多模态数据融合场景下电子商务数据安全保障机制研究

郑羽洁
广西职业师范学院　广西南宁　530007

摘　要：在当今数字化时代，电子商务凭借其便捷性和高效性蓬勃发展，多模态数据融合也成为电子商务领域的新趋势。多模态数据涵盖了文本、图像、音频等多种形式，为电商企业带来更丰富的客户信息和商业洞察。然而，这也使得电子商务数据面临更为复杂的安全挑战，如数据泄露、恶意攻击等。构建科学有效的电子商务数据安全保障机制，对于保护消费者权益、维护电商市场秩序、促进电子商务健康发展具有至关重要的意义。

关键词：多模态数据融合；电子商务；数据安全；保障机制

引言

随着信息技术的飞速发展，电子商务在经济活动中的地位日益凸显。多模态数据融合作为新兴技术，正深度融入电子商务领域，极大地丰富了数据资源，提升了商业决策的精准度。多模态数据涵盖文本、图像、音频、视频等多种形式，其融合能全面且立体地刻画用户画像与市场动态。然而，这种融合也让电子商务数据面临前所未有的安全风险。数据泄露、恶意攻击、隐私侵犯等问题频发，不仅损害消费者利益，还影响电商企业的信誉与运营。构建有效的电子商务数据安全保障机制迫在眉睫，关乎行业的健康发展与市场的稳定运行。

1. 多模态数据融合对电子商务数据安全的挑战

1.1 数据来源复杂，增加数据识别和管理难度

在多模态数据融合场景下，电子商务的数据来源极为广泛。涵盖用户在社交平台的互动信息，如评论、点赞、分享等，这些信息反映了用户的兴趣偏好和社交关系；还有购物平台的浏览记录、搜索关键词，体现了用户的消费意向；以及移动设备的定位数据，可用于分析用户的活动范围和消费场景。不同来源的数据具有不同的格式和特点，文本数据可能存在语义模糊性，图像数据可能受到拍摄环境和设备的影响，音频和视频数据则包含大量的冗余信息。

这种复杂的数据来源使得准确识别数据类型和来源变得困难。在进行数据整合时，难以清晰界定每条数据的归属和用途。同时，不同来源的数据在质量和规范性上存在差异，给数据的管理带来了极大挑战。例如，一些用户在社交平台的发言可能随意且不规范，需要花费大量精力进行清洗和整理，增加了数据管理的成本和难度。

1.2 融合过程易产生安全漏洞，威胁数据完整性

多模态数据融合涉及多种技术和算法，在数据整合和处理过程中，容易出现安全漏洞。不同格式的数据在转换和融合时，可能会因为算法的不完善而导致数据丢失或错误。例如，在将图像数据与文本数据进行融合时，如果算法对图像特征的提取不准确，可能会导致融合后的数据无法准确反映真实情况。

数据融合过程中的接口和传输环节也可能成为攻击的目标。恶意攻击者可以利用这些漏洞篡改数据，从而破坏数据的完整性。比如，在数据传输过程中，如果没有采取有效的加密措施，攻击者可能会拦截并修改数据，导致电子商务决策所依据的数据不准确，进而影响企业的运营和决策。[1]一旦数据完整性受到威胁，可能会引发一系列问题，如客户订单错误、营销策略失误等，给企业带来巨大的损失。

1.3 隐私保护难度加大，面临更多法律风险

多模态数据包含了大量用户的敏感信息，如个人身份、消费习惯、健康状况等。数据融合使得这些信息更加集中和关联，一旦泄露，将对用户的隐私造成严重威胁。例如，将用户在不同平台的消费记录和健康数据融合后，可能会泄露用户的一些隐私细节，如患有某种疾病还购买了相关的特殊商品。

随着数据保护法规的不断完善，电子商务企业在数据收集、使用和共享过程中面临着更严格的法律约束。如果企业在数据隐私保护方面措施不当，将面临巨额罚款和法律诉讼。比如，欧盟的《通用数据保护条例》（GDPR）对企业的数据处理行为有严格规定，一旦企业违反相关规定，可能会面临高额罚款。此外，隐私泄露事件还会损害企业的声誉，

导致用户信任度下降，影响企业的长期发展。

2. 电子商务数据安全保障机制的目标与原则

2.1 确保数据的保密性，防止信息泄露

电子商务涉及大量用户的敏感信息，如个人身份、信用卡号、交易记录等，确保这些数据的保密性至关重要。保障数据保密性意味着采取一系列措施，阻止未经授权的访问和信息泄露。加密技术是实现数据保密的关键手段之一。在数据传输过程中，使用 SSL/TLS 协议对数据进行加密，使数据在网络中以密文形式传输，即使数据被拦截，攻击者也无法获取其中的敏感信息。

