选题方面：

参赛作品具备商用价值，用户需求程度高，市场规模与市场接受/欢迎程度高；或者具备社会效益，解决社会广泛关注的问题，针对特殊人群、场景、行业提出新的解决方案。

①倾向于安全，想找一些不太常见但是有存在需要的领域，可能需要调研当前的现状用户的需求以及实现痛点

②编码规范：我们可以后期需要讨论一下编码的形式、名称命名等等

一、强化**会议内容**加密与**环境**监测

* **动态加密**算法优化：——根据网络环境动态调整加密算法

·利用 AI 技术**持续评估**当前**网络环境**的**安全性**。例如，通过监测**网络流量**模式、检测潜在的恶意攻击行为（如DDoS 攻击前奏、恶意扫描等），AI 系统可以动态调整加密算法的**强度和类型**。

·如果检测到高强度的攻击风险，自动切换到更高级、更复杂的加密算法，如量子加密算法（当技术成熟且可应用于此类场景时）或多层混合加密模式，确保会议内容即使在恶劣的网络环境下也难以被窃取。

·基于用户的**身份认证信息和设备特征**，**AI** 可以**生成**个性化的**加密密钥对**。例如，结合用户的生物特征（指纹、面部识别等）数据、设备硬件标识以及登录时间、地点等多因素信息，通过复杂的加密算法生成独一无二且时效性强的加密密钥，进一步提高加密的安全性和不可破解性。

* **会议环境安全**预警：

·**AI 驱动**的摄像头和麦克风**监控**功能。在会议进行时，利用图像识别和音频分析技术，实时监测会议现场是否存在**异常**设备或声音。例如，如果检测到未知的录音设备或摄像头（通过识别设备外形特征或信号发射特征），立即向会议组织者和参会人员发出警报，并自动采取措施，如切断与异常设备的连接或屏蔽其信号。

·**环境信息**加密传输与分析。对于会议所在的**物理环境信息**（如会议室位置、参会人员身份信息等），在传输过程中使用加密技术，并由 AI 进行**深度分析**。例如，AI 可以根据参会人员的位置信息和行为轨迹，判断是否存在异常的人员**聚集**或**徘徊**情况，若有可疑行为则及时发出安全预警，防止会议信息被非法**窃取**或会议过程被**干扰**。

二、**智能笔记助手**的安全升级

* 数据加密与访问控制：——笔记存储传输的加密以及访问控制

·智能笔记助手在**会议等场景**中自动**提取**内容并**分析**关键信息，且**提取**的**关键信息**在**存储**和**传输**过程中都采用**高强度加密**算法。例如，使用 AES - 256 加密算法对笔记内容进行加密，确保即使数据被窃取，攻击者也无法轻易获取其中的关键信息。

·严格的**访问控制**机制。基于 **AI 的身份识别**技术，只有经过**授权**的**用户**才能**访问**智能笔记助手提取的内容。例如，通过人脸识别、语音识别或多因素认证（结合密码、短信验证码、生物特征等）等方式，确保笔记内容的安全性。同时，AI 可以根据用户的角色和权限，**动态调整其对笔记内容的访问级别**，例如普通参会人员只能查看**自己**相关的笔记部分，而会议组织者或特定的审核人员可以查看和管理**所有**笔记内容。

* **信息防泄漏**监测：——笔记的分享以及敏感内容检测

·AI 实时监测笔记内容的**分享**和**使用**情况。如果发现笔记内容被**非法**复制、转发或在未授权的平台上**传播**，立即启动溯源机制，通过分析网络日志、设备信息等多种数据来源，快速定位信息泄漏的**源头**，并采取相应的措施，如封锁相关账号、通知相关人员等。

·基于自然语言处理技术，AI 可以对笔记内容进行语义分析，识别其中是否包含**敏感信息**（如商业机密、个人隐私等）。如果检测到敏感信息，自动提示用户进行加密或采取其他安全措施，并且在分享过程中，根据接收方的信任级别和安全需求，对敏感信息进行适当的模糊化或脱敏处理，确保信息在安全的前提下进行共享。

三、**智能文档审阅工具**的安全保障

* 文档加密与完整性验证：——文档上传加密和权限管理

·在文档上传进行审阅时，**自动**对文档进行**加密**处理，防止文档在审阅过程中被**非法访问或篡改**。采用**数字签名**和**哈希算法**等技术，确保文档的完整性和真实性。例如，对文档生成唯一的哈希值，在文档审阅前后进行对比，如果哈希值发生变化，则说明文档可能被篡改，并及时向用户发出警报。

