移动应用加密技术在用户数据保护中的应用评估

蒋廷金
杭州安恒信息安全技术有限公司　浙江　杭州　310000

摘　要：现今移动互联网繁荣兴盛，诸多移动应用得到广泛运用，众多用户数据于其中汇聚。只是，数据泄露情况屡屡发生，用户数据安全遭受严重威胁。移动应用加密技术堪称保障用户数据安全的重要办法，经对数据加密，可切实防范数据在存储以及传输时被窃取或篡改。本文对移动应用加密技术于用户数据保护里的运用展开评估，剖析其技术原理、应用场景、实际成效和面临难题，进而探究应对举措，目的在于为提升移动应用用户数据保护程度给予理论与实践方面的参考。

关键词：移动应用；加密技术；用户数据保护；数据安全；应用评估

引言

当下智能手机极为普及，移动应用已融入人们生活与工作，成为重要工具。社交娱乐、金融交易等众多领域都有其身影，还积累大量用户数据，像个人身份信息、财务数据、位置信息这类敏感内容都包含其中。近年来，数据泄露事件频频被曝光，致使用户隐私受侵，财产也遭受严重损失。移动应用加密技术可对数据加密，让数据以密文状态呈现，就算数据被获取，攻击者也难以破解。评估移动应用加密技术在用户数据保护方面的应用，对于保障用户数据安全、推动移动应用良好发展意义重大。

1 移动应用加密技术概述

1.1 加密技术基本原理

移动应用加密技术大多依据密码学原理。对称加密算法里，AES（高级加密标准）较典型，加密和解密用同一密钥。在移动应用中，客户端利用此密钥加密数据后传输，接收端凭借相同密钥解密，它加密与解密速度快，适合大量数据加密操作。拿某移动云存储应用来说，本地对用户上传照片进行AES加密，用户下载时用相同密钥解密，保障照片在存储及传输环节的安全。非对称加密算法以RSA算法为代表，存在公钥和私钥，公钥可公开用于加密，私钥由用户妥善留存用于解密。于移动支付场景，用户用商家公钥加密支付信息，商家用私钥解密，以此确保信息安全传输，防范支付信息在网络里被窃取。哈希算法像SHA-256，会把数据转变为固定长度哈希值，用于验证数据完整性，一旦数据遭篡改，哈希值就会变动。在移动社交应用中，消息发送前会算出哈希值，接收方收到消息后重新计算哈希值，与原哈希值对比，判断消息是否被篡改。

1.2 常见加密算法类型

DES（数据加密标准）也算一种加密算法，尽管其安全性渐被AES赶超，不过部分旧系统里依旧在使用。还有3DES（三重数据加密标准），通过多次加密操作提升安全性。椭圆曲线密码学（ECC）算法，借助椭圆曲线的数学特性生成密钥对，在安全强度等同的情况下，密钥长度更短，计算量不大，存储需求也小，对资源有限的移动设备颇为适用。移动应用的身份认证部分，HMAC（哈希消息认证码）算法较为常用，它把哈希函数与密钥相结合，用以验证消息的完整性以及真实性，避免消息被篡改或伪造。就拿移动办公应用登录来说，客户端把用户名、密码和一个随机数组合起来，运用HMAC算法算出哈希值后发送给服务器，服务器依据存储的用户信息以及密钥做同样计算，对比哈希值以此验证用户身份。

1.3 与传统加密技术对比优势

移动设备存在资源局限，计算能力、存储容量以及电量都相对匮乏。移动应用加密技术特意针对这些特性加以优化，以ECC算法为例，其在保障安全的同时可降低资源损耗[1]。传统加密技术的应用场景较为固定，与之不同，移动应用加密技术要能适应多样场景，无论是移动社交聊天，还是移动办公文件加密，均能灵活处置。移动网络环境下数据传输频繁且不稳定，移动应用加密技术在此种状况下，更能保障数据传输时的安全性与完整性。比如在4G网络信号欠佳的区域，移动应用所采用的加密技术依然能够确保数据精准、安全地传输，反观传统加密技术，或许会因网络波动而致使数据丢失，甚至遭受攻击。

