的用户画像,具体步骤如下:

确定用户画像所需属性,不包括可识别个人身份的敏感信息;

收集并清洗用户行为数据,进行预处理以去除无效或无关信息;

对用户数据进行匿名化处理,确保不包含可追溯到个人身份的信息;

利用零知识证明技术,证明用户属性组别,避免泄露具体个人信息;

对用户画像属性进行加密处理;

整合加密属性,形成用于推荐算法的加密用户画像;

采用差分隐私的隐私保护数据分析技术,分析用户画像,发现用户群体趋势和偏好;

对用户画像进行验证和测试,确保准确性和隐私保护的有效性;

设计定期更新机制,用于反映用户行为和偏好的最新变化,同时保护隐私;

实现访问控制机制,确保只有授权的系统 and 人员对用户画像数据进行访问;

定期进行数据访问审计;

获取用户明确同意收集和处理数据,提供数据退出或删除选项;

S3:智能合约推荐逻辑:利用智能合约实现推荐逻辑,确保推荐过程的公正性和透明性,具体操作步骤如下:

确定推荐目标 and 需求,包括推荐内容类型、用户画像属性及推荐逻辑规则;

设计智能合约逻辑,实现用户画像输入、推荐算法执行及推荐结果输出;

使用区块链编程语言编写智能合约代码;

在智能合约中嵌入隐私保护措施;

进行单元测试、集成测试 and 安全测试,确保智能合约的功能性和安全性;

将智能合约部署到区块链平台,实现去中心化执行;

将用户数据上链,确保数据不可篡改性和透明性;

调用智能合约,输入用户画像 and 参数,自动执行推荐逻辑;

输出推荐结果,并验证推荐结果是否符合预期推荐规则 and 标准;

收集用户反馈,优化推荐算法;

定期生成透明度报告,展示推荐逻辑调用次数 and 推荐结果分布;

定期对智能合约进行审计,确保逻辑正确性和安全性;

其中验证推荐结果是否符合预期推荐规则 and 标准的具体过程如下:

首先通过推荐因素进行综合分析,其中推荐因素包括:

准确率:分析推荐结果中正确推荐数量与总推荐数量的比例;

上下文相关性:评估推荐结果与用户当前情境的相关性,并通过相关百分比进行量化,记为相关比;

个性化强度:衡量推荐结果的个性化程度,即推荐内容与用户独特属性的匹配度,并赋予1-100的匹配度评分,记为匹配值;

推荐结果的个性化创新度:推荐结果中包含的新颖元素 or 创新内容的比例,并记为个

创比;

将得到的准确率、相关比、匹分值及个创比归一化处理,代入以下公式: $TPZ = 0.95(zq + xb + pp) + (gc + 1.25)^{1.21}$ 以得到推评值TPZ,式中zq、xb、pp及gc分别为准确率、相关比、匹分值及个创比,并以推评值TPZ作为衡量推荐结果验证的标准;

再收集用户对推荐结果的反馈参数,用于对计算的推评值进行修正得到综分值ZFZ;

将得到的综分值ZFZ与预设综分阈值进行比对,当综分值ZFZ大于综分阈值时,则判断推荐结果达到预设标准,反之则判断推荐结果未达到预设标准,当确定推荐结果未达到预设标准则根据用户对推荐结果的具体反馈优化推荐算法;

其中收集用户对推荐结果的反馈参数对计算的推评值进行修正的过程如下:

其中反馈参数包括:

用户参数度:用户与推荐内容互动的深度和频率,并通过停留时间及互动次数进行量化,将得到的停留时间及互动次数归一化处理后分别乘以对应的权重因子并求和,得到用参值;

用户决策时间:用户在接收推荐后做出决策所需的时间,用于反映推荐的相关性和吸引力;

用户画像的动态更新频率,用户画像更新的频率和及时性,反映推荐系统对用户行为变化的响应速度;

将得到的用参值、用户决策时间及用户画像更新频率归一化处理后,将用参值与用户画像更新频率的乘积与用户决策时间相除,得到用评比值,并以此用评比值作为衡量用户对推荐结果反馈的评价标准;

将得到的推评值TPZ及用评比值归一化处理后代入以下公式: $ZFZ = (TPZ + 1.22) * (1 - YPZ^{-1}) - 0.26$ 以得到综分值ZFZ,式中YPZ为用评比值,将得到的综分值ZFZ作为推荐结果最终的评估标准;

S4:用户行为的加密分析:对用户行为数据进行加密处理,仅在获取到用户授权时进行分析;

S5:激励机制设计:通过激励机制鼓励用户贡献数据同时保护其隐私权益。

2.根据权利要求1所述的基于用户行为和偏好的个性化内容推荐方法,其特征在于,所述S1的具体步骤如下:

对用户数据进行初步筛选,以筛选出符合预设标准的数据;

对筛选后的数据进行加密处理,用于确保数据在传输过程中的安全性;

