

人社领域电子信息工程数据加密处理方案

袁肇飞

山东省菏泽市曹县人力资源和社会保障局 山东菏泽 274400

【摘要】近年来,互联网技术越来越广泛应用于社会各个领域,同时引发人们对于信息安全特别是事关公民个人隐私相关数据的关注,同时,信息加密手段的重要性突显出来。特别是人力资源与社会保障领域电子信息工程中的信息处理系统所涉及到的数据处理部分,当前必须制定良好的数据加密手段和技术,以便可以更有效的进行信息加密,从而保证人力资源与社会保障工作在维护人民的信息安全方面能取得更好的成效。

【关键词】数据加密;电子信息工程;人社领域;数据安全;加密方案

Data encryption and processing scheme of electronic information engineering in human resources and social fields

Yuan Zhaoifei

Human Resources and Social Security Bureau of Cao County, Heze City,

Shandong Province Cao County, Heze City, Shandong Province 274400

【Abstract】In recent years, the Internet technology is more and more widely used in various fields of society, at the same time cause people's attention to information security, especially related to citizens' personal privacy related data, at the same time, the importance of information encryption means highlighted. Especially in the field of human resources and social security electronic information engineering of information processing system involved in data processing, the current must develop good data encryption means and technology, so that can be more effective information encryption, to ensure that human resources and social security work in the maintenance of people's information security can achieve better results.

【Key words】data encryption; electronic information engineering; human and social fields; data security; encryption scheme

引言:

随着信息技术高速迅猛发展,电子信息已经应用到社会的各个行业,也应用到人社部门,人社部门有许多信息涉及公民个人,同时也很机密。然而由于近些年各种信息泄露的事故,保护信息与数据安全的方法与技术变得更加重要与迫切。数据加密技术是保护各类电子数据信息安全的关键技术,其应用到了各类电子信息系统中,人社电子信息工程也变得越来越重要,本文从数据加密技术基础方法入手分析了数据加密技术在保护人社部门数据信息安全方面所要面临的问题以及如何设计、改进数据加密技术以保护数据信息的安全性。

1.人社领域电子信息工程数据加密处理概述

1.1 数据加密的基本概念

数据加密是采用相关加密技术,对原始数据进行加密,生成一个不为人知的数据,从而保证数据在传输存储中不被

第三方知道。数据加密是利用相关密钥,只有相关密钥的持有者才能对加密的数据进行逆向处理,变成原始数据。加密技术被大量运用在个人隐私保护、金融交易、通信安全等行业数据管理过程中,保证数据在传输存储中的保密性、完整性和不可抵赖性。在人社工作中,数据加密是非常重要的,特别一些个人身份、社会保障等个人的相关信息都需要通过数据加密保证数据的安全性和完整性。

1.2 人社领域对数据安全的需求

由于社会的信息化发展,人社领域的个人敏感数据信息越来越多,比如,社保、医疗保险、失业救助等个人隐私,这类数据涉及到对人民群众和社会的信任,如果此类数据被黑、数据泄露等问题就容易诱发社会矛盾,严重影响社会稳定。数据信息安全问题越来越明显,包括黑客入侵、数据泄漏等案例层出不穷。如何保障人社信息系统中的信息安全,成为人社信息系统建设的挑战之一。与此同时,针对人社信息系统中的数据加密也面临一系列新的挑战:比如,加密算法的繁杂度高、业务系统之间的互操作兼容性、数据安全加密的同时,保障系统的快速运行。这些挑战要求通过技术方

案予以解决,才能切实保障人社领域信息系统安全稳定运行。

2.人社领域电子信息工程数据加密处理中的难点

2.1 数据加密技术的实施难题

数据加密技术的实施过程中存在很多问题,比如加密算法的选取和实施。不同的加密方式有各自的特征和适用范围,数据加密技术的加密方式如何根据需求来选取,是一个关键性的难题。其次是密钥的管理,密钥的产生、分布、存储及更新等一系列过程都需要加以严格控制,加密密钥的出现必须保证不丢失且不泄露。密钥作为整个加密过程中的核心部件,在系统的结构十分复杂的前提下,如何使其很好地结合到已有的信息系统中,加密过程的透明和实施容易也是难以实施的一个关键问题。当信息系统需要改版升级,数据加密技术需要兼容性的关系,也是值得技术人员不断提升、时刻改进的问题。

