密码 数字时代的隐形卫士

□ 杨小东

每天,我们都要多次输入“密码”:解锁手机、登录微信、支付账单。但您可能不知道,这些日常生活中所谓的“密码”,在专业领域大多被称为“口令”。它们像一把简单的钥匙,核对正确即可通行。

而真正的“密码”,是一套更为复杂的技术体系。它会把您输入的信息,通过特定的数学运算进行“变形”,生成另一串结果,系统通过验证这个结果来判断核准你的身份。2020年实施的《中华人民共和国密码法》将其定义为:采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。

那么,这套看不见的技术,究竟如何守护着我们的数字生活安全呢?

密码的四大核心能力

密码技术是保障信息安全最有效、最可靠的手段,它主要拥有四大核心能力。

(1)保密性:确保“悄悄话”不被偷听。

它能把“明天下午三点见面”这样的普通信息(明文),通过加密算法和一把“密钥”,变成一堆毫无意义的乱码(密文)。即便这串乱码被截获,没有对应的“密钥”,也无人能懂。您的聊天记录、支付信息,正依赖于此。

(2)真实性:解决“你是谁”的难题。

网络世界无法面对面确认身份。密码技术中的数字签名和身份认证,就像一张无法伪造的“网络身份证”,确保正在操作的是您本人。

(3)完整性:为信息贴上“防篡改封条”。

你如何知道收到的电子合同在传输中未被修改?密码中的散列函数(哈希函数)能为任何信息生成一个独一无二的“数字指纹”。内容有任何微小变动,“指纹”就会彻底改变,接收方一比对便能发现。

(4)不可否认性:让行为“立字为据”。

网上交易,买卖双方如何防止对方抵赖?数字签名技术确保了行为的不可抵赖性。一旦您用个人“私钥”签署了订单或支付,就无法事后否认,为网络交易提供了公平保障。

可以说,没有密码的守护,我们的数字生活如同门窗大开,安全无从谈起。

波澜壮阔的密码发展史

密码的历史源远流长,最初是一门关乎国家存亡的战争艺术。

古代,斯巴达人将纸条缠绕在特定粗细的木棍上书写以保密。古罗马的凯撒大帝发明了“凯撒密码”,将字母统一后移几位进行加密。

到了20世纪,两次世界大战将密码的攻防推向巅峰。德国使用了当时被认为“不可破译”的“恩尼格玛”密码机。英国数学家艾伦·图灵(后来的“计算机科学之父”)带领团队成功破解,为结束二战做出了巨大贡献。在太平洋战场,美军破译日军密码,也成为中途岛战役胜利的关键。

至此,密码学才真正从“战争艺术”变为“科学”。1949年,香农的《保密系统的通信理论》为其奠定了数学基础。1977年,数据加密算法标准公开,让密码技术从军方走向民间。而更加革命性的突破是公钥密码思想的出现:它使用一对密钥,一个公开(公钥),一个私有(私钥)。任何人都能用公钥加密信息,但只有私钥持有者才能解密,完美解决了大规模网络中的身份认证难题。

如今,我们常用的密码算法主要分三类:对称密码(如AES,加解密用同一把钥匙)、非对称密码(即公钥密码,如RSA)和散列函数(生成“数据指纹”,如MD5、SHA系列)。我国也自主研发了SM系列算法(如SM2、SM3、SM4),广泛应用于各领域。

面向未来,量子计算机的出现对现有密码体系提出了挑战。全球科学家正在积极研究能够抵抗量子计算的后量子密码,这是一场关乎未来安全的竞赛。

密码无处不在

您或许感觉不到,但密码技术已深度融入日常生活的方方面面。我国密码法将密码分为保护国家秘密的核心密码、普通密码,以及保护商业和个人信息的商用密码。我们接触的,大部分是后者。

