

金融服务行业人工智能应用的风险管理研究

冯飞 黄成

延安大学, 陕西 延安 716000

摘要: 随着人工智能技术在金融服务行业广泛应用, 它在提高效率和改善服务的同时也带来了一系列风险, 文章意在探寻金融服务行业中人工智能使用过程中主要的风险类型, 并给出相对应的风险管理对策。通过分析智能风控系统、智能投顾、金融市场分析的 AI 模型应用等相关情况, 指出了算法偏见、数据安全问题、系统依赖与法律法规适配滞后等问题, 并且给出了算法审核、数据管理、人机协同与监管科技等一系列风险管理措施以期为金融服务行业中人工智能使用过程中的风险管理策略提供借鉴。

关键词: 金融服务行业; 人工智能应用; 风险管理; 算法审计; 数据治理

DOI: 10.63887/fem.2025.1.4.2

近些年来, 人工智能技术 (AI) 在金融服务行业里的运用越发普遍, 从智能风控, 智能投顾再到金融市场分析, AI 正在慢慢改变金融服务的样子, 不过, 随着技术的进一步运用。它所带来的风险同样不能轻视, 怎样有效地应对这些风险, 保证金融服务的安全和稳定, 这是当前急需处理的问题。文章会从人工智能在金融服务行业里的应用状况入手, 剖析主要的风险种类, 并给出对应的风险管理方案。

1 人工智能在金融服务行业的应用现状

1.1 智能风控系统的构建与运作

智能风控系统凭借大数据分析 with 机器学习算法, 给金融交易风险防控带来革新, 它可以即时搜集、整合来自不同渠道的金融交易数据, 包含交易金额, 交易时间, 交易对手之类的信息, 再用机器学习算法深入挖掘并分析这些数据, 迅速找出潜藏的风险模式和异常行为^[1], 就像通过对过去欺诈交易数据的学习, 构建起风险模型, 然后对新出现的交易实施即时对比和评价, 一旦察觉到交易特点同欺诈模式吻合, 马上发出警报。但是智能风控系统是否准确、可靠? 算法模型的好坏起决定性作用, 如果算法模型的设计有缺陷, 比如对某些风险因素设置的权重不恰当, 或者模型训练所用的数据样本缺乏代表性, 都会导致算法出错, 不能正确识别风险。数据源的完备性也很重要, 如果数据不全、有误或更新不及时, 就会影响模型对风险

的判断, 比如客户信用记录不完整, 系统就无法全面评估客户的信用风险, 影响风控效果。

1.2 智能投顾与客户服务的方向发展

智能投顾依靠 AI 技术, 给投资者给予个性化的投资意见与服务, 冲破了传统投资顾问服务的限制, 它可以依照投资者的风险偏好, 财务情况, 投资目的等要素。为量身打造投资组合, 削减了投资门槛, 提升了服务效率, 不过, 智能投顾的发展也碰上了一些问题, 它的决策过程缺少透明度, 投资者常常很难领悟智能投顾背后所用的算法逻辑和决策根据, 就像智能投顾给出的投资建议也许只是依靠繁杂的数学模型和数据分析结果, 投资者不能直接明白为什么选定这些投资产品, 这就加大了投资风险。在客户服务上, AI 聊天机器人等可以做到 24 小时在线服务, 但遇到一些复杂的问题或者情绪化的交流时就显得有些力不从心, 当客户碰到比较复杂的金融问题, 牵涉到税务、法律这些方面的时候, 聊天机器人也许就无法给出准确的答案。

1.3 AI 模型在金融市场分析中的应用

AI 模型在金融市场分析方面显示出很强的势力, 依靠大量数据分析, 它可以预估市场走向, 帮助做投资决策, 能够处理经济宏观数据, 各个行业的数据以及公司账本上的数据等多种信息, 并找出数据之间的联系和规律, 像 AI 模型通过学习过去历史股价, 交易

数量等数据。可以去预估股票价格走势，给投资者给予参照，金融市场的复杂性及其不确定性使 AI 模型的预测结果也带有不确定性，由于市场会受不少因素影响，比如政策改变，突发状况，市场气氛等。而这些都是很难全面衡量的，AI 模型大概率不能立即发觉这些变动，从而造成预测结果同真实情况不相符。

2 人工智能应用带来的主要风险类型

2.1 算法偏见与模型失真风险

算法偏见和模型失真风险是金融服务行业人工智能应用时必须面对的问题，算法偏见来自多种因素，数据选择期间，如果数据样本存在偏差，仅包含某些地区或者收入阶层的数据，那么算法在训练时会过于依靠这些有限的信息，对其他群体做出不公平的判断^[2]，算法设计上的缺陷也会造成偏见，有些算法或许默认某些特征同风险或者收益有特定联系，而忽略个人差异。模型失真受到数据改变和环境改变的影响比较大，金融市场变化飞快，新的经济形势，政策改变等等都会使得已有数据特征发生改变，如果模型不能及时更新适应，它的预测结果就会同现实情况相脱节，比如信用评价模型没有考虑到疫情这样的突发公共事件给客户还款能力带来的影响，就可能误判客户信用。

