基于计算机大数据的信息安全处理技术

巫　健
武昌职业学院　湖北武汉　430200

摘　要：在当前数字化时代，计算机大数据的应用已经深入到各个领域，为企业和组织提供了巨大的商机和增长机会。然而，随着大数据的快速增长，信息安全问题也日益突出，且大数据中包含着大量的敏感信息，如个人身份、财务数据等，一旦泄露或被恶意利用，将给个人和组织带来巨大的风险和损失。因此，为了有效保护大数据的安全，提高数据的可信度和完整性，探究计算机大数据的信息安全处理技术显得尤为重要。为此，本文主要对计算机大数据的信息安全处理技术应用进行探究，进而为提升计算机大数据信息安全处理的效果提供参考借鉴。

关键词：计算机；大数据；信息安全；处理技术；应用分析

前言：

随着大数据技术的快速发展，大数据的应用范围越来越广泛，涉及的数据量和复杂度也越来越大。然而，随着数据规模的增加，信息安全问题也变得更加重要和复杂。大数据中的信息安全处理涉及到保护数据的机密性、完整性和可用性，以及防止恶意攻击和数据泄露。由于大数据的特点，传统的信息安全处理方法已经不再适用，需要研究和探索新的技术来应对这些挑战。通过对计算机大数据的信息安全处理技术的探究，可以更好地保护大数据的安全和隐私，为大数据的应用提供可靠的保障，并且也可以为相关研究和实践提供参考和指导。

一、计算机大数据的信息安全处理技术应用的重要性

首先，大数据中包含大量的个人敏感信息，如个人身份、财务数据等，技术人员选择合适的信息安全处理技术可以有效保护这些信息，防止被恶意利用。其次，大数据存储了企业和组织的重要数据，如商业机密和用户信息，信息安全处理技术可以防止黑客攻击和数据泄露事件，保护企业和用户免受损失。此外，大数据的价值在于其准确性和可信度，信息安全处理技术可以确保数据的完整性，防止数据被篡改或伪造，保证数据的可靠性和可信度。同时，随着数据保护和隐私法律的加强，组织需要遵守相关的合规性要求，信息安全处理技术可以帮助组织满足法律要求，降低违规风险。最后，大数据的分析和共享对于组织和社会的决策和创新至关重要，信息安全处理技术可以提供可控的数据共享和分析方式，保护数据的隐私和安全。

二、计算机大数据的信息安全处理技术应用中存在的问题

1.处理速度与大数据量

计算机大数据通常包含海量的信息，对其进行安全处理需要较高的计算和处理能力。然而，信息安全处理技术在处理大数据时可能会面临处理速度慢、响应时间长的问题，从而影响系统的性能和效率。

2.复杂的数据格式和结构

目前，大数据通常涉及多种数据格式和结构，如结构化数据、半结构化数据和非结构化数据等。信息安全处理技术需要适应不同的数据格式和结构，保证在不同类型的数据中实现安全处理的一致性和有效性。

3.隐私保护与数据分析需求的平衡

在进行大数据的信息安全处理时，需要平衡隐私保护和数据分析需求之间的关系。一方面，隐私保护需要限制数据的访问和使用，以保护用户的个人隐私；另一方面，数据分析需要充分利用数据来挖掘有用的信息。如何在保护隐私的前提下，实现对数据的有效分析和利用，是一个需要解决的问题。

4.技术更新和漏洞修复

计算机大数据的信息安全处理技术需要与不断发展的技术和威胁保持同步。随着技术的进步，新的安全漏洞和威胁可能会出现，对现有的信息安全处理技术提出新的挑战。因此，技术人员及时更新和修复技术漏洞，保持信息安全处理技术的有效性和可靠性非常重要[1]。

三、计算机大数据的信息安全处理技术的应用分析

1.数据保护与加密

一是数据加密：数据加密是一种常用的数据保护技术，通过对数据进行加密，将其转化为一串看似无意义的字符，只有具有正确密钥的人才能解密并还原成原始数据。同时，加密使得被窃取的数据对攻击者来说毫无意义，从而保护敏感信息的机密性。二是数据脱敏：数

