研究与开发

面向能源互联的电力物联网安全架构及技术

张翼英[1]，周保先[1]，庞浩渊[2]，曹津平[3]，张桐嘉[4]

（1. 天津科技大学人工智能学院，天津 300457；2. 北京遥测技术研究所，北京 100761；
3. 国家电网有限公司信息通信分公司，北京 100761；4. 北京工业大学，北京 100124）

摘　要：电力物联网平台是能源互联网数字化创新服务的重要支撑，覆盖电力系统各个环节，存在诸多新的安全问题：如何实现电力物联网的广泛可信互联和可靠感知，如何实现电力系统的智能防御和安全互动，如何解决电力信息系统的数据、应用和密钥安全等，这些是当前电力物联网需解决的重要问题。面向能源互联网发展状况，对电力物联网安全需求及安全特点进行说明分析，在此基础上提出电力物联网安全框架及防护思路，总结电力物联网安全关键技术并对未来相应的发展方向进行说明。

关键词：电力物联网；安全技术；能源互联；安全架构

中图分类号：TN918

文献标识码：A

doi: 10.11959/j.issn.1000−0801.2021028

Electric internet of things security framework and technologies for energy interconnection

ZHANG Yiying[1], ZHOU Baoxian[1], PANG Haoyuan[2], CAO Jinping[3], ZHANG Tongjia[4]

1. College of Artificial Intelligence, Tianjin University of Science & Technology, Tianjin 300457, China
2. Beijing Research Institute of Telemetry, Beijing 100761, China
3. State Grid Information & Telecommunications Branch, Beijing 100761, China
4. Beijing University of Technology, Beijing 100124, China

Abstract: Electric internet of things platform is an important support of energy internet digital innovation service, covering all aspects of power system. There are also many new security problems: how to realize the widely trusted interconnection and reliable perception of the power internet of things, how to realize the intelligent defense and security interaction of the power system, and how to solve the data, application and key security of the power information system. These problems are important tasks to be solved in the current power internet of things. Based on the development of energy internet, the security requirements and characteristics of power internet of things were analyzed. On this basis, the security framework and protection ideas of power internet of things were put forward. Then the key security technologies of the power internet of things and its future development direction were summarized and explained.

Key words: electric internet of things, security technology, energy interconnection, security framework

收稿日期：2020−09−08；修回日期：2021−01−02

通信作者：周保先，945770721@qq.com

1 引言

随着能源互联网的大力推进，电力信息系统与物联网技术联系愈发紧密，发展电力系统通过部署大量现场采集部件、智能终端、感知设备等将电力方面用户及其设备以不同的方式连接起来，形成智能防御、安全互动、可信互联的电力物联网（electric internet of things，EIoT），通过对电力系统设备进行控制感知，实现电网的智能化、互动化和信息化，对能源互联网的快速发展起到重要作用[1]。

2014 年中国提出了能源生产与消费革命的长期战略，并以电力系统为核心试图主导全球能源互联网的布局。至 2017 年，全国首批能源互联网示范项目已陆续开展。电力物联网作为“新基建”信息支撑设施，更加侧重于突出产业转型升级的新方向，将与坚强智能电网相互协同并进、相辅相成、融合发展，包含智慧化、多元化、生态化特征的“另一张网”[2-3]，并不断向用户侧、应用侧、服务侧延伸。但是，电力物联网具有泛在、开放、互联等特点，使本来相对封锁、专业和安全的能源安全系统始终保持开通，网络安全漏洞存在于系统各业务环节。同时，管理网和控制网的相互间信息交互成为“新常态”，控制权限不停增加，加大了攻击点、受攻击面和安全的网络边界。黑客可以利用边缘计算网络节点进行一系列攻击操作，如信息窃听、增添虚假信息、注入木马病毒等攻击，使得安全威胁向电力系统广泛蔓延，所以电力设备及相关网络的安全也应受到相应的重视。能源互联网电力信息系统关系到国民生计，若受到入侵或遭到破坏，会严重威胁到国家的安全及广大人民的利益[2]。

2015 年乌克兰国家电网因“暗黑力量”的恶意代码遭受攻击，造成大面积的停电事故[4]。2016 年他国黑客通过非法途径，入侵了美国网络，进而控制大量物联网终端设备使其发动 DDoS 攻击，致使近一半的美国网络发生异常；2017 年在多个国家发现针对变电站智能终端的恶意软件，可对全球近百个变电站的智能终端进行控制。2019 年，委内瑞拉发生了有史以来从未有过的大规模停电，全国仅少部分地区未受到波及。以上事件的攻击者大多以使用错误代码为主要攻击工具，发送恶意代码直接攻击，暴露出漏洞，通过网络操控令其停电，以达到摧毁破坏电力系统致其迟滞、致盲的目的[5-10]。