将加密后的数据分割成多个片段,适应区块链的存储结构;

对每个数据片段生成哈希值,作为数据的唯一标识,确保数据的完整性和可追溯性;

编写智能合约,定义数据存储的规则和条件,用户保证数据的访问权限和存储位置;

将数据片段和数据指纹通过智能合约上传到区块链网络,实现数据的去中心化存储;

利用区块链网络中的多个节点对上传的数据进行验证,确保数据的一致性和不可篡改性;

为存储在区块链上的数据构建索引;

设定数据访问权限,确保只有授权的用户或系统对数据片段进行访问;

在区块链网络中实现数据的多节点备份;

通过智能合约实现数据的更新和维护规则；

采用零知识证明隐私保护技术,确保用户数据的隐私性,即使在区块链上也能保持匿名性。

3. 根据权利要求2所述的基于用户行为和偏好的个性化内容推荐方法,其特征在于,所述S1中对用户数据进行初步筛选的具体操作步骤如下:

根据应用场景和业务需求,确定数据筛选的标准和规则,从各种来源收集用户数据;

对收集到的数据进行清洗,去除无效、错误或不完整的数据记录,验证数据的准确性和一致性,确保数据符合预设的标准,去除重复的数据记录;

根据数据类型和用途对数据进行分类,采用数据压缩技术减少数据的存储空间需求。

4. 根据权利要求1所述的基于用户行为和偏好的个性化内容推荐方法,其特征在于,所述S2中对用户画像进行验证和测试,确保准确性和隐私保护的有效性具体过程如下:

确定衡量用户画像准确性和隐私保护效果的衡量指标包括:

一致性:用户画像与实际用户行为的匹配程度;

覆盖度:用户画像覆盖的用户特征和行为的广度;

可预测性:用户画像在预测用户未来行为时的有效性;

隐私保护:用户画像在保护用户隐私方面的性能;

从用户数据集中选择样本进行测试;

准备测试集,包括用户的实际行为数据和相应的用户画像数据;

针对确定的衡量指标进行逐一分析,具体的:

一致性检验:比较用户画像中的特征与用户的实际行为数据,评估一致性;

覆盖度分析:分析用户画像覆盖的用户特征和行为的广度;

可预测性测试:使用用户画像预测用户未来的行为,并与实际结果进行比较,评估预测的准确性;

隐私保护评估:通过混淆测试评估用户画像的隐私保护效果,确保即使在数据被非法访问的情况下,也无法准确推断出用户的具体信息,评估用户画像在保护用户隐私方面的性能;

通过A/B测试,对比不同用户画像构建方法的效果,选择最优的方法;

收集用户对推荐内容的反馈,评估用户画像的准确性和用户满意度;

使用统计方法分析用户画像数据,评估用户画像的可靠性和有效性;

模拟潜在的隐私攻击,测试用户画像的抗攻击能力。

5. 根据权利要求1所述的基于用户行为和偏好的个性化内容推荐方法,其特征在于,所述S4的具体步骤如下:

确定并分类需要加密的用户行为数据类型;

使用强加密算法对用户行为数据进行加密处理;

管理加密密钥,确保密钥的安全性和生命周期;

设计用户授权机制,获取用户对其数据收集和分析的同意;

在分析前验证用户授权,确保数据使用符合用户意愿;

实现安全的数据访问控制,限制未授权访问;

在用户授权的情况下解密数据,并进行隐私保护的数据分析;

采用差分隐私或同态加密技术保护解密后数据的隐私；
生成并加密分析结果；
记录和审计数据使用情况；
提供用户反馈机制；
制定数据泄露应对计划,用于应对数据安全事件。

6. 根据权利要求1所述的基于用户行为和偏好的个性化内容推荐方法,其特征在于,所述S5的具体步骤如下:

确定激励机制的目标,包括提高用户参与度和数据质量;
调研用户需求和偏好,确定激励类型和用户接受度;
制定数据贡献标准,明确可获激励的数据类型和质量;
设计激励规则,包括条件、计算方式和发放时间;
使用智能合约自动执行激励规则,确保公正性和透明性;
进行激励机制的模拟测试,评估对用户行为和系统性能的影响;
实施激励机制后,收集用户反馈,评估效果和满意度;
根据反馈和系统表现调整优化激励机制;
向用户公开激励机制详细信息;
记录和审计激励发放情况;
平衡激励效果和隐私保护,避免用户隐私泄露;
提供用户退出激励机制的选项,尊重用户自主选择权。

基于用户行为和偏好的个性化内容推荐方法

技术领域

[0001] 本发明涉及内容推荐技术领域,具体为基于用户行为和偏好的个性化内容推荐方法。

背景技术

[0002] 随着信息技术的飞速发展,个性化推荐系统已成为电子商务、社交媒体和内容提供商等在线平台的核心组成部分。这些系统通过分析用户的历史行为和偏好,提供定制化的内容或商品推荐,以增强用户体验和满意度。然而,现有的个性化推荐系统在提供个性化服务的同时,往往需要收集和处理大量的用户数据,这引发了用户隐私保护的问题。如何在不侵犯用户隐私的前提下提供个性化推荐服务,是一个亟待解决的问题;