在数据存储方面，采用对称加密或非对称加密算法对数据进行加密存储。例如，使用 AES 算法对数据库中的用户信息进行加密，只有授权的用户和系统才能通过正确的密钥进行解密。此外，访问控制也是保障数据保密性的重要措施。通过设置严格的用户权限,限制不同用户对数据的访问范围。[2] 只有经过授权的人员才能访问特定的数据，防止内部人员的违规操作和外部的非法入侵，从而有效防止信息泄露。

2.2 维护数据的完整性，保证数据准确可靠

数据的完整性是指数据在存储和传输过程中不被篡改、损坏或丢失。在多模态数据融合场景下，数据来源复杂，格式多样，维护数据完整性面临更大挑战。为了保证数据的准确可靠，需要采用数据校验技术。例如，使用哈希算法对数据进行哈希计算，生成哈希值。在数据传输和存储过程中，定期对数据的哈希值进行验证，如果哈希值发生变化，则说明数据可能被篡改。

同时，建立数据备份和恢复机制也是维护数据完整性的重要手段。定期对重要数据进行备份，并存储在不同的位置。当数据出现损坏或丢失时，可以及时从备份中恢复数据，确保业务的连续性。此外，在数据融合过程中，要对不同来源的数据进行严格的质量控制和审核，确保融合后的数据准确反映真实情况。

2.3 保障数据的可用性，确保业务正常运行

数据的可用性是指在需要时能够及时、准确地获取数据。在电子商务中，数据的可用性直接关系到业务的正常运行。如果数据不可用，可能会导致订单处理延迟、客户服务中断等问题，影响企业的声誉和经济效益。为了保障数据的可用性，需要建立高效的存储和管理系统。[3] 采用分布式存储技术，将数据分散存储在多个节点上，提高数据的可靠性和可访问性。

需要建立数据冗余和容错机制。例如，采用 RAID 技术对磁盘阵列进行配置，当部分磁盘出现故障时，仍然可以保证数据的正常访问。此外，还要制定应急预案，应对可能出现的自然灾害、网络攻击等突发事件。在发生故障时，能够迅速切换到备用系统，确保数据的可用性，使业务能够尽快恢复正常运行。

3. 多模态数据融合场景下电子商务数据安全保障机制的构建策略

3.1 加强数据加密技术，保障数据传输和存储安全

数据加密是保障电子商务数据安全的基础手段。在数据传输过程中，采用先进的加密算法对数据进行加密处理，可有效防止数据在网络传输时被窃取或篡改。例如，SSL/TLS 协议广泛应用于电子商务网站，它能在客户端和服务器之间建立安全的加密通道，确保数据在传输过程中的保密性和完整性。使用高强度的加密密钥，如 256 位的 AES 加密算法，能大大提高加密的安全性，让攻击者难以破解。

在数据存储方面，对存储在服务器和数据库中的数据进行加密存储同样重要。可以采用对称加密和非对称加密相结合的方式，将数据以密文形式保存。对于重要的敏感数据，如用户的信用卡信息、身份证号码等，采用单独的加密策略，进一步增强数据的安全性。定期更新加密密钥，防止密钥被破解后导致数据泄露，从而全方位保障数据传输和存储的安全。

3.2 建立数据访问控制体系，规范用户操作权限

建立完善的数据访问控制体系是规范用户操作权限、保障数据安全的关键。首先，对用户进行严格的身份认证，采用多种认证方式相结合，如用户名和密码、短信验证码、指纹识别等，确保只有合法的用户才能访问系统和数据。为不同的用户角色分配不同的操作权限，根据其工作职责和业务需求，精确控制其对数据的访问范围和操作类型。[4] 例如，普通客服人员只能查看部分客户的基本信息，而高级管理人员则可以访问更全面的数据。

设置审计和监控机制，对用户的操作行为进行实时监控和记录。一旦发现异常操作，如未经授权的访问、数据篡改等，系统能及时发出警报并采取相应的措施。定期对用户权限进行审查和调整，确保权限分配始终符合用户的实际工作需求，防止因权限滥用而导致的数据安全问题。

3.3 运用人工智能和机器学习技术，实现数据安全智能监测

人工智能和机器学习技术在数据安全监测方面具有独特的优势。利用机器学习算法对大量的历史数据进行分析和学习，建立数据安全模型。该模型可以识别正常的数据访问模式和异常行为模式，如异常的登录时间、频繁的数据下载等。当系统检测到异常行为时，能自动触发预警机制，及时通知管理员进行处理。