据脱敏是对敏感数据进行处理，以保护隐私和遵循数据保护法规，且数据脱敏技术可以通过替换、删除、屏蔽等方式，对敏感数据的部分信息进行处理，使得敏感信息无法被识别出来，这样即能保护数据的机密性，又能保留数据的完整性和可用性。三是密钥管理：在数据加密中，密钥是保证数据安全的关键，密钥管理技术涉及到密钥的生成、分发、存储和更新等方面的管理。合理的密钥管理能够保证密钥的安全性，防止密钥泄露和滥用，从而保护加密数据的安全。四是访问控制与权限管理：数据保护还需要通过访问控制和权限管理来限制对敏感数据的访问和使用，访问控制和权限管理技术可以对用户进行身份验证、授权和审计，确保只有合法的用户可以访问和使用敏感数据，同时可以对数据的访问行为进行监控和审计，及时发现和阻止未授权的访问。

2.异常检测与威胁识别

首先，异常检测：异常检测是一种通过对数据进行统计分析和建模，识别出与正常模式不符的数据点或事件的技术。在大数据环境下，技术人员可以利用机器学习、统计分析和数据挖掘等技术，对大规模的数据进行分析，发现其中的异常行为。例如，通过对网络流量进行监测，可以检测到网络入侵和恶意攻击等异常行为。其次，威胁识别：威胁识别是指通过对大数据中的信息进行分析和检测，发现并识别出潜在的安全威胁。它可以通过建立威胁情报库，对已知的威胁进行识别和匹配，也可以通过行为分析和模式识别等技术，对未知的威胁进行检测和识别。威胁识别可以帮助及早发现和应对潜在的攻击和安全威胁。同时，实时监测与响应：在大数据环境下，异常检测与威胁识别需要具备实时性，能够对大规模的数据进行实时监测和响应。技术人员通过利用分布式计算和实时数据处理技术，可以实时地对大数据进行监测，及时发现和应对异常行为和威胁。最后，整合其他安全技术：异常检测与威胁识别需要与其他安全技术进行整合，以提高安全防护的能力。例如，可以将异常检测与防火墙、入侵检测系统（IDS）等安全设备进行集成，实现多层次的安全防护和威胁识别[2]。

3.数据溯源与追踪

一是数据溯源：数据溯源是指通过对大数据中的数据流动进行跟踪和记录，确定数据的来源和流向的过程，技术人员通过建立数据流管控系统，可以对数据的生成、传输、存储和访问等环节进行监测和记录，以实现数据的全程可追溯。数据溯源可以帮助快速定位数据泄露和滥用的源头，追查责任和监督数据的合规使用。二是数据追踪：数据追踪是指通过对大数据中的数据流动和操作进行跟踪和监测，实时追踪数据的流向和使用情况。技术人员通过对数据的操作日志、访问记录和行为分析等技术，可以实现对数据的实时追踪和监控。数据追踪可以帮助及时发现数据滥用、窃取和篡改等违规行为，提高数据安全和隐私保护的能力。三是实时告警与响应：数据溯源与追踪需要具备实时性，能够对大规模的数据进行实时的监测和响应。通过建立实时告警系统，对异常数据流动和操作进行监测，一旦发现异常情况就能及时发出告警信号，并采取相应的响应措施。实时告警与响应能够帮助快速发现和应对数据泄露、滥用和违规行为。四是隐私保护和合规性：数据溯源与追踪需要与隐私保护和合规性要求相结合。在数据追踪过程中，技术人员需要采取措施保护敏感数据的隐私，防止个人隐私信息被滥用和泄露。同时，也需要确保数据追踪的合规性，遵守相关法律法规和隐私保护政策[3]。