[0003] 现有的推荐系统多采用中心化的数据存储和处理方式,用户数据的安全性和隐私性难以得到充分保障。用户对于自己的数据如何被收集、存储和分析往往缺乏足够的了解和控制。此外,数据泄露和滥用的风险也随着数据量的增加而上升。用户对于个人隐私的担忧限制了他们对推荐系统的接受度和信任度,这对推荐系统的发展和应用构成了重大障碍。

[0004] 为了解决上述缺陷,现提供技术方案。

发明内容

[0005] 本发明的目的在于解决如何在不侵犯用户隐私的前提下提供高效、准确的个性化内容推荐的问题,而提出基于用户行为和偏好的个性化内容推荐方法。

[0006] 本发明的目的可以通过以下技术方案实现:

[0007] 基于用户行为和偏好的个性化内容推荐方法,包括以下步骤:

[0008] S1:去中心化数据存储:将用户数据存储在区块链上,确保数据的不可篡改性和透明性;

[0009] S2:隐私保护的用户画像构建:通过零知识证明密码学技术,构建不泄露用户具体信息的用户画像;

[0010] S3:智能合约推荐逻辑:利用智能合约实现推荐逻辑,确保推荐过程的公正性和透明性;

[0011] S4:用户行为的加密分析:对用户行为数据进行加密处理,仅在获取到用户授权时进行分析;

[0012] S5:激励机制设计:通过激励机制鼓励用户贡献数据同时保护其隐私权益。

[0013] 进一步的,所述S1的具体步骤如下:

[0014] 对用户数据进行初步筛选,以筛选出符合预设标准的数据;

[0015] 对筛选后的数据进行加密处理,用于确保数据在传输过程中的安全性;

[0016] 将加密后的数据分割成多个片段,适应区块链的存储结构;

[0017] 对每个数据片段生成哈希值,作为数据的唯一标识,确保数据的完整性和可追溯

性;

[0018] 编写智能合约,定义数据存储的规则和条件,用户保证数据的访问权限和存储位置;

[0019] 将数据片段和数据指纹通过智能合约上传到区块链网络,实现数据的去中心化存储;

[0020] 利用区块链网络中的多个节点对上传的数据进行验证,确保数据的一致性和不可篡改性;

[0021] 为存储在区块链上的数据构建索引;

[0022] 设定数据访问权限,确保只有授权的用户或系统对数据片段进行访问;

[0023] 在区块链网络中实现数据的多节点备份;

[0024] 通过智能合约实现数据的更新和维护规则;

[0025] 采用零知识证明隐私保护技术,确保用户数据的隐私性,即使在区块链上也能保持匿名性。

[0026] 进一步的,所述S1中对用户数据进行初步筛选的具体操作步骤如下:

[0027] 根据应用场景和业务需求,确定数据筛选的标准和规则,从各种来源收集用户数据;

[0028] 对收集到的数据进行清洗,去除无效、错误或不完整的数据记录,验证数据的准确性和一致性,确保数据符合预设的标准,去除重复的数据记录;

[0029] 根据数据类型和用途对数据进行分类,采用数据压缩技术减少数据的存储空间需求。

[0030] 进一步的,所述S2的具体操作步骤如下:

[0031] 确定用户画像所需属性,不包括可识别个人身份的敏感信息;

[0032] 收集并清洗用户行为数据,进行预处理以去除无效或无关信息;

[0033] 对用户数据进行匿名化处理,确保不包含可追溯到个人身份的信息;

[0034] 利用零知识证明技术,证明用户属性组别,避免泄露具体个人信息;

[0035] 对用户画像属性进行加密处理;

[0036] 整合加密属性,形成用于推荐算法的加密用户画像;

[0037] 采用差分隐私的隐私保护数据分析技术,分析用户画像,发现用户群体趋势和偏好;

[0038] 对用户画像进行验证和测试,确保准确性和隐私保护的有效性;

[0039] 设计定期更新机制,用于反映用户行为和偏好的最新变化,同时保护隐私;

[0040] 实现访问控制机制,确保只有授权的系统和人员对用户画像数据进行访问;

[0041] 定期进行数据访问审计;

[0042] 获取用户明确同意收集和处理数据,提供数据退出或删除选项。

[0043] 进一步的,所述S2中对用户画像进行验证和测试,确保准确性和隐私保护的有效性具体过程如下:

[0044] 确定衡量用户画像准确性和隐私保护效果的衡量指标包括:

[0045] 一致性:用户画像与实际用户行为的匹配程度;

[0046] 覆盖度:用户画像覆盖的用户特征和行为的广度;