2.2 数据安全与隐私泄露风险

金融服务行业数据安全与隐私保护非常重要，AI 技术应用加大了难度，该行业掌握着客户很多敏感信息，涉及身份信息，交易记录，财务状况等。这些信息如果泄露或者被滥用，客户会遭遇身份盗用，资金损失等严重后果，金融机构也会因为声誉受损而失去客户信任，AI 技术使得数据处理变得复杂且危险，数据收集时，若没有遵守合法，正当，必要原则，过度收集客户信息，便增大了数据泄露的风险，在数据存储和传输期间，若安全防护不到位，像加密技术不完备，网络有漏洞等。数据就有可能被黑客窃取，而且，数据共享过程中的不恰当操作也会造成隐私泄露。

2.3 系统依赖与技术失控风险

伴随 AI 技术应用金融服务业的普遍化，金融机构对系统的依赖度逐步提升，系统依赖及技术失控的风险亦浮现出来，很多金融机构的核心业务像交易事务，

风险评估，客户接待之类的都非常依存于 AI 系统。倘若系统发生状况，比如说服务器崩盘，软件存在漏洞等情况，金融服务便会马上中断，客户就无法开展正常的交易活动，而且会给金融机构带来极大的经济损失^[3]。最严重的就是，若是系统遭遇黑客的攻击，就会造成客户的个人信息泄露，客户的钱款被盗取等重大的事故，还有可能造成系统性风险的出现。同时新技术的不断发展也对技术的把控造成了困难。新出现的 AI 技术不断涌现出来，如果金融机构没有能赶上技术前进的步伐，则会出现技术失控的问题。

2.4 法律法规适应滞后问题

AI 技术发展迅速，法律法规相对滞后，金融服务行业存在许多合规风险，AI 技术更新速度非常快，新的业务模式和应用场景不断出现，但相关的法律法规要经过一段时间才能制定并更新，这就造成一些依靠 AI 的创新业务处在法律监管的空白区域。有些依靠 AI 做智能投顾，区块链金融等新兴业务，在法律上没有明确的规范和引导，金融机构开展这些业务时碰到很大的不确定性，要是出现问题，就有可能陷入法律纠纷和惩罚。而且，不同国家和地区的法律法规有所不同，这就造成跨国金融服务出现法律冲突和合规问题，金融机构在各个国家和地区开展业务的时候，要遵照当地的法律法规，可是，由于各个国家和地区的法律对 AI 技术的要求不一样，金融机构也许无法做到完全符合所有要求，加大了其合规难度和成本。

3 金融行业人工智能风险管理的应对策略

3.1 算法审计机制的构建路径

想要保证算法正确且公平，金融机构就得打造算法审查体系，审查算法模型的时候，得组织专业的审查小组，算法审查小组里应有算法专门人才，金融业务专家以及法律合规专家等。审查算法模型的时候，要细致探究其设计思路，看是否遵从金融行业惯有的准则及道德标准，比如在审查信用评定算法之时，看这个算法是不是足够全面地考量各影响到信用的要素，是不是有针对某些特定群体的不公平偏见，审查算法模型的时候还要做模拟，要模仿各种具体情境，彻底测试算法模型，不能只是在正常情况之下测试算法的

运转状况，也要测试算法在极端状况下的稳定性和正确率，比方说市场大起大落时，算法能不能做出合理的判断，要不要做出过激或者错误的决定。验证环节，算法输出的结果要符合预期目标，并且具有可复制性，通过同历史数据作比较，来验证算法的有效性及其可靠性，还要创建算法审计的常规机制，定时对算法展开评价和改良^[4]，由于市场环境不断改变，金融政策调整。市场趋势变动等状况出现，算法也许就不再适合当前的情形，所以，金融机构务必关注市场动向，及时更新和改良算法，比如说，当新的金融产品涌现时，算法就得尽快去学习并顺应，从而正确评判相关风险，而且要形成起算法审核的回馈机制，把审核得到的结果立即传达给算法研发团队，使得可以尽早察觉到问题，予以修正。保证算法一直处在良好的运作状态，从而给金融服务赋予可靠的支撑。

