ISSN:2661-3719(Print);2661-3727(Online)

电商平台消费者数据隐私保护模型的构建与实证分析

陈毓秀　李家耀
广州科技职业技术大学　广东　广州 510550

摘　要：本文从电商平台消费者数据隐私保护的必要性出发，通过调研和分析不同类型的数据，将其进行分类处理，设计出一套由数据加密、访问控制和匿名化等策略构成的隐私保护模型，并通过实验验证了其有效性。
关键词：电商平台；消费者；数据隐私；保护模型

Construction and empirical analysis of the consumer data privacy protection model of the e-commerce platform

Yuxiu Chen，Jiayao Li
Guangzhou Vocational University of Science and Technology Guangzhou, Guangdong, 510550

Abstract: Based on the necessity of consumer data privacy protection of e-commerce platform, this paper classifies and analyzes different types of data, designs a set of privacy protection model composed of data encryption, access control and anonymity strategies, and verifies its effectiveness through experiments.
Key words: e-commerce platform; consumer; data privacy; and protection model

随着数字经济的快速发展和电子商务法的实施，消费者对个人隐私的保护日益重视，电商平台对此也在不断加强规范。但在电商平台与消费者之间的隐私保护博弈中，由于信息不对称和自身效用最大化的影响，难免会存在一些道德风险决策。消费者对个人隐私保护意识不足，也会导致平台未经允许擅自使用用户非必要数据的情况出现，使得平台与消费者签订的合同无法有效保护消费者的个人数据。

1. 电商平台消费者数据隐私保护的必要性

在电商平台中，平台商家根据消费者用户的个人位置、消费习惯、收入分布等信息进行定向推送产品与服务信息，用户可能察觉不到平台企业的数据采集情况。此外，有部分电商平台严重侵害了消费者的权益，将收集到的海量用户信息进行信息倒卖或跨平台的信息寻租，以人工智能为基础对个人信息进行联网监控，这对数智化时代的个人隐私保护提出了严峻的挑战。数据隐私保护是电商平台发展中面临的严峻挑战之一，消费者数据隐私保护事关消费者个人信息安全，其远远不止是个人隐私泄露问题，还涉及消费者的财产安全、人身安全等重大问题。在电商平台中，数据隐私保护是一个重要的问题。要理解数据隐私保护的挑战和意义，需要对数据隐私和数据安全进行区分。数据安全通常是指保护数据的完整性、可用性和保密性，而数据隐私主要强调保护数据的隐私性，防止个人敏感信息被滥用或泄露。在实际生产生活中，数据隐私泄露的案例屡见不鲜，电商平台也不例外。这也为如何保护消费者数据隐私提出了巨大挑战。

2. 相关技术概述

对于消费者数据隐私模型的构建，相关技术概述是非常重要的一个环节，算法的选择和应用、数据的加密和解密等技术方面都需得到充分考虑。确保消费者个人数据的安全才能让消费者安心使用电商平台。数据加密与数据脱敏技术是重要的数据隐私保护技术手段，对敏感数据进行加密和脱敏可以有效避免数据泄露和滥用。特别是隐私保护算法相关技术的应用，通过采用差分隐私、同态加密、安全多方计算等技术，在保持数据分析结果准确度的同时，最大限度保护消费者的隐私权。采用不同的数据隐私保护模型，其实现方式也有所不同。将构建适合电商平台的消费者数据隐私保护模型，该模型力图从数据收集、存储、传输和分析等各个环节，采取综合技术手段，保护消费者数据隐私和数据安全。

3. 数据分类与处理

3.1 数据分类方法

3.1.1 基于属性的分类。其目的是将消费者的隐私数据根据其属性进行分类，以便针对不同属性数据采用不同的保护措施，保护消费者的隐私数据。先明确属于哪些属性，然后根据属性值的不同对数据进行分类，从而

实现对数据的分类。

3.1.2 基于哈希函数的数据分类方法。该分类方法使用特定的哈希函数算法，对相似的数据进行分类。为了提高分类准确性，需要选择合适的哈希函数算法，并且要对数据进行处理，以确保数据的唯一性。

3.1.3 采用聚类方法对数据进行分类。聚类方法是一种无监督学习方法，根据样本之间的相似性将样本聚成不同的群体。使用聚类方法实现数据分类时，需要先选择合适的聚类算法，再根据样本的特征值对数据进行聚类。

3.2 数据处理流程

3.2.1 数据采集一环节非常重要，涉及数据来源的合法性和数据的真实性。在采集数据时，应注意数据的来源，数据是否已获得消费者的允许，在不侵犯消费者隐私的情况下采集数据，并对数据来源进行合法性验证。对于采集到的数据进行预处理是为了去除无用的噪声和错误，以保证数据质量。

