工程与管理科学
Engineering and Management Science
第 7 卷◆第 7 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

物联网环境下电子信息安全管理机制研究

佟昊萌
身份证号码：210105199202213715

DOI:10.12238/ems.v7i7.14246

[摘　要] 在物联网应用越来越多的情况下，其安全性问题也越来越突出。针对这一问题，本文将从设备访问、数据传输和存储安全、网络体系结构架构和网络安全实际应用等方面对其进行研究。深入研究加密算法的应用，完善身份认证系统，创新入侵检测和防御方法，建立多层次、全方位的安全保护体系。本文研究成果将为未来物联网与电子信息技术的交叉融合奠定基础，促进相关产业的健康发展，减少隐患。

[关键词] 物联网；电子信息；安全管理

物联网（IoT）是当今信息技术的重要发展趋势，对人类生产、生活等方面产生了巨大的影响。随着物联网的普及，我国的电子信息产业迎来了新的发展契机，同时也面临着安全、隐私和管理方面的挑战。物联网以互联设备为基础，完成数据的采集、传输、处理与应用。由于设备规模巨大，具有异构性、实时性和移动性等特点，使得整个网络的开发与管理变得更加复杂。在物联网的背景下，需要在保证数据的安全性、可靠性的前提下，有效地进行数据的传递与处理。物联网设备具有海量、敏感和易遭受攻击的特点。由于硬件设施受限，导致密码算法难以实现。设备品种繁多，安全隐患多，易成为网络攻击平台。无线通信协定存在缺陷、网络界限不清、传统的保护无法发挥作用。由于移动设备采集用户的数据，使得用户的隐私难以保障，而协同则会加大泄露的危险。

1物联网环境下面临的安全问题

由于物联网的快速发展，我国在这方面的研究也有了长足的进步。目前，我国已从多个方面开展了物联网的安全研究，并在软件安全机制、轻量级密码算法、差分隐私保护等方面取得了一定的研究进展[1]。国际上在这方面的研究处于国际前沿，目前已有的研究成果包括：利用 PUF 进行身份认证，QKD 加密通信，同态加密隐私保障等。物联网是当前信息技术的重要研究方向，它通过互联网将设备、传感器和设备等设备接入到一起，进行实时的采集、传输和处理。随着物联网的普及，其安全性面临着越来越多的挑战。由于设备数量众多、运算容量有限、资源有限等原因，具有先天的弱点。由于硬件因无法及时升级，导致长期存在安全性缺陷，从而使得黑客可以通过这些缺陷来获得对设备的控制。有些设备是在工厂生产时预设的使用者名称及密码，使用者不能变更，因此会加大遭袭击的危险。

2物联网环境下电子信息安全管理架构

2.1 架构设计

对物联网中的安全保护系统进行了研究，并对其进行了详细分析。其中，感知层承担着用户的身份认证（PKI 或轻量级密码算法）、固件安全性检验（静态分析和动态分析）、异常行为监控（机器学习算法）、物理环境监测（传感器和摄像头）等。网络层面保证信息的安全性，主要研究内容有：（对称和不对称加密、哈希、数字签名）、网络分区管理（VLAN、NAT）、攻击行为识别（特征匹配、行为分析）、恶意流量过滤（NGFW，DPI）等。平台级对 IoT 进行管理，对 IoT 进行全面的控制，使用 RBAC 和 ABAC 对接入权进行管理，PAM 对恢复权进行动态分配，ELK Stack 对日志进行监测，SPM 对安全性进行管理。在应用层面，通过对 IoT 服务进行安全性测试，对其进行静态分析和动态测试，发现系统的缺陷，并通过软件的自动维护和手工修补，使用同态加密和差分隐私来保障用户的信息，APM 监测系统的运行效率[2]。其中，以管理者为中心，负责对系统的安全性要求进行解析，并通过 TI 平台进行系统的风险智能采集，IRMS 对系统的安全事故进行及时的反应，并对系统进行持续的改善评价。上述安全管理架构的建立，能够综合解决物联网的各种安全隐患，保证整个网络的平稳运行。

