大数据与云计算背景下的信息安全技术

张达超
中航西飞 陕西 西安 710089

摘 要：本文就大数据与云计算的背景下的信息安全技术进行了探讨，介绍并分析了当前信息安全的挑战与背景，提出了利用人工智能技术来提高云数据的安全性的措施，同时建议建立完善的信息安全技术管理机制来预防各种安全事件的发生。

关键词：大数据；云计算；信息安全技术

引言：随着大数据和云计算技术的迅速发展，数据量和流量的增长使得信息安全问题越来越受到关注。在大数据和云计算背景下，信息安全技术不仅需要满足传统的数据安全防护能力，还需要具备大规模数据处理和随时响应的能力。因此，建立完善的信息安全技术管理机制，提出并应用高新技术，以确保数据在传输、存储和应用中的安全，提高企业和公众对信息安全的信任是当前亟需的工作。

1 云计算与大数据的内涵分析

云计算是一种分布式计算模型，它将大量的计算资源（包括存储、计算、网络等）进行集成和整合，通过互联网等方式向用户提供高效、便捷、灵活的计算服务。云计算的核心思想是将用户所需的计算资源汇聚起来，共享和管理，以强大的计算能力和可靠的存储服务为用户带来卓越的体验感受。与此同时，云计算也能够为企业和组织带来更高效的业务管理和信息共享服务。

大数据是一种利用先进的数据处理和分析技术处理海量数据的方法。它的出现和发展源于互联网时代所带来的数据爆炸式增长，传统信息处理技术难以胜任海量数据管理和分析任务。大数据的涵义包括数据管理、数据分析、数据检索、数据挖掘等方面，对于企业、政府和组织等机构的决策制定和业务规划有着至关重要的作用[1]。同时，大数据也为新型产业的发展带来了无限可能性，如智慧城市、智慧医疗、智慧交通等。

总体来说，云计算和大数据是紧密关联的，云计算提供了对大数据的处理和分析的基础设施和支持，大数据则为云计算提供了新业务的发展需求和新应用的推动力。云计算和大数据的结合，为人们带来了更加便捷、高效和智能的信息化服务，不仅使得信息革命不断向前推进，而且也将推动人类社会的进步和发展。

2 大数据与云计算下的信息安全技术

2.1 数据加密技术

在当前大数据和云计算的背景下，数据加密技术的重要性日益凸显。随着数十亿的互联网用户和不断增长的数据存储需求，数据安全已成为各大企业和机构关注的焦点。数据加密技术作为一种基础保障技术，已经成为了关键信息的保护必备技术。

数据加密技术是一种将明文数据通过密码算法变换成密文的技术。在数据传输和存储过程中，只有拥有相应密钥的个人才能够解密数据，保证了信息的机密性和安全性。在大数据和云计算环境下，数据加密技术的应用更加广泛和复杂。主要原因是这些模型涉及到的数据和程序可能来自许多不同机构和终端，所以数据加密需要在数据传输、数据存储和数据处理的各个密码算法中实现。

在数据传输过程中，人们通常使用SSL等协议进行加密。SSL属于基于传输层协议的数据加密技术，通过SSL协议可以确保数据在传输过程中不被篡改，确保数据的机密性和完整性。在数据存储方面，人们使用基于数据文件的加密技术，可以将数据加密后存储到云存储中。基于数据文件的加密技术通过数据加密形式保证安全性，同时也让云管理人员无法访问到文件内容[2]。在数据处理环节，人们采用基于计算的数据加密技术。这种技术更加智能化、灵活化，它把计算任务分配到多条MDT路和加密引擎中，采用分散式加密技术，从而达到充分利用资源的目的。

虽然数据加密技术能够对数据的安全性提供充分的保障，但是仍存在多重风险和挑战。例如，一些恶意的黑客、间谍、软件病毒可以在实施数据加密技术之前截获数据，将信息泄露给其他人。因此，加密技术必须具备高度的安全性，不能出现任何漏洞。此外，顶级密码算法技术的开发和维护具有较高的成本，需要大量人力、物力和财力的支持。

2.2 内容感知加密技术

在大数据和云计算环境下，内容感知加密技术成为了数据安全保障的重要手段。传统的加密算法可能会因为随机加密过程中的信息损失，导致加密后的密文质量变差，容易被人攻破。而内容感知加密技术通过对加密前数据进行分析，实现对数据的更加准确和高效的加密保护。内容感知加密技术主要有以下三个关键步骤：