- [0047] 可预测性:用户画像在预测用户未来行为时的有效性;
- [0048] 隐私保护:用户画像在保护用户隐私方面的性能;
- [0049] 从用户数据集中选择样本进行测试;
- [0050] 准备测试集,包括用户的实际行为数据和相应的用户画像数据;
- [0051] 针对确定的衡量指标进行逐一分析,具体的:
- [0052] 一致性检验:比较用户画像中的特征与用户的实际行为数据,评估一致性;
- [0053] 覆盖度分析:分析用户画像覆盖的用户特征和行为的广度;
- [0054] 可预测性测试:使用用户画像预测用户未来的行为,并与实际结果进行比较,评估预测的准确性;
- [0055] 隐私保护评估:通过混淆测试评估用户画像的隐私保护效果,确保即使在数据被非法访问的情况下,也无法准确推断出用户的具体信息,评估用户画像在保护用户隐私方面的性能;
- [0056] 通过A/B测试,对比不同用户画像构建方法的效果,选择最优的方法;
- [0057] 收集用户对推荐内容的反馈,评估用户画像的准确性和用户满意度;
- [0058] 使用统计方法分析用户画像数据,评估用户画像的可靠性和有效性;
- [0059] 模拟潜在的隐私攻击,测试用户画像的抗攻击能力。
- [0060] 进一步的,所述S3的具体操作步骤如下:
- [0061] 确定推荐目标 and 需求,包括推荐内容类型、用户画像属性及推荐逻辑规则;
- [0062] 设计智能合约逻辑,实现用户画像输入、推荐算法执行及推荐结果输出;
- [0063] 使用区块链编程语言编写智能合约代码;
- [0064] 在智能合约中嵌入隐私保护措施;
- [0065] 进行单元测试、集成测试和安全测试,确保智能合约的功能性和安全性;
- [0066] 将智能合约部署到区块链平台,实现去中心化执行;
- [0067] 将用户数据上链,确保数据不可篡改性和透明性;
- [0068] 调用智能合约,输入用户画像和参数,自动执行推荐逻辑;
- [0069] 输出推荐结果,并验证推荐结果是否符合预期推荐规则 and 标准;
- [0070] 收集用户反馈,优化推荐算法;
- [0071] 定期生成透明度报告,展示推荐逻辑调用次数和推荐结果分布;
- [0072] 定期对智能合约进行审计,确保逻辑正确性和安全性。
- [0073] 进一步的,所述S3中验证推荐结果是否符合预期推荐规则 and 标准的具体操作步骤如下:
- [0074] 首先通过推荐因素进行综合分析,其中推荐因素包括:
- [0075] 准确率:分析推荐结果中正确推荐数量与总推荐数量的比例;
- [0076] 上下文相关性:评估推荐结果与用户当前情境的相关性,并通过相关百分比进行量化,记为相关比;
- [0077] 个性化强度:衡量推荐结果的个性化程度,即推荐内容与用户独特属性的匹配度,并赋予1-100的匹配度评分,记为匹配值;
- [0078] 推荐结果的个性化创新度:推荐结果中包含的新颖元素 or 创新内容的比例,并记为个创比;

[0079] 将得到的准确率、相关比、匹分值及个创比归一化处理,代入以下公式:

$TPZ = 0.95(zq + xb + pp) + (gc + 1.25)^{1.21}$ 以得到推评值TPZ,式中zq、xb、pp及gc分别为准确率、相关比、匹分值及个创比,并以推评值TPZ作为衡量推荐结果验证的标准;

[0080] 再收集用户对推荐结果的反馈参数,用于对计算的推评值进行修正得到综分值ZFZ;

[0081] 将得到的综分值ZFZ与预设综分阈值进行比对,当综分值ZFZ大于综分阈值时,则判断推荐结果达到预设标准,反之则判断推荐结果未达到预设标准,当确定推荐结果未达到预设标准则根据用户对推荐结果的具体反馈优化推荐算法。

[0082] 进一步的,所述收集用户对推荐结果的反馈参数,用于对计算的推评值进行修正的过程如下:

[0083] 其中反馈参数包括:

[0084] 用户参数度:用户与推荐内容互动的深度和频率,并通过停留时间及互动次数进行量化,将得到的停留时间及互动次数归一化处理后分别乘以对应的权重因子并求和,得到用参值;

[0085] 用户决策时间:用户在接收推荐后做出决策所需的时间,用于反映推荐的相关性和吸引力;

[0086] 用户画像的动态更新频率,用户画像更新的频率和及时性,反映推荐系统对用户行为变化的响应速度;

[0087] 将得到的用参值、用户决策时间及用户画像更新频率归一化处理后,将用参值与用户画像更新频率的乘积与用户决策时间相除,得到用评比值,并以此用评比值作为衡量用户对推荐结果反馈的评价标准;

[0088] 将得到的推评值TPZ及用评比值归一化处理后代入以下公式:

$ZFZ = (TPZ + 1.22) * (1 - YPZ^{-1}) - 0.26$ 以得到综分值ZFZ,式中YPZ为用评比值,将得到的综分值ZFZ作为推荐结果最终的评估标准。