3.2.1 预处理阶段一般包括数据清洗、数据变换、特征选择等步骤，通过这些步骤可以更精准地描述和解释数据信息。

3.2.3 数据分析主要是为了了解数据的属性、结构和规律等，从中挖掘有用的信息。同时，数据分析还可以帮助确定适当的数据挖掘方法和模型，为后续的数据挖掘提供依据。

3.2.4 数据挖掘是整个数据处理流程的核心，在从海量数据中发现有用的、隐含的信息，并将这些信息用于决策和规划。数据挖掘一般包括分类、聚类、关联规则挖掘、异常检测等技术。

3.2.5 数据可视化展示是将数据转换为图表、图形等形式，以便于人们观察和分析。数据可视化可以使数据形象直观，更容易被人们理解和应用。

3.3 数据加密与解密

3.3.1 数据加密技术。数据加密是一种保护数据隐私的技术手段。数据加密技术主要采用对称和非对称两种方式。对称加密方式是指发送方和接收方需要共享一个密钥。加密的过程中，经过明文输入，利用相同的密钥进行加密处理后，获得密文输出。解密的过程中，再利用相同的密钥进行解密操作，得到明文。非对称加密方式则需要一对密钥，分别用来加密和解密数据。

3.3.2 数据解密技术。数据解密技术是数据加密逆过程。在数据传输过程中，接收方获取加密的密文数据，必须使用密钥进行解密才能够获得原始的明文数据。数据解密过程与数据加密过程相似，但顺序相反，即先对密文使用密钥进行解密操作，再得到明文数据。

3.3.3 数据加密与解密的应用。在电商平台消费者数据隐私保护模型中，数据加密与解密技术起到了重要作用，可有效地提高用户数据隐私保护的安全性。数据加密与解密技术通过使用密钥来对数据加密和解密，可以使得数据在传输过程中不易被窃取，确保数据的合法性和安全性。

4. 隐私保护策略

4.1 数据访问控制

数据访问控制方法是保护消费者数据隐私的有效方式之一，平台通过指定数据访问规则和相关权限，限制访问数据的人员和范围，从而避免越权访问和滥用数据的风险。这种方法可以采用基于角色的访问控制、基于数据的访问控制、基于灵活访问控制框架等多种技术手段，实现对数据的管理和保护。例如，在基于角色的访问控制方法中，平台可以针对不同的角色设置不同的权限，从而有效控制这些人员获取数据的权限和范围。此外，数据脱敏技术也是另外一种常见的数据隐私保护方法。平台采用各种算法和方法对敏感数据进行加密、脱敏、掩码等操作，从而保证敏感数据的隐私性和安全性。在电商平台中，数据访问控制方法和数据脱敏技术是两种非常重要的隐私保护方法。使用这些技术手段可以有效保护消费者的数据隐私，避免数据泄露和滥用等风险位。

4.2 数据脱敏技术

数据脱敏技术是一种常用的隐私保护手段，其目的是在保证数据使用价值的前提下，尽可能地减少敏感信息泄露的风险。一般来说，数据脱敏技术主要包括数据加密、数据混淆和数据掩码等几种方式。其中数据加密是指通过一定的算法将明文数据转换为密文数据，只有获得相应密钥的人才能解密并查看明文数据，同时保护了数据隐私；数据混淆则是通过随机化和扰动等方式，将敏感数据变得难以理解，从而降低数据泄露风险；数据掩码是指在数据源头对数据进行修饰，比如以“*”或“#”代替一些敏感数据，从而避免了敏感数据的明文存储。数据脱敏技术并不是只有一种方式，不同的方式对应的实现难度、保护效果、使用场景等都不尽相同，因此在使用数据脱敏技术时，需要根据实际情况选择最合适的方式，以最大化实现数据隐私保护的效果。另外，在应用数据脱敏技术时，要注意脱敏后数据质量的改变以及脱敏对数据分析的影响，需要对这些因素进行充分的评估，从而确保应用数据脱敏技术不会对数据使用带来负面的影响。

4.3 隐私保护协议

隐私保护协议由平台和用户双方共同签署，规定了在平台上用户提交数据的范围和使用方式。它为消费者提供了非常有利的保护，确保了用户在平台上的数据不会被滥用。在制定隐私保护协议时，平台需要充分考虑到用户的利益，确保用户的信息不会被泄露或滥用。隐私保护协议的实现需要依靠技术手段，主要是通过数据加密、数据脱敏、访问控制等技术手段来保障用户数据的安全性。其中，数据加密可以有效地保护用户数据的机密性，数据脱敏技术可以在保护数据质量的同时保护