（1）内容分析和特征提取：通过聚类、分类以及特征提取等技术，对传入的数据进行分析和识别，将数据进行划分，将数据特征提取出来并生成适合的加密策略。

（2）加密算法设计：基于上一步分析结果，针对不同的数据类型和特征，设计出不同的加密算法。这些算法能够针对不同的数据特征进行不同的加密操作，从而保障加密效果和性能。

（3）加密处理：使用设计好的加密算法对数据进行加密处理。同时，由于加密算法是根据数据的特征来定制的，因此可以根据不同的数据特征将加密策略进行优化和优化，从而保证加密的准确性和高效性。

3 大数据与云计算信息安全存在的问题

3.1 相关人员缺乏信息安全意识

大数据和云计算是当今信息技术领域的两个热门话题，它们的出现和发展极大地推动了社会的信息化进程，为企业和用户提供了更加便捷和高效的信息化服务。然而，大数据和云计算发展中的另一面是，涌现出很多涉及到信息安全的问题。其中，关键问题是大数据和云计算相关人员缺乏足够的信息安全意识，无法完善地执行信息安全策略和规范。在大数据和云计算的环境下，许多企业和机构将数百甚至数千台服务器集成在一起，以支撑业务运作。然而，这种架构主要关注数据的处理和计算速度，却忽略了数据安全问题。企业和个人对于数据保护的意识不够强烈，相对而言，数据加密技术和管理规范等安全策略也没有得到足够重视，从而造成数据的泄露和滥用风险的加大[3]。此外，大数据和云计算行业的快速发展，人才缺乏、技术更新也是潜在的风险。很多企业和机构为了求快速发展，而没有足够地投入进行信息安全培训和安全规范完善，他们可能很快就会被新技术和黑客攻击所淘汰。继而，第三方机构也会陷入数据泄露等风险，并造成巨大的信息安全问题。

3.2 系统复杂性提高了信息安全问题发生的概率

随着大数据和云计算技术的快速发展，人们对数据信息的处理和存储方式发生了重大变革。然而，因为大数据和云计算环境的系统复杂性难以掌控，很容易导致信息安全问题的发生。下面将从云计算系统复杂性角度，分析其对信息安全问题发生概率的影响。云计算系统的复杂性是指云计算技术中涉及到的各种技术，服务和软件系统之间的相互影响和相互作用，包括硬件、软件、网络和其它因素[4]。这种复杂性给信息安全带来一系列的挑战和威胁。这些挑战可能会导致以下一些问题：

（1）不确定的数据位置：由于大多数云服务提供商可能将客户的数据存储在多个位置，复杂的系统使得这种“数据漂泊”变得更加普遍。这种情况下，完全掌握数据的位置变得更加困难，也更容易被黑客攻击。

（2）多样的网络架构：当前的云计算系统使用各种多样化的网络模型，这使得网路安全变得更加困难，包括权限和访问管控等各个方面。

（3）高度自动化的系统：云计算系统通常采用高度自动化的系统，可能控制各种服务管理，从而使得漏洞、错误的发生和信息安全问题发生的概率大大增加。

（4）不同的安全平台：不同的云平台支持不同的安全性措施，这增加了在整个系统范围内开展一致性的安全性保护的难度，同时还加重了安全性的负担。

4 大数据与云计算背景下的信息安全防护策略

4.1 充分利用人工智能技术提高云数据的安全性

随着大数据和云计算技术的快速发展，人们对数据安全性的需求也越来越高。传统的数据加密技术已经不能满足大规模和高复杂度信息安全管理的需要，因此可以借助人工智能技术，在保护数据的同时提高云数据的安全性。人工智能技术可用于大数据和云计算安全中的三个主要方面：一、基于人工智能技术的威胁检测、攻击分析等安全管理机制，二是基于智能分析引擎的恶意代码检测、攻击预防、风险评估，三则是身份验证、权限管理等受控访问识别等安全机制。首先，基于人工智能技术的安全威胁检测和攻击分析是提高云数据安全性的重要手段。运用人工智能技术建立起一套快速、准确的威胁检测、防范和处理机制，能够识别安全事件并快速响应，进而避免数据泄露等安全问题的发生。引入深度学习、机器学习等算法，可以通过考虑的最新事件进行威胁分析和趋势预测，追踪攻击者的足迹，及时识别潜在安全威胁并迅速做出响应。其次，基于智能分析引擎的安全防护，通过计算机模型的训练，使智能分析引擎学习常见的攻击样本和攻击手法，并提供防范措施。通过分析大量的数据，智能分析引擎将检测出的信息进行分析和处理，及时推送该事件的预警信息和安全处理建议，提升网络运维和安全防范的效率和精度[5]。最后，身份验证和访问控制技术可以使云数据的安全性更加可控与安全。通过人工智能技术，设备具有智能身份认证技术，来识别并验证设备的身份。通过智能授权，设备

