

智能问答系统中的隐私保护与数据安全技术研究

张森达, 崔昕, 曲延刚, 刘博, 孙健
北京中电普华信息技术有限公司, 北京 102200
DOI:10.61369/EPTSM.2025010008

摘要： 文章围绕智能问答系统展开论述，概述了智能问答系统的定义、特点和技术架构，介绍了数据加密、匿名化、访问控制等隐私保护技术及其在数据收集、处理、输出阶段的应用。同时讲解了数据备份与恢复、入侵检测与防御、安全审计与监控等数据安全技术，分析了这些技术在系统架构、存储、传输层面的应用。

关键词： 智能问答系统；隐私保护；数据安全技术

Research on Privacy Protection and Data Security Technology in Intelligent Question Answering System

Zhang Senda, Cui Xin, Qu Yangang, Liu Bo, Sun Jian
Beijing CLP Puhua Information Technology Co., LTD. Beijing 102200

Abstract： This paper focuses on intelligent question answering system, summarizes the definition, characteristics and technical framework of intelligent question answering system, introduces data encryption, anonymization, access control and other privacy protection technologies and their applications in data collection, processing and output stage. At the same time, it explains data security technologies such as data backup and recovery, intrusion detection and prevention, security audit and monitoring, and analyzes the application of these technologies in system architecture, storage and transmission.

Keywords： intelligent question answering system; privacy protection; data security technology

在当今数字化时代，智能问答系统正广泛应用于众多领域，从客户服务到个人信息查询等，随着其应用的深入，隐私保护与数据安全成为了至关重要的议题。近年来，一系列文件和政策凸显了这一问题的紧迫性，如《中华人民共和国网络安全法》明确规定了网络运营者对用户信息保护的责任，要求保障用户个人信息安全。欧盟的《通用数据保护条例》（GDPR）更是严格规范了数据处理者在数据收集、存储和使用过程中的行为，旨在保护公民的个人隐私和数据权利。因此，深入研究智能问答系统中的隐私保护与数据安全技术，既符合法律法规的要求，也是保障智能问答系统健康发展和用户权益的必然选择。

一、智能问答系统概述

（一）定义与特点

智能问答系统（Intelligent Question Answering System）是一种利用自然语言处理（NLP）和机器学习（ML）技术，模拟人类回答疑问的智能系统，该系统能够理解用户提出的自然语言问题，并从海量数据中检索相关信息，最终给出准确、合理的答案。智能问答系统的核心在于其自然语言理解能力，它使得系统能够解析用户以自然语言形式提出的问题，识别其中的关键词、实体及语义关系，进而理解用户的真实意图，这一过程涉及复杂的语言处理技术，如分词、词性标注、句法分析等^[1]。自动化、个性化、高效性是智能问答系统的主要特点，其中，自动化是指系统能够自动处理用户的问题，无需人工干预，提高了信息处理的效率。个性化则是指系统能够根据用户的历史行为和偏好，提

供定制化的回答，提升用户满意度。高效性体现在系统能够在短时间内处理大量用户的咨询，确保每个用户都能得到及时、准确的回复。此外，智能问答系统还具备持续学习和优化的能力，通过收集用户反馈和不断迭代模型，提高回答的准确性和智能化水平，图1为智能问答系统的工作原理。

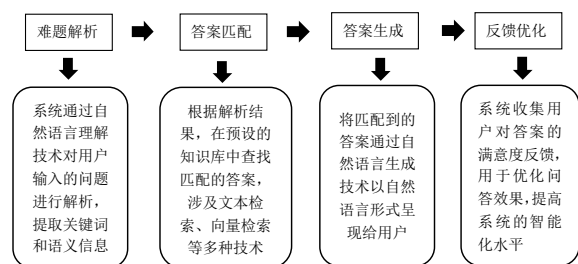


图1 智能问答系统的工作原理

作者简介：张森达（1993.06-），男，满族，黑龙江人，学历：大学本科，专业：信息管理与信息系统，职称：工程师，研究方向：大数据、数据中台、人工智能（数据应用方向）。