在电力物联网发展过程中，行业保护范围日益扩大，安全边界逐渐模糊，将会暴露出更多的攻击面，传统安全体系不能适应新的要求，安全风险日益加剧。因此，面向能源互联网的电力物联网安全问题，成为研究热点。参考文献[11-12]对电力网络中数据漏洞挖掘技术提出相应的技术。参考文献[13]介绍电力入侵检测技术的基本原理，以 BP 神经网络为例进行介绍。参考文献[14-15]介绍拟态防御技术原理，并说明 IPO 模型。参考文献[16]说明电力行业当前作用及相关保障。参考文献[17]隔离交换技术原理和主要特性。参考文献[18-19]介绍身份认证技术和 VPN 技术在电力行业的主要应用和基本原理。参考文献[20-22]介绍量子通信技术在电力物联网中的特性，且说明其主要特点。参考文献[23-26]对电力物联网应用层及数据层中数据隐私防护技术、加/解密技术和区块链技术等技术原理及相应特点进行说明。

电力物联网的智能终端将成为攻击电网的主要目标和跳板，直接影响能源互联网的安全稳定运行。如何保护能源互联网及其设备不受网络侵害和干扰，是当前刻不容缓的任务。本文面向能源互联网，根据电力物联网的基本特征，探讨了其安全需求和特点，并提出了相应的安全架构和防护思路，介绍了电力物联网的安全关键方法及技术，并对电力物联网将来的发展提出建议。

2　电力物联网的安全需求和特点

2.1　电力物联网安全需求

（1）可靠感知的需求

在能源互联网的运行和维护过程中，电力物联网感知层中的传感器感知并采集相关多种数据，而大量传感器、智能设备终端及其不同的接入方式，给能源互联网安全系统带来新的、未知的安全隐患。因此边缘可靠感知、防御跨空间（信息–物理）的联动攻击成为电力物联网安全运行的前提和保障，是极具挑战性的难题。

（2）可信互联的需求

能源互联网立足于网络互联，覆盖了电力物联网网络层各个环节，包括短距离无线通信网络、无线公网/专网、EPON、主站与通信网络层边界和主站局域网等。在其连接过程中，需要根据电力物联网不同应用方向，选择不同连接技术。通过安全身份认证、密码服务等，建立可信互联环境，保障资源、服务的安全互动，实现全域安全互联互通，是实现网络共享的有效支撑[9-10]。

（3）智能防御的需求

能源互联网架构复杂、应用繁复，且拥有高频动态、海量数据，因此需要电力物联网在应用层及数据层实现安全、全面集中管控，促成多能协调利用和能效管理，建立需求感知、智能共享和主动防御机制，结合大数据技术、拟态防御技术、人工智能技术等，实现业务安全审计、数据安全防护、风险智能处理。

2.2　电力物联网安全特点

鉴于能源互联网具有高效智能、开放互联、平级互补和开源节流等特点，对比传统安全，电力物联网具有以下特点。

（1）边缘计算安全

能源互联网部署了海量各异的终端设备，在电网边缘侧形成边缘计算网络，负责将网络中传感设备节点和数据统一接入骨干网中，具有用户控制、业务提供、业务监测等重要业务功能。不同于传统的计算机终端，边缘计算网络中接入的电力物联网传感设备节点种类繁多、网络异构、协议不同、数量庞大；同时，由于边缘计算终端所汇聚接入的电力物联网传感设备节点计算资源受限、长期运行，传统“补丁”安全加固机制无法适用于物联网传感设备节点，非受控环境下传感设备节点被恶意利用的风险极高，导致边缘计算终端极容易成为攻击目标或跳板。因此，如何有效进行网络的主动防御，提前检测防御来自电力物联网传感设备节点的远程渗透攻击行为，建立实时安全防御体系是需要重点研究的课题之一。

（2）跨空间复杂联动攻击防御

泛在计算业务系统伴随计算能力下沉后，在边缘侧形成了全时域空域互联的边缘分布式计算系统，与电网控制网跨“信息–物理”空间实时互联，结构比较复杂，表现出混杂多尺度的动态特性与复杂网络特性。有别于传统电网“N–1”或“N–2”等故障性质，其安全威胁可能会引起连锁性反应，针对边缘计算网络攻击会影响终端设备执行监测功能的能力，增加了系统的脆弱性，造成两网的相互穿透，甚至可能危及物理网，产生大扰动，从而威胁电力系统安全。

3　电力物联网的安全架构和防护

3.1　电力物联网安全架构

从技术视角看，基于能源互联网思想的电力物联网可分为感知层、网络层、平台层、应用层和安全防护 5 个部分，如图 1 所示，其中感知层实现泛在互联及可靠感知；网络层实现全时空覆盖；平台层实现开放共享、安全互动；应用层加大业务创新、智能防御；网络安全防护保障其可信互动及安全互动。