2.2 关键数据保护的技术瓶颈

人社领域中保护重要的个人身份、社会保险、医卫数据等数据都需要采用各种技术手段,数据加解密技术可以限制非授权访问数据,但是如何在数据加密的前提下满足加解密后,授权用户可以高效访问和处理数据是一个难题。对于复杂的多种数据结构,一般加解密技术可能降低数据的处理性能与系统响应速度,如何通过加解密保障数据安全的同时兼顾访问和效率的问题,是目前的技术挑战之一^[1]。由于数据存储的分布式趋势,数据的加解密如何才能确保数据加解密后的分布式访问与共享的安全性以及各个节点数据的访问等问题也是当前数据加解密技术的瓶颈。

2.3 加密处理对系统性能的影响限制

虽然通过数据加密可以保护数据的安全,在一定程度上避免了数据泄露的情况,但却会对系统的性能造成影响。加密以及解密都需要消耗系统计算资源,尤其是对加密大量数据的信息系统进行加密操作之后,会降低系统的运行处理速度,延迟系统的响应时间。针对人社等领域中具有较高时效要求的系统,例如社保系统、医保系统等,在对其进行加密处理之时,往往受到系统性能的制约,会影响到业务过程的连贯性与便捷程度。而加密操作不仅仅会对系统造成资源方面的影响,同时也会给数据信息的存取与传输造成一定的压力^[2]。因此,如何实现信息系统安全,又不会对系统整体性能造成太大影响,减少加密操作对系统性能的负面影响成为技术当前的解决困难。这个难题不仅影响着系统的使用,而且也会制约信息系统的拓展性,致使信息安全管理难度大

大增强。

3.人社领域电子信息工程数据加密处理方案探讨

3.1 数据加密方案的设计思路要求

根据人社领域对数据保护的要求,在设计加密方案时,首先需要确定数据加密的预期目标,保护数据的保密性、完整性以及可用性等。其数据加密方案设计的第一步即对数据进行划分、分类和分级,界定需要重点保护的数据信息,例如个人信息数据、社保数据、工资支付数据等,然后选择对应的加密算法以加密这些重要的数据信息。在选择算法时,要综合考虑数据类型,例如,若为实时数据,则其加密及加密的速度必须能满足加密通信数据量的要求,并能维持对系统数据负载的最低影响,因而可以选择对称密钥算法,如 AES 高级加密标准;若为非实时数据,数据加密方案可以选择加密存储,非对称密钥算法,如 RSA 算法的安全性更佳。数据加密方案设计中还要考虑密钥管理,即从生成密钥开始直到销毁过程中如何确保密钥的安全性,避免密钥泄密带来的安全隐患。此外,数据加密方案设计应基于合规性,如在社会领域经常涉及个人敏感数据,该类数据必须符合国家或地区数据保护的法律法规及相关标准的规定,例如欧洲的数据保护和隐私法(GDPR)等^[3]。方案还要具备较高的灵活性,能够根据数据量的大小和数据处理的数据类型动态改变相应的数据加密策略,以应对数据在使用环境中遇到的各种不同情况。此外,数据加密方案应同时满足数据基本安全保护的需求,也要关注数据访问权限方面的需求,避免加密之后由于数据访问权限控制方面的疏漏,导致数据的安全隐患。综上,数据加密方案的制定要兼顾保障数据的安全性和控制加密算法的运行成本与系统性能损耗与用户体验之间。

3.2 数据加密方案的实施步骤要点

在采用数据加密手段开展防护时,首先理清项目的需求与工作范围,确定需要加密保护哪些数据和哪些系统。数据分类标定为工作的第一步,对数据的分类和标定是保证加密工作重点性的基础。选择合适的算法与技术。数据加密为满足不同的数据和加密需求,要选择对应的算法和技术。例如,对于大数据量的加密, AES 比 RSA 更合适,但是当对密钥进行交换与身份验证时, RSA 更适用;对于长期存放、需求长期保密的数据,结合使用哈希和数字签名等技术能够提升数据保密程度。在实施工作过程中,密钥管理工作亦至关重要,需要考虑密钥的存储和分发,密钥的存储、分发过程也需要极高安全性,每个加密过程都有严格的权限控制^[4]。因此,密钥管理系统需要和加密体系有更紧密的结合,确保密

钥的创建、交换和销毁的工作都需要管理及审计,而数据加密的工作也要充分考虑和现有的系统框架是否兼容,因此,在实施过程中也需进行全面充分的测试,以确保不会对系统的运行性能产生过大的负面影响,如数据的处理时间以及系统的响应性能。当系统投入运行后,需要对系统进行长期的监控和维护,及时修复加密体系出现的缺陷,保持长期的工作效力。