[0089] 进一步的,所述S4的具体步骤如下:

[0090] 确定并分类需要加密的用户行为数据类型;

[0091] 使用强加密算法对用户行为数据进行加密处理;

[0092] 管理加密密钥,确保密钥的安全性和生命周期;

[0093] 设计用户授权机制,获取用户对其数据收集和分析的同意;

[0094] 在分析前验证用户授权,确保数据使用符合用户意愿;

[0095] 实现安全的数据访问控制,限制未授权访问;

[0096] 在用户授权的情况下解密数据,并进行隐私保护的数据分析;

[0097] 采用差分隐私或同态加密技术保护解密后数据的隐私;

[0098] 生成并加密分析结果;

[0099] 记录和审计数据使用情况;

[0100] 提供用户反馈机制;

[0101] 制定数据泄露应对计划,用于应对数据安全事件。

[0102] 进一步的,所述S5的具体步骤如下:

- [0103] 确定激励机制的目标,包括提高用户参与度和数据质量;
- [0104] 调研用户需求和偏好,确定激励类型和用户接受度;
- [0105] 制定数据贡献标准,明确可获激励的数据类型和质量;
- [0106] 设计激励规则,包括条件、计算方式和发放时间;
- [0107] 使用智能合约自动执行激励规则,确保公正性和透明性;
- [0108] 进行激励机制的模拟测试,评估对用户行为和系统性能的影响;
- [0109] 实施激励机制后,收集用户反馈,评估效果和满意度;
- [0110] 根据反馈和系统表现调整优化激励机制;
- [0111] 向用户公开激励机制详细信息;
- [0112] 记录和审计激励发放情况;
- [0113] 平衡激励效果和隐私保护,避免用户隐私泄露;
- [0114] 提供用户退出激励机制的选项,尊重用户自主选择权。
- [0115] 与现有技术相比,本发明的有益效果是:
- [0116] 本发明,通过采用去中心化的数据存储方式,将用户数据存储在区块链上,利用区块链的不可篡改性和透明性,显著提高了数据的安全性,结合零知识证明等隐私保护技术,确保了用户在区块链上的匿名性,增强了用户对系统的信任度,这种信任是基于数据的加密处理和安全存储,以及智能合约的公正性与透明性,为用户提供了一个安全可靠的个性化推荐环境;
- [0117] 本发明,通过综合分析推荐结果的准确率、上下文相关性、个性化强度和个性化创新度,使用归一化处理和特定的计算公式,得到推评值,进而结合用户反馈参数进行修正,得到综分值,这一过程不仅优化了推荐算法,确保推荐内容的相关性和吸引力,而且通过定期收集用户反馈,动态调整推荐逻辑,有效提升了用户的满意度和参与度;
- [0118] 本发明,通过激励机制设计,鼓励用户贡献高质量数据,同时通过智能合约确保激励规则的自动执行,保障了激励过程的公正性和透明性,通过平衡激励效果与隐私保护,避免了在激励过程中对用户隐私的潜在泄露,提供用户随时退出激励机制的选项,尊重了用户的自主选择权,进一步强化了用户对自己数据的控制权和系统的透明度,这些措施共同促进了一个既激励用户参与,又严格保护用户隐私的推荐系统环境。

附图说明

- [0119] 为了便于本领域技术人员理解,下面结合附图对本发明作进一步的说明;
- [0120] 图1为本发明的方法流程图。

具体实施方式

[0121] 下面将结合实施例对本发明的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其它实施例,都属于本发明保护的范围。

[0122] 应当理解,本披露的说明书和权利要求书中使用的术语“包括”和“包含”指示所描述特征、整体、步骤、操作、元素和/或组件的存在,但并不排除一个或多个其它特征、整

体、步骤、操作、元素、组件和/或其集合的存在或添加。

[0123] 还应当理解,在此本披露说明书中所使用的术语仅仅是出于描述特定实施例的目的,而并不意在限定本披露。如在本披露说明书和权利要求书中所使用的那样,除非上下文清楚地指明其它情况,否则单数形式的“一”、“一个”及“该”意在包括复数形式。还应当进一步理解,在本披露说明书和权利要求书中使用的术语“和/或”是指相关联列出的项中的一个或多个的任何组合以及所有可能组合,并且包括这些组合。

[0124] 如图1所示,基于用户行为和偏好的个性化内容推荐方法,包括以下步骤:

[0125] 去中心化数据存储:将用户数据存储区块链上,确保数据的不可篡改性和透明性;

[0126] 首先对即将存储的数据进行初步筛选,具体过程如下:

[0127] 根据应用场景和业务需求,确定数据筛选的标准和规则,从各种来源收集用户数据,包括日志文件、用户输入、传感器数据等;对收集到的数据进行清洗,去除无效、错误或不完整的数据记录,验证数据的准确性和一致性,确保数据符合预设的标准,去除重复的数据记录;根据数据类型和用途对数据进行分类,采用数据压缩技术减少数据的存储空间需求,提高存储效率。