2 移动应用加密技术的应用场景

2.1 数据存储加密

拿移动银行应用来讲，用户的账户信息、交易记录等都存于设备当中。借助AES加密算法对这些数据加密存

储，就算设备遗失或者被盗，要是没有正确密钥，攻击者根本无法获取敏感信息。有调查显示，那些未采用加密存储的移动银行应用，一旦设备丢失，用户敏感信息泄露风险高达70%，可采用AES加密存储后，该风险就降低到10%以内了。如此显著的风险差异，将加密存储的重要性体现得淋漓尽致。对于云存储的移动应用数据，像照片、文档之类，加密技术同样不可或缺。用户在上传数据之前先加密，云端存储的便是密文，这样能保障数据在云端存储期间不被非法访问，切实确保用户隐私安全。

2.2 数据传输加密

社交应用发送消息时，TLS协议会对数据加密传输，避免数据在网络传输时被窃取或篡改。网络安全机构监测数据表明，未用TLS加密的社交应用，消息传输中被窃取概率约5%，而使用TLS加密后，这一概率降至0.1%以下。这般明显的概率变化，清晰展现出TLS协议强大的防护能力。移动支付应用方面，数据传输加密极其重要。用户支付时，银行卡号、密码等信息经SSL/TLS加密传输，保障支付信息安全，防止因支付信息泄露造成财产损失。物联网移动应用里，设备和服务器之间的数据传输也依靠加密技术，以保证设备数据在复杂网络环境中安全传输。就像智能家居移动应用，借助加密技术保障设备控制指令以及设备状态数据的安全传输，防范黑客入侵操控智能家居设备。有些智能家居应用还运用端到端加密技术，进一步确保数据传输时只有发送端和接收端能解密，有效抵御中间人攻击。

2.3 用户身份认证加密

不少应用采用基于密码的身份认证手段，用户密码在客户端经哈希算法处理后，才传输至服务器，服务器所存储的同样是哈希值。用户登录之际，服务器对输入密码再次执行哈希操作，并与存储值做比对，以此规避密码明文传输引发的风险。指纹识别、面部识别这类生物识别认证中，加密技术用于保护生物特征数据。生物特征数据采集后便加密存储，使用时经加密通道传输并验证，防止生物特征信息遭泄露与滥用。以某移动支付应用的指纹支付功能为例，指纹数据采集后即刻加密处理，支付验证期间，加密后的指纹数据通过安全通道传输到服务器用于比对，保障指纹信息安全[2]。为进一步强化安全性，该应用运用多重加密方式，指纹数据传输时，不但对指纹数据自身加密，还对传输通道加密，同时结合动态密钥技术，每次支付生成不同密钥，大幅提升生物特征信息安全性，让用户支付过程更安全可靠。

3 移动应用加密技术的应用效果评估

3.1 数据安全提升表现

移动应用加密技术大幅提高了数据安全性。数据存储上，加密后的数据极难被破解，有效降低了数据泄露的风险。有统计显示，运用AES加密存储用户数据的移动应用，因数据泄露而使敏感信息被获取的成功率下降超90%。这一成效有力地保护了用户隐私，像用户的身份证号、银行卡号等关键信息在加密存储的情况下，即便应用受到攻击，信息也不易被窃取。数据传输时，TLS加密能切实防止数据被窃取和篡改。研究指出，采用TLS加密传输的移动应用，数据传输时遭受攻击的成功率不到1%。这让用户在使用移动支付、社交聊天等应用时，信息传输更安全可靠。身份认证方面，哈希算法与加密技术的运用，让身份认证被破解的概率大幅降低，保障了用户账户的安全。比如某知名社交应用采用更高级的哈希算法和加密技术进行身份认证后，账户被盗用的事件减少了八成，为用户打造了更安全地使用环境。

3.2 可靠性验证

实验室环境下，开展大量加密、解密测试，模拟形形色色的攻击场景，以此检测加密算法安全性。像针对移动支付应用开展模拟网络攻击测试，检验加密技术能否抵挡常见的中间人攻击、重放攻击等[3]。此类测试能提前察觉加密技术存在的漏洞，进而及时修复，确保应用在实际运用时的安全性。在实际应用过程中，凭借用户反馈与数据分析评估加密技术可靠性。倘若用户未频繁反馈数据泄露或者身份认证方面的问题，且安全事件发生概率低，那就表明加密技术在实际使用中较为可靠。部分安全机构也会对移动应用加密技术予以评估、认证，进一步核验其可靠性。比如某移动金融应用通过国际知名安全机构的严苛测试与认证，其加密技术可靠性获广泛认可，这不但增强用户对该应用的信任，还为整个移动应用行业树立典范。