2.2 制度策略

在建立了网络安全保障系统之后，要保证网络安全保障系统的高效运行，需建立完善的安全制度及组织管理制度。企业应当设置安全生产领导小组，统筹安排各项工作，制订

相应的安全生产管理规定及作业规范。该制度包括设备管理，数据保护，紧急情况处理等方面的职责划分，例如 IT 部的技术保护，数据的管理，法律法规的审核。构建交流机制，实现信息交流和协作。以技术落地为中心，分步实施，先行试验，再逐步扩大。在资源有限的情况下，采用轻型的方法进行资源分配，在重点服务器系统中进行先进的保护。在实际应用之前，需要进行一系列的测试，包括功能测试，性能测试，兼容性测试和安全性测试。安全系统既要有技术措施，也要有人的投入。企业要加大员工的培训力度，增强员工的安全观念与技术水平，加大网络安全宣传力度。组织经常性的紧急情况演习，并检查计划的执行情况。建立不断改善的制度，对各项安全行动的执行状况进行周期性的评价，不断地进行技术升级和完善。在生产过程中，要有良好的工作环境，要及时发现问题，及时提出建议和解决问题。建立基于物联网的电子信息项目的安全防御系统，保证整个网络的安全性和稳定性。

2.3 物理策略

在构筑“不可摧毁”的网络防御体系中，物理存取是最根本的，也是最根本的保障，即仅允许被授权的个体使用。提出了一种基于生物识别技术的智能卡与加密技术。比如，像指纹、眼底扫描这样的生理特征，就可以有效保护用户的隐私。在当前频繁发生的信息泄露中，物理层的存取控制显得尤为重要，其设计与实施要根据企业的实际环境，通过对企业内部环境的风险进行评价，并制订相应的安全政策，以保证企业的总体安全目标。环境安全既要保护物质空间，又要注意对设施的工作环境进行监测与维修。比如，如果对一个数据中心的温湿度进行控制，就有可能造成系统的硬件失效，严重的还会引起火灾。按照 ISO27001 的规定，为了保证企业的信息财产的安全性，企业必须对企业进行环境危害评价，并采取相应的控制行动[3]。在电子信息安全领域，环保是非常重要的。而在设备防护方面，需要对这些产品进行一系列的防护，以避免对产品的损坏和对产品的非法存取。构建防震、防水、防尘的机房，并装有监视摄像机和警报系统，以避免未经许可的身体触摸。

2.4 技术策略

在进行电子信息工程技术的安全管理工作时，必须要在技术层次上进行相应的管理，通过电脑设备来对使用者的资料进行加密，可以提高使用者的资料储存的安全与可靠度，以此来减少在使用电子信息工程技术时可能出现的隐患。不对称密码与对称密码不同，它的加密与解密所需的密钥并不相同，所以要进行解密，需要确保两者的一致性，尽管公共密钥是公开的，但私有密钥的隐私性更强，可以更好地对数据进行加密，提高了使用者的信息安全。从电子工程信息技术的安全角度来看，防火墙也需要进一步的完善，这是一种比较常用的安全防护手段,它可以用来增强企业的内外网络，当有一个不熟悉的接入信息请求接入到互联网上时，它会对接入的信息进行自动的判定，如果发现接入的是一个有敌意的消息，就会被主动地拦截，防止有任何的恶意消息进入到系统中。在使用中采用了“身份验证”的方式，要求使用者注册一个帐号，以便对其进行信息的存取。此外，在电子信息工程技术的应用中，也要进行定时的杀毒，对可能出现的恶意程序和病毒进行监控和清理，并将其安装在系统中，可以对其进行定期的病毒搜索，并对其进行实时的修补，以此来确保电子信息工程技术的应用安全[4]。对物联网中的信息采用密码技术，可以有效地避免在传送、储存时，被人窃取或修改。当前，常见的加密方法有对称加密、不对称加密以及哈希加密等。提出了基于网络的安全管理系统。当前，通用的认证与访问控制方法主要有：实名认证，生物识别，令牌认证等。入侵检测与防护是指对物联网中的各种设备及网络进行实时监控，及时地对其进行监控，及时地对其进行监控，从而对其进行有效地防护。当前，常见的入侵监测与防护技术有防火墙、入侵监测系统、安全事件管理等。安全审核及记录的方法；基于分布式存储的、面向大规模物联网应用的新型物联网系统。通过对网络中发生的各种安全事故及记录数据的统计，能够及时地识别出网络中存在的威胁或恶意攻击，从而制定出有效的防御策略。当前，常见的安全审计与日志管理方法主要有日志分析工具、安全审计等。以保证物联网的安全、可靠地工作。采用密码技术，可以有效地避免在传送、保存时，出现信息泄露、伪造等问题。常见的加密方法有对称加密，不对称加密，哈希加密等[6]。为了保证物联网中的设备的安全性，需要对其进行认证。通过对设备的识别，可以有效地阻止非授权设备进入 IoT。常见的认证方法有基于钥匙的认证，基于证书的认证等等。借由设定使用者或设备的存取权利来阻止非授权的存取与运作。目前

