基于可信计算的信息安全防护技术研究

李德智[1]　柳　来[2]　薛思威[1]
1. 华信咨询设计研究院有限公司　浙江　杭州　310000
2. 浙江华云电力工程设计咨询有限公司　浙江　杭州　310000

摘　要：随着信息技术的迅猛发展，信息安全问题日益凸显。可信计算，作为一种新型的安全防护技术，以其独特的理念和技术手段，为信息安全领域带来了新的解决方案。本文深入探讨了可信计算的理论基础、技术特点，详细分析了其在提升系统整体安全性、硬件级别的信任建立以及强化身份验证和授权机制等信息安全防护方面的深入应用。同时，也探讨了可信计算技术的发展趋势与面临的挑战，旨在为构建更加安全可靠的信息系统提供全面的理论支持和技术指导。

关键词：可信计算；信息安全；防护技术；硬件信任；安全策略

引言

在信息化时代，信息安全问题已成为社会关注的焦点。随着网络攻击手段的日益复杂和多样化，传统的安全防护手段虽然在一定程度上能够保护信息系统的安全，但在面对一些高级威胁时仍显得力不从心。可信计算的提出，为信息安全领域注入了新的活力，其核心理念是通过在硬件和软件层面建立协同工作的信任基础，确保计算设备和数据的安全性。

1 可信计算的理论基础

可信计算是一种基于硬件信任的安全计算技术，其核心思想是通过建立可信环境，确保计算设备和数据的安全性。它依赖于特殊的硬件设备，如可信执行环境（TEE）和可信平台模块（TPM），以及相应的软件支持。可信计算的原理是通过建立可信链来保证数据的安全性，该链由一系列可信计算基础组件构成，通过相互验证和授权，形成一个可信的计算环境。

1.1 关键功能

（1）启动过程的可信性验证：在系统启动时，通过验证启动代码的完整性和真实性，确保系统从最初的引导阶段就处于安全状态。这可以有效防止恶意代码的注入和篡改。（2）可信传输：在数据传输过程中，可信计算技术通过加密和身份验证机制，确保数据在传输过程中的机密性、完整性和真实性。这对于保护敏感信息和防止数据泄露至关重要。（3）可信运行：在系统运行过程中，可信计算技术通过实时监控和验证应用程序的行为，确保其按照预定的安全策略执行。这可以防止恶意软件或未经授权的操作对系统造成损害。（4）可信存储：通过加密和访问控制机制，可信计算技术确保存储在系统中的数据只能被授权的用户或应用程序访问。这大大增强了数据的保密性和安全性。

1.2 技术特点分析

1.2.1 硬件与软件的深度融合

可信计算技术的核心优势在于其实现了硬件与软件的深度融合。这一融合并非简单的技术叠加，而是在系统架构的每一层面都进行了安全性设计与考量。硬件的安全特性，如防篡改、防窃取等，为整个系统提供了坚实的基石。通过与软件系统的紧密结合，这些硬件特性得以最大化利用，形成了一个统一、协调的安全防护体系。这种深度融合不仅提升了系统的整体安全性，更使得对潜在威胁的响应速度和准确性大大提高[1]。此外，硬件与软件的共同协作还意味着系统能够更高效地执行安全策略，及时识别并隔离潜在风险，为用户提供更加安全、可靠的计算环境。这种深度融合代表了信息安全技术的新方向，是可信计算技术的重要特点之一。

1.2.2 主动防御机制

可信计算技术所展现的主动防御机制，是其与传统信息安全技术的重要区别。传统的安全防护多采取被动应对方式，即在威胁出现后进行应对，这种方式往往存在响应延迟，且难以全面预防未知威胁。而可信计算技术则通过实时监控和验证系统的行为，实现了对潜在威胁的主动识别和预防。这种机制可以实时分析系统活动，检测异常行为，及时在攻击发生前发现并阻止潜在的威胁，大大提高了系统的安全防护能力。这种主动防御不仅限于已知威胁的防御，更能通过行为分析预测并防范未知威胁，为信息系统提供了更加全面的保护。这种前瞻性的安全策略，确保了系统在面临各种安全挑战时，都能迅速、有效地做出响应。

1.2.3 全面的安全防护

可信计算技术为信息系统提供了前所未有的全面安全防护。从系统启动的初始阶段到数据传输、软件运行，再到数据存储，每一个环节都受到了精心的保护。在系统启动时，通过验证机制的引入，确保了系统的初始状态是安全和未被篡改的。在数据传输过程中，利用加密和身份验证技术，保障了数据的机密性和完整性，防止了数据在传输过程中被窃取或篡改。在软件运行时，通过实时监控应用程序的行为，防止了恶意软件的执行和未授权的操作。而在数据存储时，又通过加密和访问控制，确保了数据的保密性和安全性。这种从始至终、无死角的安全防护，大大提升了信息系统的整体安全性，使得用户能够在一个更加安全、可靠的环境中处理和使用数据。