人工智能技术还可以实现对数据的实时监测和分析。通过对多模态数据的融合分析，能够更全面地了解数据的安全状况。例如，结合用户的行为数据、设备信息和网络流量等多方面数据，判断是否存在潜在的安全威胁。不断优化和更新数据安全模型，以适应不断变化的安全环境和攻击手段。

4. 电子商务数据安全保障机制的实施与监督

4.1 制定详细的实施计划，明确各阶段任务和责任

制定详细的实施计划是电子商务数据安全保障机制落地的关键。该计划需依据多模态数据融合场景的特点和企业自身业务需求来制定。将整个实施过程划分为不同阶段，如准备阶段、实施阶段和优化阶段。在准备阶段，要进行全面的风险评估，识别可能存在的数据安全隐患，确定保障机制的目标和范围。同时，收集和整理相关的数据资源，为后续的实施工作做好准备。

明确各阶段的具体任务和责任。每个阶段都应有明确的任务清单，包括技术措施的实施、人员培训安排、制度建设等。将任务分配到具体的部门和个人，确保责任落实到位。例如，技术部门负责数据加密技术的应用和系统的安全配置，人力资源部门负责组织人员培训，法务部门负责审查相关的规章制度是否符合法律法规要求。通过明确任务和责任，提高实施效率，确保保障机制能够顺利推进。

4.2 加强人员培训，提高员工数据安全意识

员工是电子商务数据安全保障的重要环节，加强人员培训、提高员工的数据安全意识至关重要。开展定期的数据安全培训课程，内容涵盖数据安全法规、安全操作规范、常见的安全威胁及应对方法等。通过案例分析和模拟演练，让员工直观地了解数据安全的重要性和数据泄露可能带来的严重后果。

针对不同岗位的员工，制定个性化的培训方案。例如，对于技术人员，培训重点放在数据加密技术、网络安全防护等方面；对于业务人员，培训则侧重于数据的合理使用和保护客户隐私。[5] 鼓励员工积极参与数据安全管理，建立奖励机制，对在数据安全方面表现突出的员工给予表彰和奖励。通过提高员工的数据安全意识，形成全员参与的数据安全防护体系。

4.3 建立监督评估机制，定期检查和改进保障机制

建立监督评估机制是确保电子商务数据安全保障机制持续有效的重要手段。成立专门的数据安全监督小组，负责对保障机制的实施情况进行定期检查和评估。检查内容包括技术措施的执行情况、人员的操作合规性、制度的落实情况等。采用多种评估方法，如内部审计、外部评估机构测评等，确保评估结果的客观公正。

根据监督评估的结果，及时发现保障机制存在的问题和不足，并制定改进措施。对于发现的安全漏洞，要及时进行修复；对于不合理的制度和流程，要进行优化和完善。定期对保障机制进行更新和升级，以适应不断变化的技术环境和安全威胁。通过持续的监督评估和改进，不断提高电子商务数据安全保障机制的有效性和可靠性。

5. 结语

多模态数据融合为电子商务带来了新的发展机遇，也带来了前所未有的数据安全挑战。构建有效的电子商务数据安全保障机制，是应对这些挑战的关键。通过明确多模态数据融合对数据安全的挑战，确立保障机制的目标与原则，构建合理的保障策略，并加强实施与监督，能够为电子商务数据安全提供坚实保障。随着技术的不断进步和应用场景的不断拓展，数据安全问题将持续演变。因此，需要持续关注和研究新的安全威胁，不断优化和完善数据安全保障机制，以适应电子商务行业的快速发展，确保行业的稳定与健康。

参考文献

[1] 江月 . 探讨大数据技术在电子商务数据分析中的应用 [J]. 中国储运 ,2024,(04):109-110.

[2] 程训勇 . 计算机网络安全技术在电子商务运维中的有效应用 [J]. 科技创新与应用 ,2024,14(13):171-174.

[3] 冀巧然 . 算法决策对电子商务隐私安全的影响研究 [J]. 现代商业 ,2025,(01):63-66.

[4] 李泳佳 . 数字经济背景下跨境电子商务发展的机遇与挑战研究 [J]. 中国商论 ,2025,34(03):39-42.

[5] 王靖一 . 大数据在电子商务个性化推荐系统中的应用 [J]. 商场现代化 ,2025,(12):28-30.

项目类型：广西高校中青年教师科研基础能力提升项目，《基于“AI + Web 3.0”的全球电子商务跨境数据安全治理策略研究》项目编号：2024KY0933