感知层主要实现以智能传感设备为基础的泛在互联，将电力物联网的末端信息进行采集并上

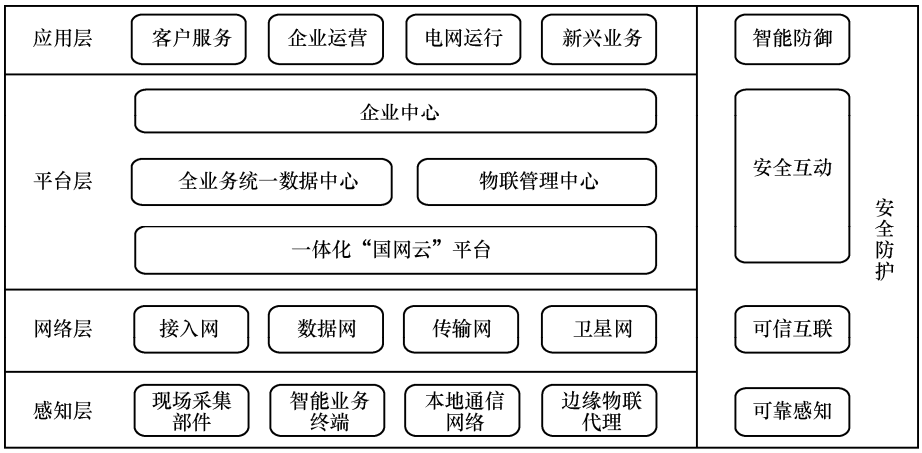

图 1　电力物联网安全架构

传。采集对象包括电网基础设施、运行环境、运行状态以及电网接入应用侧状态等。随着电力物联网业务的不断深入发展，感知层逐渐延伸到用户侧，配用端神经末梢是其根本基础。网络层是电力物联网业务输送通道，电力物联网建设网络层的重点任务是全时空覆盖构建“空天地”协同一体化的电力泛在通信网，加大网络覆盖范围，增强网络的带宽，提升系统调配能力。

平台层的关键技术是开放共享，例如，国家电网公司提出的“国网云”一体化平台根据云基础设施、云平台组件、云服务中心和云安全软件合成，能够实现设施、数据、应用等 IT 资源的一体化管理，进一步加大信息的存储、传输等服务水平，有力促进业务集成融合，缩短应用的上线时间，快速响应业务变化，从根本上提升国网客户便捷性，加大电力系统安全工作的可靠性。应用层承载对内、对外业务，感知层、网络层和平台层实现网络基础支撑和数据共享承载。

3.2　电力物联网防护思路

（1）电力物联网发展

构建安全可靠的网络体系，推广以“安全”和“业务”为核心的防护理念，对可靠感知、可信互联、安全互动和智能防御等相关技术进行研究，并开发应用。从能源物联网基本特性提出电力物联网安全防护思路，根据架构安全等服务技术，保证物联网电力数据从采集到传输，再到整合应用的安全过程，具体如图 2 所示。

（2）可靠感知和可信互联

建成全场景网络安全体系，为能源互联网产业生态奠定安全基础，促进能源行业安全互动。

（3）安全互动

以动态配置、组合复用方式快速满足业务安全防护需求，通过统一建设物联安全框架，配置全景安全监测与智能处置等技术装置，避免重复发展，节约建设成本。

（4）智能防御

通过安全芯片和关键技防措施，提升终端安全管控能力，实现物联终端的统一身份安全管控，解决“谁是谁”的身份安全标记和验证难题；提升物联安全交互能力，解决万物互联时的信任问题和安全可靠问题，实现交互权限可控、交互行为可查、敏感交互保密。

4　电力物联网安全关键技术

为了保护电力物联网敏感信息、预防信息被攻击者通过侦听等方式获取，且接收方可以正常安全地获得所需的信息，根据图 2 将电力物联网的相关技术分为感知层、网络层和应用及数据层 3 类，对此分别进行描述。

<table>
<tr><td rowspan="2">智能防御</td><td>架构安全</td><td rowspan="3">数据隐私防护技术</td><td rowspan="3">加/解密技术</td><td rowspan="3">病毒防范技术</td></tr>
<tr><td>在系统规划、建设、运维过程中同步考虑安全能力的建设</td></tr>
<tr><td rowspan="2">安全互动</td><td>主动、被动防御</td></tr>
<tr><td>消耗攻击者资源、迟滞攻击，通过持续检测、分析、对抗高级威胁</td><td colspan="3"></td></tr>
<tr><td rowspan="2">可信互联</td><td>威胁情报</td><td>防火墙技术</td><td>隔离交换技术</td><td>身份认证技术</td></tr>
<tr><td>收集数据，挖掘信息，生产和共享情报，猎取捕获新的威胁</td><td colspan="2">VPN技术</td><td>量子通信技术</td></tr>
<tr><td rowspan="2">可靠感知</td><td>进攻反制</td><td colspan="2">漏洞挖掘技术</td><td>入侵检测技术</td></tr>
<tr><td>以自我保护为目的，在规定框架下，对抗入侵者的措施</td><td colspan="2">安全态势感知技术技术</td><td>边缘计算安全技术</td></tr>
</table>

图 2　电力物联网网络安全防护思路

4.1　感知层安全关键技术

4.1.1　漏洞挖掘技术

电力网络漏洞引起漏电且增加访问权限，使黑客可以在安全范围内外进行操作，从而诞生了漏洞挖掘技术。漏洞挖掘技术包含数据挖掘、Fuzz 原理、二进制对比和网络爬虫等技术。其中，数据挖掘是根据相应的信息获得漏洞原因，通过网络爬虫等方法可以得到数据信息，通过爬虫技术对信息进行处理、整合、分类等，然后通过特定算法或统计来抽取有用信息。数据挖掘可以进行故障异常情况分析，充分使用数据分析技术、网络安全检测等技术，获得电力网站、基站或者系统存在的问题，对相关异常进行修复。Fuzz 原理技术是一直不断地进行数据测试，将可能发生错误漏洞的位置无限放大，从而可以进行修复，该技术测试时需要大量的数据样本，以发现异常的数据，其根本原理是通过异常数据来发现可能存在的漏洞[11-12]。