4.安全合规与审计

首先，安全合规监测：安全合规监测是指通过对大数据系统的安全策略、访问控制、数据加密等安全机制进行监测和评估，确保系统的合规性。通过实时监测和分析系统的安全状态，可以及时发现和防止安全漏洞、异常行为和攻击行为，确保系统的安全合规性，遵守相关的法律法规和行业标准。其次，安全审计：安全审计是指对大数据系统和数据操作进行日志记录和审计，以追踪和监测数据的使用和操作情况。通过对系统的操作日志、访问记录和行为审计等手段，可以实现对数据的全程监控和审计。安全审计可以帮助发现数据滥用、窃取和篡改等违规行为，保护数据的安全和隐私。同时，合规性报告：合规性报告是指对大数据系统和数据操作进行定期的合规性评估和报告，以证明系统和数据的合规性。通过收集和分析系统的安全日志和操作记录，可以生成合规性报告，包括系统安全状态、访问控制、数据保护和隐私保护等方面的评估结果。合规性报告可以作为评估和监督数据安全的依据，帮助企业和组织确保数据安全和合规性。此外，安全合规策略：安全合规与审计需要建立相应的安全合规策略，包括安全规范、权限管理、数据加密和隐私保护等方面的要求。通过制定和执行安全合规策略，可以确保大数据系统和数据操作的安全性和合规性[4]。

5.预测与预警

一是威胁预测：技术人员通过对大数据系统中的安

全事件、攻击行为和异常行为进行分析和建模，可以预测出潜在的安全威胁。且通过利用机器学习、数据挖掘和统计分析等技术，可以发现并识别出与安全威胁相关的模式和规律。通过对这些模式和规律的分析和预测，可以提前预警并采取相应的防护措施，以避免安全事件的发生。二是异常检测：技术人员通过对大数据系统中的行为数据进行分析，可以发现异常行为和异常事件。通过建立基线模型和行为特征模型，可以识别出与正常行为不符的异常行为，且通过对这些异常行为的检测和分析，可以提前预警并采取相应的措施，以防止安全事件的发生或扩大。三是实时监测：技术人员通过对大数据系统的实时监测，可以及时发现和响应安全事件，且通过对系统的实时数据流进行分析和处理，可以实时监测系统中的网络流量、访问日志和异常行为等。通过实时监测，可以及时发现并预警系统中的安全威胁，并采取相应的应对措施，以保护系统和数据的安全。四是智能预警：通过结合大数据处理和人工智能技术，可以实现智能化的预警系统。通过对大数据系统中的安全事件和威胁进行实时分析和学习，可以建立智能化的预警模型。通过这些模型，可以自动识别和预测出潜在的安全威胁，并发出相应的预警通知。智能预警系统可以大大提高安全事件的检测和响应效率，帮助企业和组织更好地保护系统和数据的安全[5]。

四、结论

综上所述，随着数据量的增加，处理速度和效率成为关键问题，且隐私保护和数据完整性验证仍然是难题，需要进一步研究和改进。同时，新兴的技术和攻击手段也对信息安全带来了新的威胁，技术人员需要继续深入研究和探索计算机大数据的信息安全处理技术，这包括改进现有技术，开发新的安全算法和协议，以及加强对恶意攻击的检测和预防。同时，还需要加强跨学科的合作，整合计算机科学、数学、统计学等领域的知识，共同推动信息安全处理技术的发展。通过不断的探索和创新，可以为大数据的安全和隐私保护提供有效的解决方案，推动大数据的可持续发展。

参考文献：

[1]王伟.基于计算机大数据的信息安全处理技术分析[J].网络安全和信息化，2022（08）：138-140.

[2]张冠兰，谢小刚.基于计算机大数据的信息安全处理技术分析[J].网络安全技术与应用，2022（05）：75-76.

[3]尹海翔.基于大数据的计算机信息安全处理技术研究[J].电子技术与软件工程，2022（09）：17-20.

[4]刘云，吴宗显.计算机大数据的信息安全处理技术分析[J].数字通信世界，2022（03）：173-175.

[5]陈荣.基于计算机大数据的信息安全处理技术[J].中国新通信，2021，23（21）：136-137.