3.3 现存挑战与解决方案

加密会加重移动设备的计算负荷，对应用性能产生影响，致使应用响应速度变缓。为处理这一状况，开发者运用优化算法与硬件加速技术，比如借助移动设备的专用加密芯片，来加快加密和解密的速度。举例来讲，某款高端智能手机配置了专门的加密芯片，在运行加密应用时，加密和解密的速度提高了50%。这不仅提升了用户的使用感受，也让加密技术在移动设备上的应用更为切实可行。密钥管理同样是个棘手问题，要是密钥丢失或者泄露，就会造成数据安全保障失效。能够采用密钥托管、多因素认证等手段强化密钥管理，保障密钥的安全。加密技术标准不统一也是问题，不同应用采用各异的加密方式，给用户带来麻烦。行业需要加强标准的制

定工作，推动加密技术朝着规范化和统一化方向发展。当前，部分行业协会正积极推进加密技术标准的制定，这种情况有望得到改善。一旦标准实现统一，用户在使用不同的移动应用时，将能够更好地理解并信任其加密机制，从而推动整个移动应用行业朝着健康方向发展。

4 移动应用加密技术的未来发展趋势

4.1 新兴加密技术的应用探索

量子加密以量子力学原理为根基，具备绝对的安全性，从理论层面而言，能够抵御任何类型的攻击。尽管现阶段量子加密技术在移动应用领域的应用仍面临着技术瓶颈以及成本方面的难题，不过在未来极有可能实现重大突破[4]。同态加密技术则允许在密文状态下开展特定的计算操作，直接得出加密后的计算成果，无需进行解密过程，这在移动应用的数据解析场景中展现出巨大的发展潜力，能够在有效保护数据隐私的同时，进行数据的处理与分析工作。就像在医疗移动应用当中，医生能够针对已加密的患者数据展开病情分析，却无需对数据进行解密，从而切实保护了患者的隐私。

4.2 与其他安全技术的融合

将访问控制技术引入，依用户身份与权限对加密数据实施访问管控，以此提升数据安全水平。企业移动办公场景下，仅获授权用户方可读取特定加密文档。数据脱敏技术融入其中，加密数据投入使用或对外分享之际，对敏感信息予以脱敏处置，从而降低数据泄露风险。区块链技术也与之融合，借区块链去中心化、不可篡改特质，强化加密数据安全与可追溯性，全方位保障移动应用数据全生命周期的安全。就像某供应链管理移动应用，借区块链技术记录加密数据流转轨迹，切实确保数据安全与可追溯性。

4.3 应对不断变化的安全威胁

加密技术得不断演进，才能应对新威胁。面对人工智能驱动的攻击，像借助机器学习破解加密算法这种情况，加密技术得引入人工智能防御手段，靠机器学习算法优化加密策略，增强对新型攻击的抵御能力[5]。5G网络普及开来，移动应用数据传输速度加快，数据量增大，加密技术要能适应更快传输速率和更多数据量，确保数据在高速传输时的安全。当下研究人员正研发适配5G网络的新型加密协议，用来满足高速数据传输的安全要求。

结语

对数据存储、传输以及身份认证予以加密，切实增强数据安全性，历经可靠性检验，有力保障了用户数据安全。虽说当前存在计算负担、密钥管理棘手、标准不统一等难题，不过凭借优化算法、强化密钥管理、统一标准等办法，能逐步化解。往后新兴加密技术投入使用、与其他安全技术融合，以及对持续变化的安全威胁加以应对，会促使移动应用加密技术不断进步，给用户数据保护提供更强劲动力，推动移动应用行业稳健、安全发展。

参考文献

[1]李洁,张培勋.计算机网络安全中数据加密技术的运用探讨[J].数字技术与应用,2024,42(04):83-85.

[2]张莉.加密移动应用程序流量分类技术研究[D].哈尔滨工程大学,2023.

[3]杨昕雨.移动应用隐私数据保护关键技术研究[D].北京邮电大学,2020.

[4]聂国春.用户数据安全和隐私保护可望提升[N].中国消费者报,2024-09-27(003).

[5]王辉鹏.移动应用软件架构安全技术研究[J].网络安全技术与应用,2018,(09):83+85.