4.1.2　入侵检测技术

入侵检测可以造成网络安全隐患威胁的入侵行为，对这种行为进行实时动态监控、检测、抵御，是入侵检测技术的基本内容。入侵检测技术先将电力网络上的运行信息收集起来，包括行为信息、网络数据等；之后对得到的信息进行系统的分析、检测，并将收集到的数据信息进行统计、分类等分析；最后依据数据的分析结果设计相应的防御措施，在进行网络安全测试的时候进行风险判定并制定对应解决方案，若被入侵的概率较高，需专门制定防护方案，如图 3 所示即入侵检测系统框架。

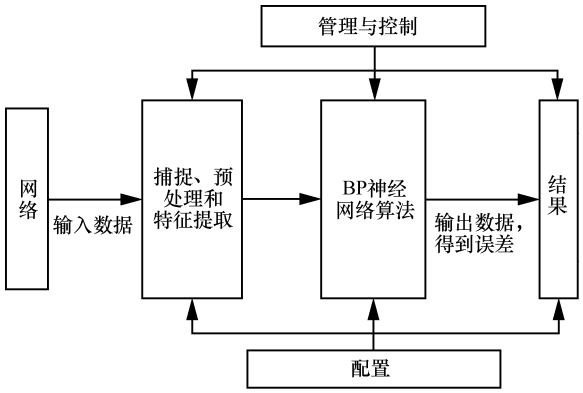

图 3　入侵检测系统框架

根据 BP 神经网络的入侵检测系统，捕捉实时网络流量数据之后进行预处理，将数据转化成标准的二进制形式，然后通过 BP 神经网络算法进行训练，对输入网络数据进行分类，确保每个神经元节点的构建能表示正常、潜在的攻击行为；之后输出结果，若检测到网络异常则发出预警，并及时处理[13]。

4.1.3　边缘计算安全技术

边缘计算网络属于一种混合网络架构，涉及

多个环节、多种技术。针对边缘计算网络的安全防护技术包括密码防护、安全模型、访问控制策略、主机加固、异常检测、关联分析等。在终端渗透防御方面，现有边缘计算终端安全主要利用密码技术、可信计算技术实现终端的安全认证与数据存储计算安全。通过边缘计算终端行为特性进行动态学习和动态度量，检测出恶意终端的渗透攻击行为且不能进行提前防御控制。在数据安全交互方面，采用密码技术和安全传输协议，并结合网络攻击危害程度自适应调整数据传输方案确保传输效率，同时约束数据输出，保障隐私不泄露，进而抑制网络攻击行为。在系统攻击防御处置方面，针对电力物联网特性，需要考虑协同、联动的安全处理方法，如通过告警关联分析的防御处置技术和基于状态攻击图的防御处置技术有效防御，边缘计算安全架构如图 4 所示。

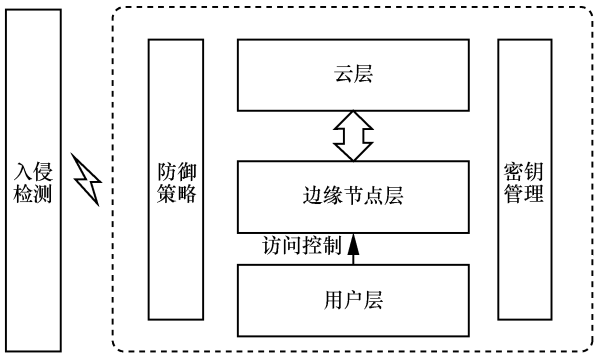

图 4　边缘计算安全架构

4.1.4　拟态防御技术

拟态防御技术是以功能等价、结构相异的计算或服务组件为元素，以具有高可用性、高可靠性的“非相似多余度”结构为基础，配合不依靠规则与特征为基础的多模表决机制，并通过系统对外特征的非线性变换扰乱攻击者的判断。目前，基于拟态防御技术思想构建的主动防御模型基本为 iPo 模型，如图 5 所示，当提交的请求输入进入系统后，首先经过输入代理单元将其复制成 n 份转发至执行体集中，执行体集中包含 n 个相似冗余执行体（$P_1, P_2, \cdots, P_n$）；每个执行体接受 1 个请求的副本并处理，经过表决器的表决后输出响应。利用网络攻击对于环境的依赖性，一次针对特定漏洞的攻击无法同时在异构的执行体中有效发挥，从而达到了抵御漏洞攻击的防御效果。目前基于拟态防御技术已经形成了拟态防御构造路由器、拟态防御构造分布式存储系统、拟态防御构造 Web 服务器等多种具有拟态防御构造的系统。