3.3 加密技术在数据处理中的具体应用

应用到数据操作处理的加密技术主要分为数据传输加密和数据存储加密。数据传输加密主要是保证传输过程中的数据安全,例如应用最广泛的 TLS/SSL 协议可以确保网络传输过程中的数据安全,能防止网络上的数据被窃取篡改。在人社部门主要应用在社会保障数据、个人信息数据的网络传输过程中,确保在网络传输时,这些敏感数据不会被第三方盗听、篡改。数据存储加密则主要用来确保在存储介质上存储的数据安全,特别是当存储介质被盗或者非法访问时,存放在其中的敏感数据内容也是不可读的。这些技术典型应用在磁盘加密以及数据库加密,特别是在应用云存储的大背景下,数据库加密成为保护存储数据安全的重要技术之一,比如企业单位可能会将存储的包括社会保障信息在内的重要数据存储到云端,那么采用加密数据库系统则可以确保哪怕云服务提供商工作人员也无法访问到数据^[5]。结合基于角色的访问控制(RBAC),还可以进一步增强数据安全,防止由于错误权限设置出现的数据泄密。加密技术还可以与身份认证结合,通过访问数据时用户仅具备访问加密数据的权限才能访问到。比如可以基于多因素身份验证(MFA)的技术,在需要访问到敏感数据的时候进行2因素甚至是3因素的认证,进一步增加系统的安全性。

3.4 加密处理方案的优化与保障措施

为了提升加密方案优化的效率和降低成本以及系统的长期稳定性,需要针对加密算法的优化。针对密码算法的优化主要是为了提升效率,因此对于高负荷的系统,使用硬件

加速加密(使用GPU或者专用加密芯片),可以提升系统加密的处理能力,而且随着硬件加速对安全影响不会很大。对于低负荷的系统,可以选择轻量密码算法来减少资源的使用;针对不同的数据和应用场景的加密算法设计,使用分层的加密方案,能够提升处理的效率和系统资源的消耗;加密方案的优化另外一个难点在于密钥的管理,对密钥管理系统使用基于HSM的方案,有效保证了密钥的存储和使用,在密钥的管理上,可以使用周期性的密钥更新,选择全自动化的密钥更新系统可以提升密钥管理的效率;在整个过程中,使用了密钥生命周期管理(KLM)可以进一步加强整个密钥使用过程的安全性。为了让密钥方案能在长期稳定的工作,系统中还要集成自恢复系统,可以自动监测出漏洞,修补漏洞,防止被不法分子利用。定期进行系统的安全审计与漏洞扫描,及时发现风险与安全漏洞并进行修补,是维护加密方案稳定有效的日常性工作,加强用户的系统安全意识教育培训,使其了解日常使用中可能存在的一些安全问题,也将为加密方案的有效实施提供重要保障。加密方案实施不应局限与技术方面,同时也应结合组织整体安全管理框架的要求,通过制度、过程化的方式保证加密方案的有效性^[6]。融合业务与合规的视角,定期完善加密处理方案的修改和完善,使其持续应对不断变化的安全环境与技术要求。

结束语:

越来越多的数据信息泄露事件的发生,也促使了数据安全成了各领域尤其是人社领域所关注的一个点。本文在针对数据加密技术进行研究与应用分析的基础上,提出数据的加密处理,以便在实际的数据应用过程中,可针对数据的人事单位电子信息工程技术所提供技术支持与措施,解决数据处理安全的问题。由于当前数据加密技术存在着实施困难以及性能等不足,但是随着数据加密技术的完善与措施的不断优化与应用,将会为数据提供有效的安全保障。

参考文献

- [1]王晓波.网络信息安全中数据加密技术的应用研究[J].信息安全研究, 2020, 9(01): 35-38.
- [2]李建国.数据加密技术在电子政务中的应用研究[J].信息技术与信息化, 2019, 12(10): 52-55.
- [3]陈建辉.数据保护中的加密技术探讨[J].网络安全技术与应用, 2021, 8(03): 121-124.
- [4]刘志远.人社领域数据加密处理的关键技术[J].信息安全与通信保密, 2022, 30(06): 17-21.
- [5]张婷.信息系统中数据加密技术及其在政府部门中的应用[J].计算机与数字工程, 2021, 49(05): 74-76.
- [6]王彬.信息安全领域的加密技术现状与挑战[J].计算机科学与探索, 2020, 14(02): 102-105.