（二）技术架构

智能问答系统的技术架构通常包括多个核心组件，这些组件相互协作，共同实现智能问答的功能。自然语言处理（NLP）是智能问答系统的核心技术之一，负责将用户输入的自然语言问题转化为计算机可理解的格式，通过语义分析、情感分析等处理，NLP技术能够准确理解用户的意图和需求。机器学习（ML）技术在智能问答系统中也扮演着重要角色，它通过不断学习和优化，提高系统的智能化水平，如机器学习算法可以用于训练模型以识别用户提问的意图、实体以及语义关系，从而提高答案的准确性和多样性。此外，机器学习还可以用于优化知识库的构建和维护，确保系统能够持续提供高质量的回答。知识库是智能问答系统的另一个重要组成部分，主要用于存储系统所需的知识，包括事实、规则、推理方法等。知识库可以是结构化的数据库、半结构化的文档集合或非结构化的文本数据，它的丰富性和准确性直接影响到系统回答问题的质量。在智能问答系统中，知识库通常与NLP和ML技术相结合，共同实现信息的检索、推理和回答^[2]。除了上述核心组件外，智能问答系统还可能包括预处理模块、召回模块、精排模块和决策模块等辅助组件。预处理模块负责对用户输入的问题进行清洗、分词、词性标注、实体识别等预处理操作。召回模块负责从知识库中检索出与问题相关的信息。精排模块则负责对检索到的候选答案进行排序和选择。决策模块则负责根据用户的意图和需求，生成最终的回答。这些组件相互协作，共同实现智能问答系统的高效、准确和智能化。

二、智能问答系统中的隐私保护技术

（一）隐私保护技术

1. 数据加密技术

数据加密是保护数据安全的重要手段之一，主要分为对称加密和非对称加密两种方式。对称加密采用相同的密钥进行数据的加密和解密操作，具有高效性，但在密钥管理方面相对复杂。非对称加密则使用一对密钥（即公钥和私钥），其中公钥负责加密数据，私钥则用于解密，这一机制可以有效解决密钥分发的安全问题，尽管其加密速度相对较慢（如图2）^[3]。通过运用加密技术，用户数据可以被转换为密文形式，从而确保数据在传输和存储过程中的安全性，有效防止未经授权的访问和数据泄露。

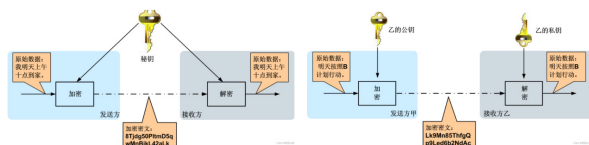


图2 对称加密和非对称加密

2. 匿名化技术

匿名化技术是一种通过对原始数据进行处理，使得数据中的个体无法被识别的技术，该技术主要通过数据变换、模糊处理等方式实现，如删除、替换或混淆数据中的敏感信息。匿名化技术既能保护用户隐私，又能保持数据的可用性和分析价值，在智能问答系统中，这一技术可以应用于处理用户输入的问题和答案，

确保用户身份不会被泄露。

3. 访问控制技术

访问控制技术通过身份验证和授权管理等方式限制对数据的访问，涉及两个主要实体：访问者和资源对象。访问者需要通过身份验证机制证明自己的身份，并获得相应的访问权限，系统管理员则根据用户的角色和需求，为其分配不同的访问权限，以确保数据只能被授权用户访问（如图3）。在智能问答系统中，访问控制技术可以用于保护用户数据和系统资源的安全，防止未经授权的访问和滥用行为。