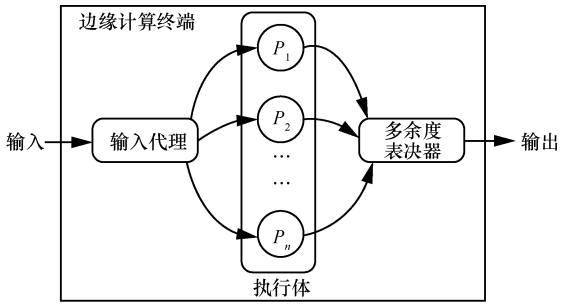

图 5　拟态防御 IPO 模型

4.2　网络层安全关键技术

4.2.1　防火墙技术

电力系统外部网与内部网间有一道屏障，称为防火墙，防火墙可以对网络安全的数据信息进行安全性操作，防火墙能为电力系统的信息安全与网络安全提供保障。隔离控制技术是防火墙技术中使用最为频繁的技术，极大地制止保护体系外的输出和访问。一些复合防护的技术使需要保护的信息处于安全状态，运用动态过滤有较大的效果。根据电力设备的运行目标和防火墙访问策略，得到地址和相应端口，发现电力设备网络系统的当前运行情况，为电力信息的安全工作开展添加有效的保障[16]。

4.2.2　隔离交换技术

随着信息安全技术的突飞猛进，网络安全的隔离交换技术成为被广泛使用的全新技术。隔离交换技术先进行人工数据交换，在两个网络完全断开的情况下进行数据交换；之后是网络硬件隔离，就是将电力设备进行分开归类；最后进行生成网络隔离交换技术。该技术运用相应的结构模

型，主要是防止一些 TCP/IP 的协议攻击，保障电力系统的安全，其次是使用交换的存储器，可以加快安全信息的交换[17]。系统收到数据后，对其数据包进行全面扫描，根据其特性和数据对比分析得到需要的 IP 地址和端口等相关信息。

4.2.3　身份认证技术

身份认证技术是并行计算、分布式计算、虚拟化技术、网络存储等电力安全设备技术渐渐发展融合的一种新技术。身份认证技术包含基于 SAML 身份认证、基于 OAuth 的认证授权管理和基于 OpenID 的身份认证技术等。以 OpenID 身份认证为例，更新 OpenID 的传统方法，而且在适应原环境的基础上，在域内和域外实现电力用户访问的统一身份认证，其次根据新方法存在的漏洞，可以把动态口令功能增加到新的安全方法中[18]。

另外，边缘计算、云计算及互联技术的快速发展导致传统内外网边界模糊，企业无法通过建立传统的物理边界构筑安全基础设施，因此，提出了基于免疫的拟态防御和基于以身份认证为边界的零信任网络认证技术。

4.2.4　VPN 技术

VPN 表示虚拟的私有网络，在公共电力网络的作用下，把分布在不同地方的网络进行整合连接，在物理上称为虚拟子网，在数据信息传输时，确保其安全。VPN 技术需使用某些操作，如信息认证、访问控制及保密性等措施，这样可以保证传输的安全性。比较常见的 VPN 技术有密钥管理技术、访问控制技术等。在 VPN 技术中，在进行传输之前需要更改原始信息，即提前进行封装协议，对其加密并压缩，在对不同协议的数据包嵌套后，再传到电力网络，这样可以保证公共网络的公开透明。在数据信息进行处理传输时，该技术只能根据信源端、信宿端完成，而其他用户端无法识别该信息[19]。

4.2.5　量子通信技术

量子通信技术属于电力物联网中的网络层，是量子比特作为信息的载体传输数据信息的一种通信技术。它和传统技术的最大区别是利用基本力学和量子原理达到传输效果。量子通信技术和其他技术不同的是，其具有安全性高、传输效率高和超空间通信等特点。电力物联网量子通信通过量子信道的波分复用技术、城域网共纤技术等实现数据传输的安全性。这些技术和传统技术不同，其可以改变输出脉冲强度，保持很好的光强稳定性，提升通信网络的容量，扩展通信网络的速率，甚至随着环境的变化，光的偏振状态也会随着发生改变，不断改变通信系统的各种有效功能。量子通信技术的思路是在退相干效应低的情况下，还能保证量子态之间相对较远的相干传输[20-22]；量子保密通信技术协议中 BB84 协议最先被提出，如图 6 所示。

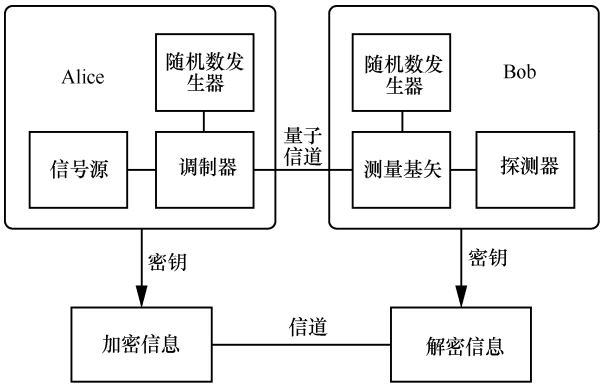

图 6　BB84 协议

4.3　应用及数据层安全关键技术

4.3.1　数据隐私防护技术

数据隐私防护技术主要分为数据存储防护、数据处理防护、数据共享防护。数据存储防护是把已有的数据通过拆分，进行加密后将数据上传到云端，在数据传输、存储发生意外，暴露关键信息时，由于技术的加密不会造成信息泄露；数据处理防护根据 Hadoop 的基本框架，运用对应的模式对其进行大量的分布式处理，这种方式基本可以兼容数据的基本特征，而且有成本低、容错性低等优点，最重要的是可以利用相关的资源。