可以集成访问控制技术来控制用户的权限，提高数据的访问可控性，保护数据隐私。

4.2 建立信息安全技术管理机制

随着大数据和云计算技术的不断发展和应用，各种数据和信息被大量存储在云端，涉及到的信息数量和数据量呈几何级数的增长，因此如何保障信息数据的安全性，建立信息安全技术管理机制成为当前发展的紧迫需求。安全是相对而言的，通过建立完善的DN、DdoS攻击报警系统，以及相关的网络监管机制，可以及时侦查事项信息。同时，在安全人员的支持下，能够及时获得最新的网络攻击事件与技术咨询，紧跟新技术与新模式的发展,及时对各类安全事件进行排查与反应。关注安全详细日志监测。日志是关键到安全问题的警示与证据，同时也是监测恶意软件和黑客攻击的关键资源。因此，建立日志采集与处理平台，对所有重要日志进行安全性的日志记录，及时排查存在的风险性事件。修补和升级安全补丁。即便是最先进的安全技术也无法避免安全补丁的更新，随着日益更新的安全技术的涌现，不断修补安全漏洞，加强数据保护。及时安装已有的补丁与软件更新，规避安全漏洞的攻击风险。

4.3 建立信息安全问题识别的智能体系

随着大数据和云计算技术的发展，信息安全问题已经成为关键问题之一。为了建立一个智能的信息安全问题识别体系，需要首先了解当前大数据和云计算环境下的威胁和漏洞，包括各种安全攻击手段、黑客攻击的多样化，以及各种数据库和系统漏洞等等。这些知识和信息可以帮助我们更好地了解现有的安全问题，从而建立一个高效智能的信息安全问题识别体系。在通常情况下，建立信息安全问题识别体系主要有以下几个步骤：

（1）制定规则集和模型：根据当前的安全问题以及已知的漏洞和攻击手段，制定规则集和模型。这些规则集和模型可以包括各种指标、监控参数和平台性能要求等等，可以用于指导智能体系的判定和反馈。

（2）数据收集和分析：通过收集大量与安全事件相关的数据，对数据进行预处理和分析，提取出与安全事件有关的特征。提取出的特征可以作为训练数据，以训练相关的安全风险评估和识别模型。

（3）建立预测和评估模型：基于已经设定好的规则集和分析处理后的数据，建立预测和评估模型。预测模型可以根据历史数据和已知的攻击策略，预测未来可能出现的攻击，提高安全防范能力；评估模型可以对已知的安全事件，进行统计分析，为改进安全策略提供数据支持。

（4）矫正模型并范围测试：通过范围测试，反馈建立的各类模型并矫正模型。范围测试是指检测模型对输入的数据是否敏感，并对其结果的可靠性进行评估。建立完善的测试机制，保证预测和评估的准确性和实时性，对信息安全问题识别体系的判断和预测起到了很大的作用。

（5）部署和应用：完成开发和测试后，将这个智能体系部署到当前的大数据和云计算环境中。同时进行持续的监控和修正，保证智能体系始终处于最佳状态，发现和诊断任何可能存在的安全问题。

结语

大数据和云计算技术的发展，加上数字化时代的大规模数据存储和处理需求，对信息安全提出了巨大的挑战。建立完善的信息安全技术管理机制，利用新技术和科学的管理方式预防安全事件的发生，提高数据的安全性是当今亟需的工作之一。只有关注大数据和云计算相关安全问题，提高信息安全意识，采取多重保障措施，才能更好地保障大数据和云计算系统用户的数据安全。

参考文献

[1]刘红霞.大数据时代计算机信息处理技术研究[J].黑河学院学报,2018,9(08):217-218.

[2]吴少莹.云计算与大数据背景下的信息安全技术研究与实践[J].电脑迷,2018(09):26.

[3]王雅婷.基于云计算的大数据安全隐私与保护探究[J].黑河学院学报,2018,9(06):86-87.

[4]焦英楠.浅谈大数据环境下的云计算信息安全问题[J].中国管理信息化,2018,21(05):165-169.

[5]董超，刘雷.大数据背景下安全分析的网络安全技术发展趋势研究[J].网络安全技术与应用，2019（8）：62-63.