常见的访问控制方法有：基于角色的访问控制，属性的访问控制，等等。

2.5 管理策略

在进行电子信息工程技术的安全管理工作时，必须要有一个专门的技术管理人员来做，因为它是一种高科技产品。所以，在进行电子信息工程的安全管理工作时，要制定出一套完善的人才竞争体系，让专业的专业人员能够更好地投入到企业的经营之中，以一种全新的思想来进行企业的安全工作，以此来提高企业的安全管理水平和工作效率。要重视提高员工的安全观念，同时也要加大对电子信息工程师的训练力度，用训练手段来逐渐提高员工的安全意识，从而将安全问题的发生从根本上降低。此外，还应对员工进行全方位的安全防护培训，提高员工的专业素质，在员工中营造良好的安全环境，降低信息泄漏现象的发生，确保电子信息工程技术的安全。在安全管理工作的同时，要将安全管理职责贯彻到底，实行安全管理责任制，由安全主管对电子信息工程技术的运用状况进行定期的审核，并对其进行分析，一旦出现问题，就会立即解决，让安全责任落到每个人的身上，这样才能更好地发挥出电子工程的信息技术运用的威力，提高其使用的安全性[5]。

3基于物联网的电子信息保密系统在实践中的运用

通过对智慧家庭系统的分析，提出了基于网络的新型安防系统。在智能家庭系统中，使用密码学方法来对使用者的资料进行密码化，有效地避免使用者在传送、储存时，资料的存取与修改。利用入侵探测与防护等方法，对智能家庭中的各种设施及网络进行实时监控，及时地对其进行监控，及时地识别出各种异常情况，并对其进行防范；通过对家庭设备及网络进行安全性审核、日志等手段，实现对家庭设备及网络中发生的各类安全事故及日志等进行有效的监控，并对其进行安全性分析与追溯。提出了基于多层网络的新型网络安全防护方法。

以“智慧住宅”为例，利用无线通信技术，把多种智能设备连接在一起，对住宅进行智慧的管理与控制。但是，随着无线通信的普及，其自身的安全性问题也日益突出。黑客可以通过监听无线通信线路，破解密码算法，实现对智能家居的远程控制，严重时会危及住户的安全。为了保证住宅的安全性，将电子信息安全技术引入到住宅小区中来是非常必要的。在工业控制中，基于网络的传感器网络已经成为新的研究热点。但在实际应用中，由于其所处的行业环境复杂多变，其安全问题也受到了极大的挑战[7]。比如，黑客可以通过对生产线的控制系统进行攻击，从而造成生产线的停滞或者制造错误；要么就是偷取了产品资料，给企业带来了巨大的经济损失。为了保证企业的正常运行，将电子信息保密技术引入到工控系统中是十分必要的。虽然在这方面已经有了很大的进步，但是仍然有很多问题有待于进一步的研究。首先，已有的安全性研究多是针对某个具体的安全问题而设计的，并不能提供完整的安全性解决方法。面对日益复杂的网络环境，以及日益多样化的网络安全问题，迫切要求研究更加综合灵活的网络安全方法。

结束语：

随着电子工程信息技术已经被应用到了各个行业、各个领域，而且还在持续地进行着革新和发展。然而，伴随着物联网技术的应用，安全性问题也日益凸显，很有可能发生信息数据丢失、被盗等危险，如果发生这样的事情，将会给电子信息工程技术应用公司带来很大的危害。为此，有必要对其进行安全管理，从技术层次和管理层次进行，从而保证其在电子工程中的安全使用。

[参考文献]

[1]董会祥.5G 与工业互联网融合中的电子信息技术应用[J].中国宽带，2024，20（11）：153-155.

[2]冯炳鑫.电子信息工程与计算机网络融合在物联网中的应用[J].电子技术，2024，53（11）：98-99.

[3]韩晓敏，张洪亮，刘杰.电子信息技术在智能制造中的应用与未来发展路径研究[J].造纸装备及材料，2024，53（11）：124-126.

[4]穆春林.基于电子信息技术的虚拟仿真实验教学平台构建研究[J].家电维修，2024，（11）：65-67.

[5]赵晓光，张玲霞.计算机通信技术在电子信息工程中的应用研究[J].中国宽带，2024，20（10）：133-135.

[6]阮晓涵.计算机通信技术在电子信息工程中的应用研究[J].电子元器件与信息技术，2024，8（10）：179-181.

[7]党啸.电子信息技术在建筑楼宇智能化工程中的应用[J].信息与计算机（理论版），2024，36（19）：141-143.