数据共享防护对于共享的数据来说，将机密技术和水印技术结合，不但可以保证数据不会被监视窃取，还可以防止被篡改和伪造[23]。

4.3.2 加/解密技术

加/解密技术不仅可以通过改变文件内容达到保护文件安全的目的，而且与传统技术相比便捷性和安全性上有了突破和发展，特点是可以强制加密指定文件，可以不可见使用，而且在不妨碍内部使用的同时，使外部使用受阻。加/解密技术原理是对打开的文件进行监察操作，自动对其密文进行解密，对文件进行操作时，把明文加密加到介质中，确保打开的文件一直处于被保护的模式中，通过加密技术进行监控的电力系统可以在系统设备的不同方面进行展开。比较常见的基本程序是在用户模式下打开，电力用户程序没有访问内核的权利，要根据 API 对内核的代码进行访问，这样可以实现所有的最后操作都存储在文件中，达到保护信息的目的[24]。

4.3.3 病毒防范技术

在网络环境下，病毒传播途径多、扩散速度极快，而且危害性大，病毒变种多且速度快，有些病毒有极强的隐蔽性，很难彻底消灭，其目的性和针对性比其他传统病毒更强。病毒防范技术通过自身校验和文件长度等来对病毒的特征进行检测[25]。电力计算机设备和系统要经常利用杀毒软件进行清除，同时使用多种反病毒的软件，能够更加有效地应对病毒；要注意电力设备的防护，当发现有异常（如内存、磁盘有变化）时，需及时采取措施，使用户及时得到应对方法并进行处理，从而对外来的入侵起到抵制的作用。加强对网络的管理，不仅需要技术手段，也需要有效的管理机制，从意识上提高才能够更好地保障系统的安全。

4.3.4 区块链技术

区块链属于泛在电力物理网中的应用层。区块链可用作基础架构和分布式计算，能够有效针对并解决电力物联网各方面之前存在的安全不足，对电力物联网快速发展有重要的作用。泛在电力区块链安全性会遭受多种多样多方面的影响，为了解决这些问题，参考文献[26]提出泛在电力区块链的安全体系，如图 7 所示。

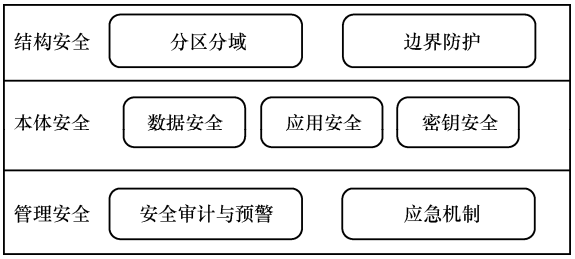

图 7 泛在电力区块链安全防护体系

其中，结构安全指的是电力物联网运用区块链技术后，根据业务的重要性、信息的开放程度和自身的保护程度等方面，在信息系统的边界设置对应的安全控制设备进行相应的隔离保护。而本体安全表示泛在电力区块链节点根据评估数据的重要程度，运用数据脱敏技术，针对相关数据库，利用其数据建立模型，定性地观测数据发生泄露的风险。管理安全会对异常情况进行审计，比如系统的资源、用户行为等，并且审计范围涉及区块链上的所有设备及时感知系统中的异常事件与整体安全态势，以便做出预警和风控措施[27]。

4.4 其他安全理论与方法

安全模型驱动防护法是由电网专家根据智能电网的发展和电力物联网的设定，Sridhar 等[28]初步建立了控制环安全模型，如图 8 所示，该系统根据控制环模型中所对应的传感器参数测量、信息采集、控制信息、数据计算和分析、物理设备测量和执行器执行这 6 个步骤所包含的安全问题、薄弱环节和响应漏洞进行了相应的识别和归类。还有些电力学者运用进行了简化的控制环模型，把其分为控制系统和物理系统两部分。通过该方法，实现对电力物联网安全的脆弱性评估和安全加固建设。

同时，随着信息数据安全事故的频发，各国大型电力公司对数据安全和用户隐私的妥协意识

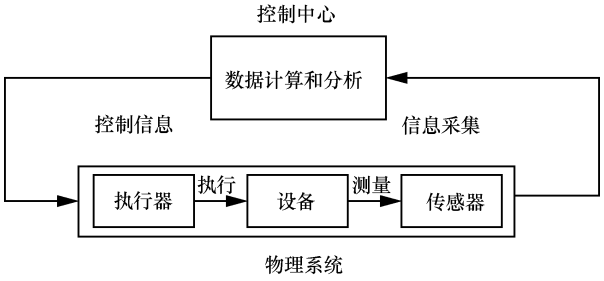

图 8　控制环模型

日益增强，对数据隐私和安全的重视已成为全球性的主要问题。为解决电力物联网中的“数据孤岛”问题，加强数据隐私和安全性，基于分布式的机器学习模型提出联邦学习这一技术，允许知识在不侵犯用户隐私的情况下共享。