2 可信计算技术在信息安全防护中的深入应用

2.1 提升系统的整体安全性

可信计算技术在信息安全领域的应用，显著提升了系统的整体安全性。其核心理念在于从系统启动的最初阶段就开始构建一个坚不可摧的信任链。这一信任链的构建始于系统的加电自检，延续至操作系统的加载，最终覆盖到用户应用程序的运行。在这个过程中，每一个环节都经过了严格的身份验证和完整性检查，确保了系统从始至终都处于一个安全、可信的状态。具体而言，当系统启动时，可信计算技术会首先对系统的基本输入输出系统进行验证，确保其未被篡改且来源可靠。随后，在操作系统加载阶段，该技术会检查操作系统的核心文件和关键组件，验证其完整性和真实性，从而防止了恶意代码的注入和系统的非法篡改。当用户应用程序运行时，可信计算技术会持续监控应用程序的行为，确保其按照预定的安全策略执行，及时发现并阻止任何异常或恶意行为。更为值得一提的是，可信计算技术并非孤立存在，它可以与现有的安全防护措施，如防火墙、入侵检测系统（IDS）等，进行完美的结合。这种结合形成了一个多层次、立体化的安全防护体系。在这个体系中，防火墙作为第一道防线，负责过滤和阻止来自外部的非法访问和攻击；入侵检测系统则负责实时监控系统的网络传输，及时发现并响应任何可疑的网络活动；而可信计算技术则从系统内部出发，确保系统的每一个组件和行为都是可信的[2]。这三者相辅相成，共同构成了一个坚不可摧的安全堡垒。

2.2 实现硬件级别的信任

可信计算技术通过引入特殊的硬件设备，如TPM（受信任的平台模块）和TEE（可信执行环境），为信息系统带来了硬件级别的信任。这些硬件设备不仅具备防篡改、防窃取等出色的安全特性，更能确保存储在其中的密钥、证书以及其他敏感信息得到严密保护。TPM，作为一种专用的微处理器，被设计为存储在计算机主板上的安全芯片。它提供了各种安全功能，包括加密、解密、数字签名等，从而确保了数据的机密性和完整性。更重要的是，TPM能够安全地存储密钥和证书，为身份验证和数据加密提供了坚实的硬件基础。这意味着，即使系统的其它部分受到攻击或篡改，TPM内的信息仍然能够保持安全，为整个系统提供了一个可信赖的根基。与TPM相辅相成的是TEE，即可信执行环境。TEE为应用程序提供了一个隔离的、安全的执行空间，确保应用程序在其内部运行时，不会受到外部恶意软件或攻击的干扰。这种环境特别适合处理敏感数据和执行关键操作，如移动支付、身份验证等。在TEE内部运行的应用程序，其代码和数据都得到了严格的保护，从而大大提高了系统的安全性。在硬件信任的基础上，我们可以进一步构建更加安全可靠的软件环境。例如，利用TPM的加密功能，我们可以确保操作系统的核心文件在传输和存储过程中不被篡改，从而保证操作系统的完整性和真实性。同时，通过TEE提供的安全执行环境，我们可以确保关键应用程序在运行时不会受到任何形式的干扰或篡改，从而大大增强了系统的稳定性和安全性。

2.3 强化身份验证和授权机制

在信息安全领域，身份验证和授权是确保系统安全的重要基石。可信计算技术在这方面发挥了关键作用，它通过构建强大的身份验证和授权机制，为系统提供了坚实的保护。身份验证是确认用户身份的过程，它是保护系统不被未授权访问的第一道防线。可信计算技术利用TPM（受信任的平台模块）的加密和签名功能，实现了对用户身份的强有力验证。TPM模块内部存储了用户的身份信息和相应的密钥，当用户尝试访问系统时，系统会要求用户提供身份验证信息。通过TPM的加密功能，系统可以验证用户提供的身份信息是否与TPM内部存储的信息匹配。这种基于硬件的身份验证方式，大大提高了身份验证的可靠性和安全性。除了身份验证，授权机制也是保护系统安全的重要手段。授权是指根据用户的身份和权限，控制其对系统资源的访问。可信计算技术通过细粒度的访问控制策略，实现了对用户访问权限的精确控制。这意味着，不同的用户根据其角色和职责，被赋予不同的访问权限。例如，管理员用户可能拥有对系统的完全控制权，而普通用户则只能访问其被授权的资源。细粒度的访问控制策略是通过一系列规则和条件来实现的。这些规则可以根据用户的身份、时间、