3.2 数据治理与权限分级管控策略

为了保证数据的安全和隐私保护，金融机构必须要做好数据治理的工作，建立完善的数据管理制度是第一步，这个制度要规定好数据收集、存储、使用、共享以及销毁等环节的具体规范和流程。在数据收集的时候，要按照合法、正当、必要的原则，清楚地告诉客户数据会被怎么用以及用途范围，得到客户的同意，对于数据存储来说，采用先进的加密技术，把敏感数据加密起来，不让别人在存储的时候盗取或者篡改。而且还要加强访问控制，只有经过许可的人才能看到某些数据，执行数据备份和恢复措施也很关键，定时把数据备份下来，把备份好的数据存放在安全的地方，免得数据弄丢。一旦出现数据丢失或者损坏的情形，就能立即予以恢复，保证金融服务正常运转，在权限分级管理上，要按照人员的岗位和职责，给它们分配对应的数据访问权限，比如，一线客服人员只能查看客户的大概信息和交易记录，高级管理人员可以访问更多的业务数据和统计分析报告，通过权限分级管理，可以减小数据泄露的风险，避免内部人员乱用数据。而且还要加大对数据访问的监督和检查力度，尽快找出并解决异常的数据访问情况，保证数据安全和隐私。

3.3 人机协同机制的制度化构建

为减少系统依赖以及技术失控风险，金融机构须建立人机协同机制，人与机器各自在金融服务中的角色和职责应被明确，在这里，机器有着高效且精准的处理能力，可应对一些反复、有规律的任务，诸如数据录入及初步的风险评判之类的事情，人拥有判断力，创造力，并具备对情感的理解能力。因此在重要时刻，能对某些情况予以干预和决策，在金融交易较为繁杂时，机器可以按照预设好的规则来执行交易操作，当市场产生意外的起伏或者出现无法预料的情形时，人能够凭借自身的经验判断去及时调整交易策略，从而免除损失，加强员工对系统的训练和教育，提升面对故障以及技术问题的能力同样不可忽略。定期安排员工参加技术培训课程，了解最新的技术发展动态以及常见的技术故障处理办法，开展应急演练活动，模仿系统出现故障或者遭受网络攻击之类的状况，促使员工在实际操作中提升自己应对突发事件的能力，还要创建起人机协同的交流机制，保证人与机器之间可以迅速而且准确地展开信息交流，当机器察觉到异常情形的时候，就能立即向有关人员发出警报，并且给予详细的资讯，从而让人员能尽快作出决定。通过制度化的创建人机协同机制，最大限度地发挥人和机器各自的长处，进而提升金融服务的稳定性和可靠性。

3.4 监管科技在风险防控中的应用嵌入

为了应对法律法规适应滞后的状况，金融机构积极采用监管科技（RegTech），这是明智之举，监管科技借助 AI，大数据等技术手段，可以提升监管效率与精确度^[5]，就风险防控而言，监管科技可对金融机构的业务数据展开即时监测并加以剖析，从而尽早察觉潜藏的风险隐患。拿交易数据来说，通过对其开展分析，就能找出一些异常的交易行为，频繁的大额交易，关联交易等等，进而发出警报，而且，监管科技还能对金融机构的合规状况实施评判，查看其是否遵照了有关的法律法规和监管规定，凭借大数据技术，对金融机构的各种业务数据实施全面梳理并加以剖析，同监管标准和要求做比较，找出其中的合规问题。监管科技还可以给金融机构给予风险预警及合规意见，经过对历史数据以及市场走向加以剖析，预估可能会产生的风险，并且给予金融机构相应的解决办法，比如市

场出现了新的政策改变，监管科技可以马上分析这些改变给金融机构带来什么样的影响，而且给出一些合规调整方面的建议，从而让金融机构更好地适应法律法规的变化，减小合规风险。金融机构要加大对监管科技公司的合作力度，一同探寻符合自身业务需求的监管科技方案，把监管科技深深融入到风险防控体系之中，改善自身的风险控制水平。

4 结束语

金融服务行业人工智能应用的风险管理是个复杂又体系化的工程。随着技术向前发展，应用场合不断被拓宽，金融机构要持续提升风险管控的能力，保障金融服务的安稳进行。依靠形成算法审查机制，优化数据治理及权限分层管理，创建人和机器共同工作的机制，使用监管科技这些办法，金融机构就能较好地应付人工智能应用产生的风险，推动金融服务行业健康前进。

参考文献

- [1] 崔启亮. 人工智能时代的语言服务行业发展趋势[J]. 北京第二外国语学院学报, 1-7.
- [2] 邓媛, 杨屿海, 袁庆. 人工智能时代语言服务行业需求分析与人才培养研究[J]. 湖南大学学报(社会科学版), 2024, 38(02): 95-102.
- [3] 孙杰贤. 人工智能：服务行业的好帮手[J]. 中国信息化, 2023, (06): 22-23.
- [4] 马静, 王磊. 金融服务标准化对金融创新的影响研究[J]. 科技与金融, 2020, (3): 26-30.
- [5] 刘畅, 张瑞, 李明. 金融服务标准化与金融风险防范研究[J]. 经济论坛, 2021, (5): 42-45.