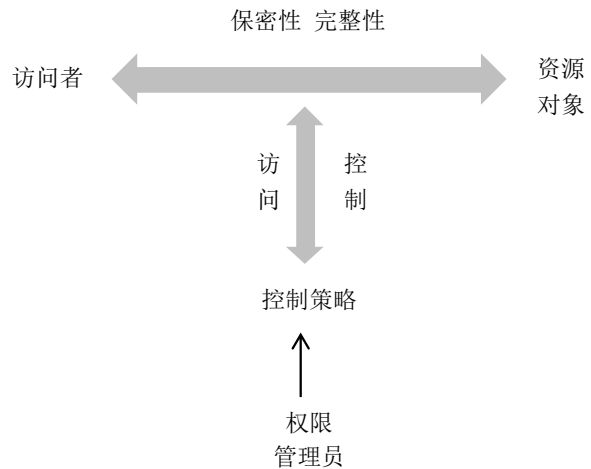


图3 访问控制模型

（二）隐私保护技术在智能问答系统中的应用

在智能问答系统中，隐私保护技术贯穿于数据收集、处理和结果输出等各个阶段，以确保用户隐私的安全。

1. 数据收集阶段

在智能问答系统的数据收集阶段，隐私保护技术起着至关重要的作用，旨在确保用户输入的问题和答案不被泄露或滥用。为此，系统可运用匿名化技术处理用户提问，对敏感信息（如姓名、地址等）进行模糊化处理或彻底删除，以有效保护用户隐私。同时，系统还可以采用数据加密技术对用户输入的数据进行加密存储，保障数据在传输和存储环节的安全性。此外，系统还应严格遵循最小数据收集原则，仅收集提供问答服务所必需的数据，从而降低隐私泄露的风险^[4]。

2. 数据处理阶段

在数据处理阶段，智能问答系统需要对用户输入的问题进行分析处理，以生成准确答案。为了保护用户隐私，系统可以采用差分隐私等技术对处理过程进行保护。差分隐私通过向数据中添加随机噪声来确保个人隐私不被泄露，即使数据被多次分析，个人信息也能得到保护。此外，系统还可以采用同态加密等技术，使数据在加密状态下即可进行处理和分析，避免在解密过程中泄露隐私。

3. 结果输出阶段

在结果输出阶段，智能问答系统需要将生成的答案返回给用户。为了保护用户隐私，系统需要对输出结果进行隐私保护处理，例如，采用匿名化技术处理输出结果中的敏感信息（如用户

身份标识等），确保用户隐私不被泄露；采用数据加密技术对输出结果进行加密传输，保障数据在传输过程中的安全性。同时，系统应遵循最小数据输出原则，仅输出必要的答案信息，以进一步减少隐私泄露的风险。通过这些隐私保护技术的应用，智能问答系统可以在保证服务质量和效率的同时，有效保护用户隐私和安全。

三、智能问答系统中的数据安全技术

（一）数据安全技术

数据安全技术是保障智能问答系统数据安全的重要手段，主要包括数据备份与恢复技术、入侵检测与防御技术、安全审计与监控技术、数据行列控制及鉴权技术。数据备份与恢复技术通过定期备份系统数据，确保在数据意外丢失或损坏时能够迅速恢复，从而保障系统的连续运行和可用性，其原理在于利用冗余存储来抵御数据丢失的风险，即使原始数据遭到破坏，也能依靠备份数据快速恢复系统功能。入侵检测与防御技术侧重于及时发现并有效阻止恶意攻击和数据窃取行为，该技术通过监控系统网络流量、用户行为等关键指标，识别出异常模式，并采取相应的防御措施，如阻断攻击源头、隔离受感染系统等，以切实保护数据安全。安全审计与监控技术则对系统操作和数据访问进行全天候的实时监控和审计，确保系统合规性，它通过详细记录系统操作日志、数据访问记录等信息，为安全事件的调查和责任追溯提供有力依据，同时也有助于及时发现潜在的安全漏洞和违规行为。数据行列控制及鉴权技术是对数据本身进行更细致的安全管理的一种手段，通过对数据的行列进行控制，可以实现对数据访问的精细化管理。具体而言，可以根据数据的敏感程度、用户角色和业务需求等因素，设定不同的行列访问权限，如对于某些敏感数据，可以设定只有特定角色或权限的用户才能访问特定的行或列。在实施数据行列控制及鉴权技术时，首先需要明确数据的敏感程度和访问需求，制定相应的安全策略。然后通过技术手段实现这些策略，如采用数据库管理系统自带的安全控制功能，或开发专门的安全控制模块。此外，还需要对访问控制进行实时监控和审计，确保数据的访问行为符合安全策略，及时发现和处理异常访问行为。