(1)移动支付的安全基石。每一次扫码支付,密码技术都在后台验证您的身份、加密交易数据、签署电子凭证,确保资金安全,抵御欺诈和盗刷。

(2)智慧政务的信任纽带。电子营业执照、电子发票、公积金在线办理等都依赖数字签名,确保网上办事如同线下盖章一样合法有效,实现了“一网通办”。

(3)便捷生活的幕后功臣。家里的智能电表通过密码技术认证身份、加密数据,让您能在手机上交电费、查用电量。数字电视、ETC不停车收费、交通一卡通,其信号安全和防复制功能都离不开商用密码的保障。

此外,在医疗健康、社会保障、税务、教育等领域,密码技术都在发挥着“安全卫士”的核心作用,支撑着数字社会的稳健运行。

提升个人密码安全意识

强大的密码技术为我们提供了盾牌,但我们个人也需要正确使用它,尤其是设置好各类账户的“口令”。

(1)杜绝弱密码:避免使用“123456”、生日、电话号码等简单或易猜的信息。

(2)创建强密码:使用8位以上,包含大小写字母、数字和特殊符号的组合。可以编一个自己熟悉但别人难猜的句子缩写。

(3)分级管理:重要账户(银行、邮箱)使用高强度独立密码,普通网站可区别对待。

(4)善用辅助:在确保安全的前提下,可使用可靠的密码管理器。

(5)拥抱双因子:尽可能为重要账户开启短信验证、生物识别(指纹、人脸)等二次验证。

(6)定期更新:养成定期更换重要账户密码的习惯。

国之重器 民之盾牌

密码技术与核技术、航天技术并称为国家安全的三大战略支撑,是当之无愧的“国之重器”。密码守护着国家网络空间的主权和安全,也是我们每个普通人享受数字生活便利的“隐形盾牌”。从移动支付到智慧城市,从人工智能到物联网,其安全发展的底层都离不开密码系统的默默护航。

了解密码、善用密码、增强密码安全意识,不仅是对个人财产与隐私的保护,也是我们共同构筑国家网络安全防线的一份责任。让我们认识并信赖这位身边的“数字卫士”,携手迎接更安全、更美好的智能未来。

(作者单位:西北师范大学人工智能与计算机学院)

如今,我们正生活在一个被人工智能(AI)温柔包裹的时代。早上醒来,智能音箱用悦耳的声音播报天气;出门上班,自动驾驶导航巧妙避开拥堵路段;晚上回家,智能门锁“认脸”开门……AI就像一位无形却贴心的伙伴,让生活更加便捷高效;AI辅助诊断、个性化教学、智能制造、精准农业、视频聊天、交通调度等各种应用,正推动社会各行业向智能化升级。然而,正如一枚硬币有两面,人工智能在带来便利的同时,也伴随着一系列安全隐患。今天,就让我们一起来探讨人工智能安全的重要性,以及我们该如何守护这个智能时代的安全。

当AI逐渐普及 安全如何守护

□ 张学军

人工智能安全是什么

想象一下,你正在使用人脸识别技术解锁手机,如果这个系统被恶意攻击,他人的脸也能轻松打开你的手机,那你的个人信息、照片等隐私将暴露无遗。再比如,自动驾驶汽车依赖复杂的AI算法来感知周围环境并做出决策,如果这些算法被干扰或篡改,可能会导致严重的交通事故。这些都不是危言耸听,而是真实存在的安全隐患。

AI安全,简而言之,就是确保AI系统在整个生命周期中——从数据采集、模型训练,到部署和使用——始终保持可靠、可控、公平且不被恶意利用。它关乎我们的个人隐私、财产安全,甚至生命安全。

它关注的不仅是系统是否遭受黑客攻击,还包括:

算法的决策是否值得信任?

数据是否在不知不觉中泄露隐私?

模型是否会被误导,做出危险判断?

技术是否可能被滥用,造成风险?