5　结束语

电力物联网在未来几年会迎来空前的发展机会，但是电力安全问题始终是不可避免的重要问题。电力物联网在安全技术方面需要克服很多难题，如何建立物联网安全体系，架设安全基础设施，保证物联终端安全、移动和互联安全以及数据的安全都是当前要研究的热点问题。同时，研究典型物联场景下的攻击路径、漏洞分析及攻击机理，研究操作系统、物联计算节点等基础软硬件安全免疫关键技术及可信计算应用，研究面向物联网设备的嵌入式安全操作系统关键技术，研究基于区块链的多方信任交互关键技术等都是需要攻克的技术难题。未来新一轮电力体制改革，将从发电、输电、配电、售电等多方面推进。随着能源市场的发展，电力物联网的感知层、网络层、平台层、应用层将向主体多元化、竞争有序化的方向发展，安全技术防护的方法和技术创新将不断涌现。

参考文献：

[1] 张翼英. 电力物联网安全技术研究[M]. 北京: 科学出版社, 2016.
ZHANG Y Y. Research on security technology of power Internet of things [M]. Beijing: Science Press, 2016.

[2] 孟月, 田小梦. 国家电网 2021 年将初步建成电力物联网[J]. 通信世界, 2019(8): 34-35.
MENG Y, TIAN X M. State grid will be initially built in the electric internet of things in 2021[J]. Communications World, 2019(8): 34-35.

[3] 何英. 能源互联网背景下网络安全重要性凸显[N]. 中国能源报, 2017-01-02.
HE Y. The importance of network security in the context of energy Internet [N]. China Energy Journal, 2017-01-02.

[4] 乌克兰电力系统遭受攻击事件综合分析报告[EB]. 2016.
Comprehensive analysis report of attacks on Ukraine's power system [EB]. 2016.

[5] COLAK I, SAGIROGLU S, FULLI G, et al. A survey on the critical issues in smart grid technologies[J]. Renewable & Sustainable Energy Reviews, 2016(54): 396-405.

[6] 顾卓远, 汤涌, 孙华东, 等. 基于响应的电力系统安全稳定综合防御技术[J]. 中国电机工程学报, 2019(39): 1-10.
GU Z Y, TANG Y, SUN H D, et al. Security and stability comprehensive defense technology of power system based on response[J]. China Electrical Engineering Journal, 2019(39): 1-10.

[7] MRABET Z E, KAABOUCH N, GHAZI H E, et al. Cyber-security in smart grid: survey and challenges[J]. Computers & Electrical Engineering, 2018(67): 469-482.

[8] 李田, 苏盛, 杨洪明, 等. 电力信息物理系统的攻击行为与安全防护[J]. 电力系统自动化, 2017(22): 168-173.
LI T, SU S, YANG H M, et al. Aggressive behavior and security protection of power information physics system[J]. Automation of Electric Power Systems, 2017(22): 168-173.

[9] 胡贺军, 孙方楠, 王迎生. 能源互联网信息安全架构研究[J]. 通讯世界, 2017(17): 31-32.
HU H J, SUN F N, WANG Y S. Research on information security architecture of energy internet [J]. Communications World, 2017(17): 31-32.

[10] JAGDEEP S. Syscoin: a peer-to-peer electronic cash system with blockchain-based services for e-business[C]//Proceedings of International Conference on Computer Communication and Networks (ICCCN). [S.l.: s.n.], 2017(26): 1-6.

[11] 卢星儒. 网站安全评估技术与漏洞挖掘技术[J]. 计算机产品与流通, 2019(1): 44.
LU X R. Website security assessment technology and vulnerability mining technology[J]. Computer Products and Circulation, 2019(1): 44.

[12] 付梦琳, 吴礼发, 洪征, 等. 智能合约安全漏洞挖掘技术研究[J]. 计算机应用, 2019, 9(7): 1959-1966.
FU M L, WU L F, HONG Z, et al. Research on the mining technology of smart contract security vulnerabilities[J]. Computer Applications, 2019, 39(7): 1959-1966.

[13] 王朱劳. 入侵检测技术在网络安全中的应用分析[J]. 数字技术与应用, 2019, 37(1): 209-210.
WANG Z L. Application analysis of intrusion detection technology in network security[J]. Digital Technology and Application, 2019, 37(1): 209-210.

[14] 谭慧婷, 唐朝京. 移动目标防御中动态网络技术现状、性能

和发展方向探讨[J]. 网络安全技术与应用, 2017(6): 22-23.
TAN H T, TANG C J. Discussion on the status quo, performance and development direction of dynamic network technology in mobile target defense[J]. Network Security Technology & Application, 2017(6): 22-23.