地点等多种因素来定义[3]。例如，可以设定只有特定用户在特定时间段内才能访问某个资源，或者只有在用户位于特定地理位置时才能访问系统。这种灵活的授权机制，不仅提高了系统的安全性，还满足了不同用户的需求和场景。

3 可信计算技术的发展与挑战

3.1 发展

随着科技的飞速进步和数字化时代的深入发展，可信计算技术也在持续演进和完善。它不再是孤立存在的安全技术，而是逐渐与云计算、大数据、人工智能等前沿技术紧密结合，共同构建了一个更加稳固、高效的信息安全防护体系。（1）在云计算领域，可信计算技术发挥着举足轻重的作用。云计算作为一种按需提供服务的模式，具有弹性可扩展、资源池化等特点，但同时也面临着虚拟机安全、数据隔离等多方面的挑战。可信计算技术的引入，为云计算环境提供了强有力的安全保障。它能够在虚拟机启动时进行身份验证和完整性检查，确保虚拟机的安全性和隔离性，有效防止了潜在的攻击和数据泄露风险。（2）在大数据处理过程中，可信计算技术同样展现出其独特的优势。大数据的采集、存储、处理和分析过程中，数据的隐私性和完整性是至关重要的。可信计算技术通过加密、签名等手段，保护了数据的机密性和完整性，防止了数据在传输和存储过程中被窃取或篡改。同时，结合访问控制和审计机制，可信计算技术还能够确保只有授权的用户才能访问和处理数据，从而有效保护了大数据的安全。（3）此外，在人工智能应用中，可信计算技术也发挥着不可或缺的作用。随着人工智能技术的广泛应用，恶意攻击和模型篡改等威胁也日益凸显。可信计算技术通过确保模型的完整性和真实性，防止了恶意攻击者对模型的篡改和利用。同时，结合人工智能的自身学习能力，可信计算技术还能够实现自适应的安全防护，及时发现并应对潜在的安全威胁。

3.2 挑战

然而，可信计算技术的发展也面临着一些挑战。首先，标准化问题是一个亟待解决的问题。目前，可信计算技术尚未形成统一的标准和规范，这在一定程度上限制了其推广和应用。其次，兼容性问题也不容忽视。由于可信计算技术涉及到硬件和软件的深度融合，因此需要解决不同厂商、不同平台之间的兼容性问题[4]。最后，成本问题也是制约可信计算技术发展的一个重要因素。由于可信计算技术需要特殊的硬件设备和软件支持，因此其成本相对较高，这可能会限制其在一些场景中的应用。

3.3 建议

为了有效克服可信计算技术发展中所面临的挑战，我们提出以下具体建议：（1）应加强国际合作和交流，推动全球范围内的可信计算技术标准化工作。通过与国际组织和相关行业的紧密合作，共同制定和完善可信计算技术的规范和标准，确保其互操作性和广泛应用。（2）必须加大研发投入，鼓励技术创新，以降低可信计算技术的实施成本并提升其性能。这包括优化算法、提高硬件效率、简化部署流程等多方面的努力，从而使其更加适用于各种规模和需求的企业。（3）用户教育和培训也至关重要。通过举办研讨会、培训班等形式，向用户普及可信计算技术的基本知识和应用前景，提高其对该技术的认知度和接受度。这将有助于推动可信计算技术的普及和应用，共同构建一个更加安全可靠的数字环境。

结语

可信计算技术作为一种新型的信息安全防护手段，以其独特的理念和技术手段为信息安全领域带来了新的解决方案。通过建立硬件和软件协同工作的信任基础，并利用强大的身份验证、授权机制以及全面的安全防护措施等手段，可信计算技术能够全面提升信息系统的安全性、可信度和可靠性。未来随着技术的不断进步和应用场景的拓展以及我们对可信计算技术研究的不断深入和完善，它将在信息安全领域发挥更加重要的作用并为我们提供更加安全、可靠的计算环境。

参考文献

[1]李志强.可信计算技术在网络信息安全中的应用[J].科技风,2023(04):44-46.

[2]曹宁.可信计算技术在网络信息安全中的应用[J].信息技术,2021(08):150-155.

[3]冯德尹,吴明念.可信计算技术在网络信息安全中的应用与研究[J].电脑知识与技术,2021,17(13):53-54.

[4]冯登国,刘敬彬,秦宇,冯伟.创新发展中的可信计算理论与技术[J].中国科学:信息科学,2020,50(08):1127-1147.