（二）数据安全技术在智能问答系统中的应用

1. 系统架构层面

智能问答系统采用多层次、分布式的架构设计来增强数据安全

全，通过将数据存储、处理和应用逻辑部署在不同的服务器上，实现数据的物理隔离和逻辑隔离，降低数据被一次性窃取的风险。同时，系统架构中融入了容错机制和负载均衡技术，确保即使在部分服务器出现故障或遭受攻击的情况下，也能够迅速切换至备用服务器，保证系统的连续性和稳定性。此外，系统架构还考虑了数据的安全传输问题，采用加密通信协议和隧道技术，确保数据在传输过程中的安全性和完整性。

2. 数据存储层面

第一，智能问答系统运用数据加密技术，对敏感数据进行加密存储，这样，即使数据不幸被非法获取，也能因其加密状态而难以被轻易解密和滥用。第二，智能问答系统实施严格的访问控制技术，通过设定精细的访问权限和身份验证机制，有效限制了对数据的访问和操作权限，确保只有经过授权的用户或系统才能访问到特定的数据资源。第三，为了应对不可抗力因素可能带来的数据丢失风险，数据存储层面还采用了数据备份和容灾技术，智能问答系统会定期对数据进行备份，并将这些备份数据存储在地理位置分散的多个数据中心，确保在遭遇自然灾害、人为破坏等情况时，数据的安全性和可用性能够得到有效保障。

3. 数据传输层面

在数据传输层面，智能问答系统采用了如 TLS/SSL 等先进的加密通信协议，确保数据在传输过程中得到加密处理，有效防止数据被窃听或篡改。同时，系统利用安全传输通道和隧道技术，如 VPN，为数据传输构建了一个安全的网络环境。此外，系统还实施了实时监控和审计机制，详细记录数据传输的各类信息，包括传输时间、传输方和接收方等，以便在发生安全事件时，能够迅速进行追溯和定位问题。这些数据传输层面的安全技术措施，为智能问答系统提供了有力的保障，确保了数据在传输过程中的安全性和可靠性。

四、结语

随着技术的不断演进和攻击手段的日益复杂，隐私保护与数据安全技术成为了智能问答系统发展中的核心议题。业界必须不断探索更为先进、有效的隐私保护和数据安全技术。只有这样，智能问答系统才能在确保用户信息安全的前提下，广泛赢得用户的信任与支持，充分发挥其智能交互、信息精准提供等功能优势，推动整个系统向着更加健康、可持续的未来方向发展。

参考文献

- [1] 许成伟, 贾晓霞, 冉青云. 智能问答系统在装备制造业的应用研究 [J]. 制造业自动化, 2023, 45 (03): 38-43+75.
- [2] 鞠晓峰, 都军, 覃军, 等. 人工智能在智能问答系统中的应用 [J]. 智能建筑与智慧城市, 2021, (03): 36-37.
- [3] 陆毅. 5G 网络中自然语言处理在智能问答中的应用 [J]. 中国宽带, 2023, 19 (11): 124-126.
- [4] 陈志坚, 彭林锋. 基于安全分析大模型应用的智能问答系统设计 [J]. 网络安全和信息化, 2024, (09): 124-126.