这可以概括为以下四个核心能力来理解AI安全。

(1)可靠性:让系统“少犯错、不乱来”。AI依赖数据学习规律,如果训练数据存在偏差,模型就可能在现实中频繁出错。可靠性要求系统在复杂环境下保持稳定表现。

(2)鲁棒性:抵御“看不见的干扰”。鲁棒性,是一个系统在面临内部结构和外部环境变化时,能够保持其性能和功能稳定的能力。研究发现,对图像或语音进行人类几乎无法察觉的微小修改,就可能让模型作出完全错误的判断,也就是常说的对抗攻击。这类风险在自动驾驶、安防识别中尤为突出。

(3)公平性:避免“算法歧视”。如果训练数据本身不均衡,AI可能在招聘、信贷、风控等场景中对特定群体产生不公平决策。

(4)隐私与可控性:知道“数据去了哪里”。在AI的世界里,数据是驱动算法运行的“燃料”。然而,这些数据往往包含大量用户的个人信息,如姓名、年龄、性别、位置等。如果这些数据被非法获取或滥用,后果不堪设想。

真实案例:人工智能安全问题就在身边

AI安全并非抽象概念,而是已经在现实中多次显现。

案例一:人脸识别带来的隐私风险

在一些公共场所,人脸识别被用于门禁、考勤和支付。但部分系统在用户不充分知情的情况下,长期存储和集中管理人脸信息。一旦系统被攻击或内部管理不当,个人生物特征数据将面临严重的泄露风险。

启示:AI越“聪明”,对隐私保护的要求就越高。

案例二:自动驾驶中的“对抗攻击”

研究人员曾演示,只需在交通标志上贴上特殊图案,自动驾驶系统就可能将“停止”误识别为“限速”。这种攻击并不依赖入侵系统,而是利用模型的认知弱点。

启示:AI“看世界”的方式与人类不同,安全测试不能只依赖正常场景。

案例三:深度伪造引发的信任危机

利用生成式AI,可以合成高度逼真的人脸视频和语音。现实中已出现冒充亲友进行诈骗的案例,使“眼见为实”的传统认知受到挑战。

启示:AI在提升效率的同时,也可能放大虚假信息的危害。

AI安全风险从何而来,综合来看,AI安全风险主要源于以下几个方面。

数据层面:数据质量不足或隐私保护不当

模型层面:算法存在偏差、可解释性不足

系统层面:缺乏针对恶意攻击的防护设计

应用层面:技术被滥用于诈骗、造谣或操纵舆论

这些问题相互交织,使AI安全成为一项系统性挑战。

人工智能安全保障:构建可信人工智能

如何构建可信的AI来应对AI安全风险,需要技术、制度和公众层面协同发力。

(1)技术层面:让系统更“稳健”。通过对抗训练、模型验证、隐私计算等手段,提高AI的安全性和可控性。

(2)制度层面:明确责任与边界。建立算法审计机制,完善数据保护与AI治理相关法律法规。

(3)公众层面:提升基本认知。理性看待AI生成的内容,不随意授权敏感数据,增强辨别能力。

作为普通公民,我们既要享受AI带来的便利,也要警惕其潜在风险。就像汽车需要安全带、药品需要临床试验一样,AI也需要安全机制。只有在安全理念的引导下,它才能真正成为造福社会的力量。实现这一目标,需推动跨学科、跨领域协同创新,强化AI全生命周期安全管理。从研发设计到部署应用,每个环节都应嵌入安全准则,确保技术发展始终服务于人类福祉。

在智能化不断加速的今天,理解AI安全,让人工智能“可用、可信、可控”,已经成为数字时代的一项重要公共素养。让AI在安全的轨道上发展,是技术进步的必然要求,也是我们共同的责任。

(作者单位:兰州交通大学电子与信息工程学院)

本报地址:兰州市白银路123号 邮编:730030 甘报集团传媒分公司:8158717(带传真) 甘报集团发行分公司:8156468 印刷:甘报集团印务分公司(电话:8156348) 昨日本报5时00分开印8时30分印完