[0128] 完成初步筛选后再进行加密处理,以确保数据在传输过程中的安全性,将加密后的数据分割成多个片段,以适应区块链的存储结构,并提高数据存储的效率;对加密后的数据片段生成哈希值,作为数据的唯一标识,确保数据的完整性和可追溯性;

[0129] 编写智能合约,定义数据存储的规则和条件,包括数据的访问权限、存储位置等;将数据片段和数据指纹通过智能合约上传到区块链网络,实现数据的去中心化存储,利用区块链网络中的多个节点对上传的数据进行验证,确保数据的一致性和不可篡改性;为存储在区块链上的数据构建索引,便于后续的数据检索和分析,设定数据访问权限,确保只有授权的用户或系统可以访问特定的数据片段;

[0130] 在区块链网络中实现数据的多节点备份,提高数据的可靠性和容错性,通过智能合约实现数据的更新和维护规则,确保数据的实时性和准确性,采用零知识证明隐私保护技术,确保用户数据的隐私性,即使在区块链上也能保持匿名性。

[0131] 隐私保护的用户画像构建:通过零知识证明等密码学技术,构建不泄露用户具体信息的用户画像;

[0132] 确定用户画像需要包含的属性,例如年龄范围、兴趣偏好、消费习惯等,但不包括任何可以识别个人身份的敏感信息;收集用户的行为数据,如浏览记录、购买历史、搜索查询等;对收集到的数据进行清洗和预处理,去除无效或无关信息;对用户数据进行匿名化处理,确保在构建用户画像的过程中不包含任何可以追溯到个人身份的信息;

[0133] 利用零知识证明技术,证明用户属于特定的属性组,而无需透露具体的个人信息,对用户画像中的属性进行加密处理,确保即使数据被非法访问,也无法解读原始信息;将加密后的属性整合成一个加密的用户画像,该画像可以用于推荐算法,但不暴露用户的具体信息;采用隐私保护的数据分析技术,如差分隐私,对用户画像进行分析,以发现用户群体的一般趋势和偏好;对构建的用户画像进行验证和测试,确保用户画像的准确性,具体过程如下:

[0134] 确定衡量用户画像准确性和隐私保护效果的衡量指标,包括:

[0135] 一致性:用户画像与实际用户行为的匹配程度;覆盖度:用户画像覆盖的用户特征和行为的广度;可预测性:用户画像在预测用户未来行为时的有效性;

[0136] 隐私保护:用户画像在保护用户隐私方面的性能;从用户数据集中选择代表性的样本进行测试,确保样本的多样性和广泛性;准备测试集,包括用户的实际行为数据和相应的用户画像数据;

[0137] 针对确定的衡量指标进行逐一分析,具体的:

[0138] 一致性检验:比较用户画像中的特征与用户的实际行为数据,评估一致性。例如,检查用户画像中的兴趣偏好是否与用户的购买历史一致;覆盖度分析:分析用户画像覆盖的用户特征和行为的广度,确保用户画像能够涵盖大多数用户的行为模式;可预测性测试:使用用户画像预测用户未来的行为,如购买意向、内容偏好等,并与实际结果进行比较,评估预测的准确性;隐私保护评估:通过混淆测试评估用户画像的隐私保护效果,确保即使在数据被非法访问的情况下,也无法准确推断出用户的具体信息,评估用户画像在保护用户隐私方面的性能;

[0139] 对比不同用户画像构建方法的效果,选择最优的方法;收集用户对推荐内容的反馈,评估用户画像的准确性和用户满意度;使用统计方法分析用户画像数据,评估用户画像的可靠性和有效性;模拟潜在的隐私攻击,测试用户画像的抗攻击能力。

[0140] 设计机制以定期更新用户画像,以反映用户行为和偏好的最新变化,同时确保更新过程的隐私保护;实现访问控制机制,确保只有授权的系统 and 人员可以访问用户画像数据;定期进行数据访问和使用的审计,确保遵守隐私保护政策;获取用户的明确同意来收集和处理其数据,并提供用户随时退出或删除其数据的选项。

[0141] 智能合约推荐逻辑:利用智能合约实现推荐逻辑,确保推荐过程的公正性和透明性。

[0142] 确定推荐的目标和需求,包括推荐内容的类型、用户画像的属性、推荐逻辑的规则等,设计智能合约的逻辑,包括用户画像的输入、推荐算法的执行、推荐结果的输出等;使用 Solidity 或其他区块链编程语言编写智能合约代码,实现上述设计好的推荐逻辑;