用户隐私，访问控制技术可以限制非授权用户的访问权限。隐私保护协议的具体实现应该根据实际应用场景进行调整。随着电商平台的不断发展，应用场景也在不断变化，因此，隐私保护协议需要进行不断的优化和完善。比如，在某些特定场景下，需要采用更强的加密算法来保证数据的安全性。为了进一步保护用户数据的安全性，平台应该不断加强对隐私保护协议的监管和执行力度。同时，消费者也应该对自己的数据有更加明确的认识，并积极维护自己的数据安全。

4.4 访问日志审计

访问日志审计是一种重要的数据隐私保护策略，可以及时发现并防范安全威胁，但需要综合考虑安全性、隐私保护和效率等因素，采用多种技术和措施进行配合，提高平台的安全性和可靠性，为用户提供优质服务。访问日志是电商平台记录用户访问历史的重要数据，根据审计结果可以及时发现潜在的安全漏洞和违规行为，从而及时采取有效的应对措施，保护用户隐私和平台安全。访问日志审计包括日志记录、日志收集、日志解析和日志分析等环节。数据管理员需要定期审查日志，及时发现异常访问行为，例如多次尝试登录失败、非法访问以及数据篡改等。此外，还需要保障访问日志的完整性和保密性，防止被篡改、泄露或者丢失。通过这些功能可以实时监控用户的访问行为，同时提高平台的安全性和合规性，为用户提供更加安全、可靠的服务。

5. 实证分析

5.1 实验环境

硬件环境：一台配置为 Intel Core i7 处理器，16GB 内存，1T 硬盘的计算机作为实验主机。

软件环境：Python 编程语言的 pandas，numpy 和 scikit-learn 等第三方库进行数据的处理、分析以及模型的构建等，MySQL 数据库存储实验数据，使用 MySQL 的查询语句进行数据的筛选和整合。

5.2 实验设计

5.2.1 数据收集。从现有的电商平台的用户数据中，随机选取 200 个用户，包括性别、年龄、收入等多维度信息。使用分层抽样的方法，保证样本的代表性和可靠性。据此构建了实验所需数据集。

5.2.2 实验组与对照组的划分。在实验组中，采用构建的数据隐私保护模型对用户数据进行了处理；对照组则直接使用未经处理的数据。为了避免建模过程中的主观干预，采用随机化的方法将样本分成两组，并且在两组中保证样本的均衡性。

5.2.3 实验方案的设计。将实验对象分别随机分配至实验组和对照组，对两组样本进行处理和比较。选择指标来评价数据隐私保护模型的有效性和可行性：数据处理后的数据质量、用户对数据隐私保护的知晓度和满意度、用户对数据隐私保护的信任度等。

5.3 实验结果分析

通过对实验结果进行分析，以验证该模型的有效性和可行性。在实验环境中模拟了一个电商平台，随机生成的 200 个用户数据。然后，将使用不同的数据保护策略应用于这些数据，并对应用策略后的数据进行实验。在实验设计中，选取传统的数据加密、数据分割和基于数据加密和数据分割的保护策略。通过对比这三种策略的实验结果，评估提出的保护模型的有效性。传统的数据加密策略在保护数据隐私方面表现出色，可有效防止数据泄露和信息窃取。但是，它也存在一定的缺陷，如数据访问效率较低和数据结构复杂等。相比之下，数据分割策略具有更好的性能，但安全性不够高，易受到攻击和破解。

基于数据加密和数据分割的保护策略不仅保证了数据的安全性，而且还具有较高的数据访问效率和灵活性。通过在实验中的应用和对比，构建的模型对保护电商平台消费者数据隐私要具有很好的可行性和可靠性，基于多方参与的思想，通过建立安全的数据共享、安全的数据交换和安全的数据存储等机制，为消费者提供了更加完善的数据隐私保护方案。

结语

总之，在电商平台上，消费者的数据一直都是非常敏感的话题。保护消费者的数据隐私不仅是法律规定的要求，同时也是商家和平台对消费者的一种尊重和信任。在电商平台上，对消费者个人隐私信息的保护是至关重要的，要构建有效且科学的电商平台消费者数据隐私保护模型。

参考文献：

[1] 李大元，潘壮，肖元英 . 大数据时代消费者隐私协同保护研究 [J]. 商学研究 ,2022,29(05):5-10.

[2] 杨昌慧 . 大数据背景下电商平台的数据伦理问题及应对措施 [J]. 老字号品牌营销 ,2022(09):54-56.

[3] 陈圣宇，李薇 . 数据挖掘对网络消费者隐私权的影响 [J]. 南方企业家 ,2018(03):211.