[15] 罗兴国, 仝青, 张铮. 拟态防御技术[J]. 中国工程科学, 2016, 18(6): 69-73.
LUO X G, TONG Q, ZHANG Z. Mimetic defense technology[J]. China Engineering Science, 2016, 18(6): 69-73.

[16] 王明明, 岳文雷, 杨振乾. 网络安全中的防火墙技术应用分析[J]. 网络安全技术与应用, 2019(3): 21, 23.
WANG M M, YUE W L, YANG Z Q. Application analysis of firewall technology in network security[J]. Network Security Technology and Application, 2019(3): 21, 23.

[17] 王诗琦. 网络安全隔离与信息交换技术的系统分析[J]. 信息通信, 2012(3): 211-212.
WANG S Q. System analysis of network security isolation and information exchange technology [J]. Information & Communications, 2012(3): 211-212

[18] 周长春, 田晓丽, 张宁, 等. 云计算中身份认证技术研究[J]. 计算机科学,2016, 43(S1): 339-341, 369.
ZHOU C C, TIAN X L, ZHANG N, et al. Research on Identity Authentication Technology in Cloud Computing[J]. Computer Science, 2016, 43(S1): 339-341, 369.

[19] 杨鑫. 网络安全技术中VPN技术的应用[J]. 电子技术与软件工程, 2019(3): 208.
YANG X. Application of VPN technology in network security technology[J]. Electronic Technology and Software Engineering, 2019(3): 208.

[20] 王磊, 赵广怀, 范晓楠, 等. 量子保密通信在电网业务应用的方案研究与设计[J]. 电力信息与通信技术, 2018, 16(3): 34-38.
WANG L, ZHAO G H, FAN X N, et al. Research and design on the application of quantum secure communication in power grid business[J]. Electric Power Information and Communication Technology, 2018, 16(3): 34-38.

[21] 周德旺, 皇安伟. 量子通信助力信息安全保密[J]. 保密工作, 2018(8): 6-8.
ZHOU D W, HUANG A W. Quantum communi- cation power information security and confiden- tiality[J]. Security Work, 2018(8): 6-8.

[22] 李文华, 袁夕征, 熊晓然. 量子保密通信关键技术及组网应用探讨[J]. 邮电设计技术, 2019(2): 69-75.
LI W H, YUAN X Z, XIONG X R. Key technology and network application of quantum secure communication[J]. Posts and Telecommunications Design Technology, 2019(2): 69-75.

[23] 肖洁, 袁嵩, 谭天. 大数据时代数据隐私安全研究[J]. 计算机技术与发展, 2016, 26(5): 91-94.
XIAO J, YUAN S, TAN T. Research on Data Privacy Security in the Big Data Era[J]. Computer Technology and Development, 2016, 26(5): 91-94.

[24] 左晓军, 丁斌, 陈泽.透明加解密技术在企业数据保护中的研究与应用[J]. 河北电力技术, 2018, 37(3): 26-28, 54.
ZUO X J, DING B, CHEN Z. Research and application of transparent encryption and decryption technology in enterprise data protection[J]. Hebei Electric Power Technology, 2018, 37(3): 26-28, 54.

[25] 王凌. 计算机病毒的感染原理及防范技术研究[J]. 中国管理信息化, 2013, 16(1): 79-80.
WANG L. Research on computer virus infection principle and prevention technology[J]. China Management Information Technology, 2013, 16(1): 79-80.

[26] 丁伟, 王国成, 许爱东, 等. 能源区块链的关键技术及信息安全问题研究[J]. 中国电机工程学报, 2018, 38(4): 1026-1034, 1279.
DING W, WANG G C, XU A D, et al. Research on key technologies and information security of energy blockchain [J]. Chinese Journal of Electrical Engineering, 2018, 38(4): 1026-1034, 1279.

[27] 郭鹤旋, 鲁斌. 基于交叉区块链的能源互联网信息物理安全防御框架[J]. 电脑知识与技术, 2018, 14(23): 7-9.
GUO H X, LU B. Energy Internet information physical security defense framework based on cross blockchain [J]. Computer Knowledge and Technology, 2018, 14(23): 7-9.

[28] 栾文鹏, 刘永磊, 王鹏, 等. 基于可信平台模块的能源互联网新型统一安全架构[J]. 吉林大学学报(工学版), 2017, 47(6): 1933-1938.
LUAN W P, LIU Y L, WANG P, et al. New unified security architecture for energy internet based on trusted platform module[J]. Journal of Jilin University (Engineering and Technology Edition), 2017, 47(6): 1933-1938.

[作者简介]

张翼英（1973− ），男，博士后，天津市高校学科领军人才，天津科技大学海河学者特聘教授，主要研究方向为物联网及其安全、安全密钥、智能电网。

周保先（1998− ），男，天津科技大学人工智能学院硕士生，主要研究方向为物联网、信息安全、知识图谱等。

庞浩渊（1995− ），男，北京遥测技术研究所助理工程师，主要研究方向为信息安全、遥测传输设备等。

曹津平（1977− ），女，博士，国家电网有限公司信息通信分公司高级工程师，主要研究方向为电力系统自动化。

张桐嘉（2001− ），女，北京工业大学在读，主要研究方向为信息安全。