·基于 AI 的**权限管理**系统，对于不同的**审阅人员**设置不同的文档**操作**权限。例如，普通审阅人员只能查看文档内容和提出修改建议，而不能直接修改文档；高级审阅人员或文档所有者可以进行修改、批准等操作，并且每一次操作都被 AI 详细记录，以便后续审计和追踪。

* 安全漏洞检测与修复建议：——语法格式和安全漏洞的检查

·AI 智能文档审阅工具可以检查**语法错误和格式**问题+判断内容是否真实（大模型），还可以检测文档中可能存在的**安全漏洞**。例如，对于包含**链接**的文档，AI 可以**自动扫描链接的安全性**，判断是否为恶意链接；对于文档中的**附件**，检查是否存在恶意软件或病毒。如果检测到安全问题，不仅提供警告信息，还可以提供相应的修复建议或自动采取隔离措施，确保文档的安全性。

四、扩展安全功能

* 行为分析与异常检测：

·AI 对**用户**在软件内的**操作行为**进行**实时分析**。例如，监测用户的**登录时间、地点、操作频率、操作类型**等信息，建立用户行为**基线模型**。如果发现用户的行为与基线模型存在较大偏差，如在非正常工作时间从陌生地点登录并进行大量文件下载或信息修改操作，立即触发安全验证机制，要求用户进行额外的身份认证或暂停相关操作，直到确认安全为止。

·对会议中的交流行为进行分析。通过**语音识别**和**自然语言处理技术**，监测参会人员的发言**内容和语气**，判断是否存在**异常情绪**或潜在的**信息泄漏风险**。例如，如果发现参会人员在会议中提及敏感信息且语气紧张，可能存在信息被胁迫泄漏的风险，此时软件可以自动采取措施，如暂停会议、通知相关安全人员等。

* 数据安全态势感知与可视化：

·AI 收集和分析软件运行过程中的各种**安全数据**，包括网络流量、用户行为、设备状态等信息，构建数据安全态势感知平台。通过**可视化界面**，向管理员和用户展示当前**软件的安全状况**，如网络攻击风险级别、数据加密状态、用户权限分布等信息，让用户直观地了解软件的安全态势，并及时发现和处理安全问题。

·基于 AI 的预测分析功能，根据**历史安全数据**和当前的**安全态势**，**预测**未来可能发生的安全事件，并提供相应的预防建议。例如，预测在特定时间段内可能遭受的网络攻击类型和规模，提前调整安全策略，如增加防火墙规则、更新加密算法等，提高软件的安全防御能力。

**参赛项目阶段评分标准见附件8**

选题分析：

**创新点**

* 使用场景创新：打破传统办公软件仅注重功能实现而忽视安全与智能融合的局限，将 AI 安全技术贯穿于会议、笔记、文档处理等整个办公流程。

·在会议场景中，不仅实现了基本的沟通功能，还通过 AI 对会议环境和内容进行全方位安全防护，开创了安全智能会议的新场景。

·对于智能笔记助手，改变了以往用户手动记录和整理笔记的方式，实现了自动提取关键信息并在安全保障下灵活分享的创新使用场景，满足了用户在快节奏办公中高效处理信息的需求。

·使用方式创新：借助 AI 实现了加密手段的智能化选择与动态调整，用户无需手动设置复杂的加密参数，软件根据环境和安全需求自动完成。例如，根据网络状况和会议重要性自动切换加密算法，这是一种全新的加密使用方式。

智能文档审阅工具以 AI 为驱动，用户只需上传文档，即可自动获得语法、格式和安全漏洞等多方面的审阅结果和修改建议，改变了传统文档人工检查和逐个处理问题的繁琐方式。

* 用户体验创新：

·为用户提供了一站式的安全智能办公体验，从会议组织到后续的信息整理与文档处理，所有环节都有 AI 保驾护航，减少了用户在安全管理方面的精力投入，让用户能够更专注于业务本身。

·例如，行为分析与异常检测功能在保障安全的同时，不会过多干扰用户正常操作，只有在出现异常时才进行精准提示和干预，使安全防护变得无感且高效，极大地提升了用户体验。

* **商业价值**

·对于涉及金融、科技等行业的企业，会议内容和文档中的敏感信息至关重要，软件的安全防护功能将吸引大量此类企业用户。

·智能笔记助手和智能文档审阅工具也能提高办公效率，减少人力成本和错误率

·可以针对不同规模的企业（从中小企业到大型跨国公司）以及不同行业（如教育、医疗、政府等）进行定制化推广，其通用性和适应性将使其获得广泛的市场接受度。