[0143] 在智能合约中嵌入隐私保护措施,如数据加密、零知识证明等,确保用户数据的安全,在部署智能合约之前,进行充分的测试,包括单元测试、集成测试和安全测试,确保合约的功能性和安全性;将编写好的智能合约部署到区块链平台上,使其可以在区块链网络中执行,将用户数据按照去中心化数据存储的步骤上链,确保数据的不可篡改性和透明性;当需要进行推荐时,调用智能合约,输入用户画像和相关参数,由智能合约自动执行推荐逻辑,智能合约根据预设的推荐逻辑处理用户数据,输出推荐结果,并确保结果的公正性和透明性;对智能合约输出的推荐结果进行验证,判断推荐结果符合预期的推荐规则 and 标准;具体首先通过推荐因素进行综合分析,其中推荐因素包括:

[0144] 准确率:分析推荐结果中正确推荐数量与总推荐数量的比例;上下文相关性:评估推荐结果与用户当前情境的相关性,并通过相关百分比进行量化,记为相关比;个性化强度:衡量推荐结果的个性化程度,即推荐内容与用户独特属性的匹配度,并赋予1-100的匹配度评分,记为匹分值;推荐结果的个性化创新度:推荐结果中包含的新颖元素或创新内容的比例,并记为个创比;

[0145] 将得到的准确率、相关比、匹分值及个创比归一化处理,代入以下公式:

$TPZ = 0.95(zq + xb + pp) + (gc + 1.25)^{1.21}$ 以得到推评值TPZ, 式中zq、xb、pp及gc分别为准确率、相关比、匹分值及个创比, 并以推评值TPZ作为衡量推荐结果验证的标准;

[0146] 再收集用户对推荐结果的反馈参数, 用于对计算的推评值进行修正, 其中反馈参数包括:

[0147] 用户参数度: 用户与推荐内容互动的深度和频率, 并通过停留时间及互动次数进行量化, 将得到的停留时间及互动次数归一化处理后分别乘以对应的权重因子并求和, 得到用参值; 用户决策时间: 用户在接收推荐后做出决策所需的时间, 用于反映推荐的相关性和吸引力; 用户画像的动态更新频率, 用户画像更新的频率和及时性, 反映推荐系统对用户行为变化的响应速度;

[0148] 将得到的用参值、用户决策时间及用户画像更新频率归一化处理后, 将用参值与用户画像更新频率的乘积与用户决策时间相除, 得到用评比值, 并以此用评比值作为衡量用户对推荐结果反馈的评价标准; 将得到的推评值TPZ及用评比值归一化处理后代入以下公式: $ZFZ = (TPZ + 1.22) * (1 - YPZ^{-1}) - 0.26$ 以得到综分值ZFZ, 式中YPZ为用评比值, 将得到的综分值ZFZ作为推荐结果最终的评估标准; 将得到的综分值ZFZ与预设综分阈值进行比对, 当综分值ZFZ大于综分阈值时, 则判断推荐结果达到预设标准, 反之则判断推荐结果未达到预设标准, 当确定推荐结果未达到预设标准则根据用户对推荐结果的具体反馈优化推荐算法。

[0149] 根据用户反馈和系统性能监控结果, 对智能合约进行升级和优化, 以提高推荐系统的准确性和用户体验; 定期生成智能合约执行的透明度报告, 包括推荐逻辑的调用次数、推荐结果的分布等, 以增强系统的透明度; 定期对智能合约进行审计, 确保其逻辑的正确性和安全性, 防止潜在的漏洞和攻击。

[0150] 用户行为的加密分析: 对用户行为数据进行加密处理, 仅在用户授权的情况下进行分析。

[0151] 确定需要加密的用户行为数据类型, 如浏览记录、点击行为、搜索查询等, 并进行分类; 对识别出的用户行为数据进行加密处理, 使用强加密算法(如AES)确保数据的机密性; 管理加密过程中使用的密钥, 确保密钥的安全性和生命周期管理; 设计用户授权机制, 允许用户明确同意其数据被收集和分析;

[0152] 在分析加密数据之前, 验证用户是否已授权, 确保数据的使用符合用户意愿; 实现安全的数据访问控制, 确保只有授权的系统或人员可以访问加密数据; 在用户授权的情况下, 使用相应的密钥对加密数据进行解密, 以便进行分析; 采用隐私保护的数据分析技术, 如差分隐私或同态加密, 以保护用户数据的隐私。

[0153] 根据解密后的数据, 生成分析结果, 如用户行为模式、偏好趋势等, 将分析结果再次加密, 以确保在存储和传输过程中的安全性; 记录和审计数据的使用情况, 确保数据的使用符合隐私政策和法律法规; 提供用户反馈机制, 允许用户了解其数据如何被使用, 并提供修改或撤销授权的选项; 制定数据泄露应对计划, 以应对可能的数据安全事件。

[0154] 激励机制设计: 设计一种激励机制, 鼓励用户贡献数据同时保护其隐私权益。

[0155] 确定激励机制的目标, 包括提高用户参与度、提高数据的多样性和质量、鼓励用户长期参与等; 调研用户的需求和偏好, 了解他们对于激励机制的期望和接受度; 确定激励的

类型,如物质奖励(代币、折扣券、礼品等)、精神奖励(排行榜、徽章、认证等)或服务奖励(高级功能、个性化服务等),设计激励机制时,确保用户数据的使用和处理遵循隐私保护原则,不侵犯用户隐私;

[0156] 制定用户贡献数据的标准和要求,明确何种类型和质量的数据可以获得激励,设计具体的激励规则,包括激励的条件、激励的计算方式、激励的发放时间等;使用智能合约自动执行激励规则,确保激励的公正性和透明性;在实施前对激励机制进行模拟测试,评估其对用户行为和系统性能的影响;在激励机制实施后,收集用户的反馈,了解激励机制的实际效果和用户满意度;

[0157] 根据用户反馈和系统表现,对激励机制进行调整和优化,向用户公开激励机制的详细信息,包括激励的计算方法、发放流程等,提高透明度;记录和审计激励的发放情况,确保激励机制的执行符合预期,在设计激励机制时,平衡激励效果和隐私保护的需求,避免过度激励导致用户隐私泄露;提供用户随时退出激励机制的选项,尊重用户的自主选择权。

[0158] 以上公开的本发明优选实施例只是用于帮助阐述本发明。优选实施例并没有详尽叙述所有的细节,也不限制该发明仅为的具体实施方式。显然,根据本说明书的内容,可作很多的修改和变化。本说明书选取并具体描述这些实施例,是为了更好地解释本发明的原理和实际应用,从而使所属技术领域技术人员能很好地理解和利用本发明。本发明仅受权利要求书及其全部范围和等效物的限制。

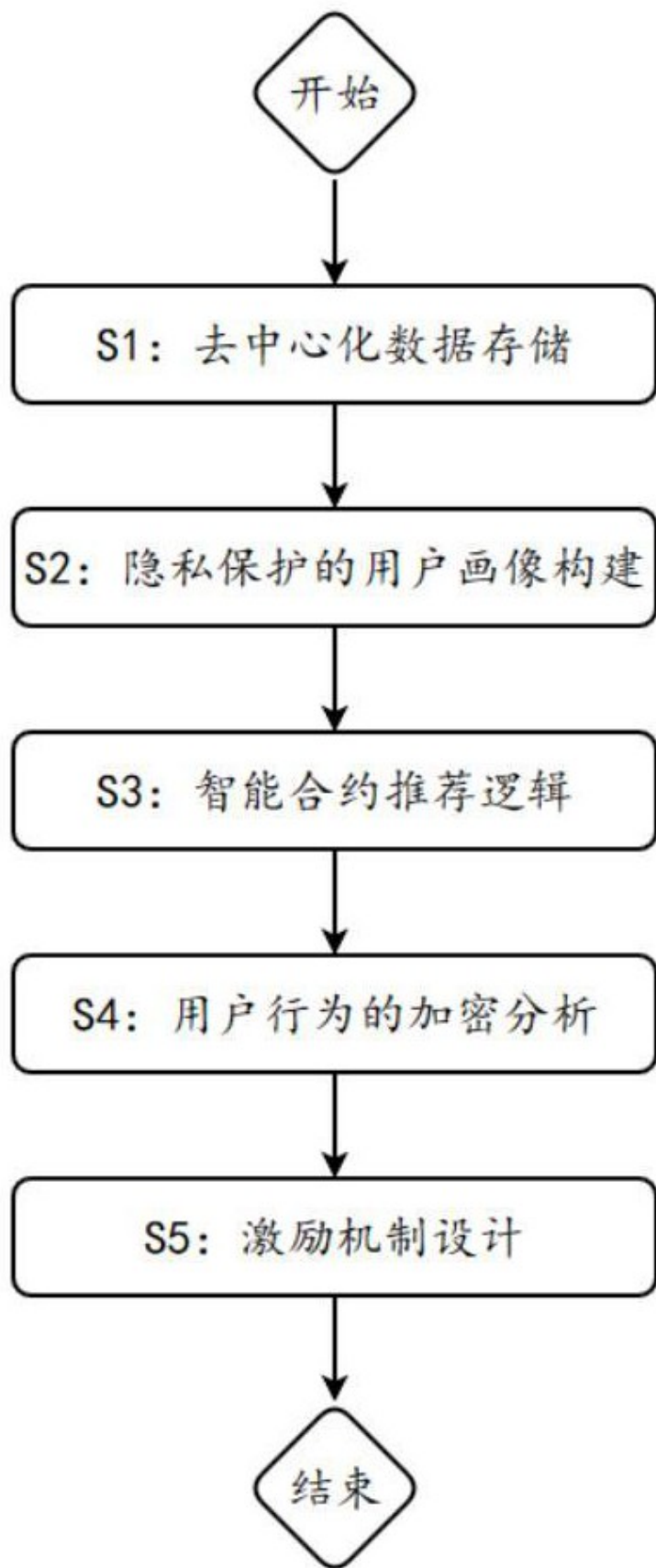


图 1