山东财经大学

本科毕业论文（设计）

题目：防范大数据金融信息安全风险的对策

学　　院　金融学院

专　　业　金融学辅修专业

班　　级　金融学辅修 1702 班（三年制）

学　　号　20161866148

姓　　名　于松黎

指导教师　王荣

山东财经大学教务处制

二〇20 年 4 月

防范大数据金融信息安全风险的对策

摘　要

在大数据与大数据金融时代，如何保障用户的信息安全这件事依然面临着新的挑战。但是大多数信息安全手段在目前依然不适合大数据金融面临的安全风险。本文首先概述了金融大数据模型及其成因，然后分析了大数据技术面临安全风险的原因。在此基础上，重点讨论和分析大数据金融面临的安全风险和保障措施，并阐述了解决大数据信息安全所面临的风险，以及对未来大数据和金融领域潜在安全风险的预测。

关键词：大数据金融；金融信息风险；供应链技术

Countermeasure to Prevent Information Security Risk of Big Data Finance

ABSTRACT

In the era of big data finance, information security is facing new challenges.. the original information security means are not suitable for the security risks faced by big data Finance.. this paper focuses on the analysis of the security risks and security measures faced by big data Finance.. this paper first summarizes the financial big data model and its causes, and then analyzes the reasons for the security risks faced by big data technology. On this basis, the risk and potential security risk of big data information security in the future and financial field are predicted.

Keywords: Big Data Finance;Finance Information Security Risk; Supply Chain Technology

目录

一、引言.....1
二、大数据金融信息的模式与安全风险.....1
（一）平台模式.....1
1.平台模式的特点.....1
2.平台模式存在的信息安全问题.....1
（二）互联网供应链金融模式.....2
1.互联网供应链模式的特点.....2
2.互联网供应链金融模式存在的信息安全问题.....2
三、大数据金融信息安全风险的形成过程与原因分析.....2
（一）平台模式的产生原因.....2
（二）互联网供应链金融模式的产生原因.....2
四、有效防范大数据金融信息安全风险的对策建议.....3
（一）平台模式的信息安全风险对策.....3
1.风险识别.....3
2.风险评估.....3
3.风险转移.....3
4.风险接受.....3
（二）互联网供应链金融模式的信息安全风险.....3
五、展望.....4
参考文献.....4

一、引言

随着互联网计算机技术的飞速发展，我国传统的金融模式发生了巨大的变化。 以区块链、云计算等网络技术为核心的基于金融领域互联网的信息处理系统被广泛推广应用，尤其是在企业和银行的日常运营中应用广泛。近年来，基于大数据的网络金融模式开始对传统的金融发展模式产生一定的影响。 在我国金融服务领域，融合大数据分析技术的现代金融发展模式逐渐扩大了市场份额，得到了全面推广。 其中，基于大数据的移动支付、企业众筹和支付宝业务已成为人们日常生活和生产中不可或缺的一部分。一些传统金融企业开始利用大数据分析，积极构建自己的网络金融服务和管理平台，扩大影响力，提高竞争力。 大数据分析技术可以不断促进金融业的创新和发展，使其逐渐成长为影响我国传统金融业发展的新力量。 占据国内电商平台的重要地位。

大数据在短时间内快速发展，数据价值不断挖掘，数据竞争日益激烈.. 虽然大数据金融可以为金融企业带来更完善的投资环境，优化金融资源配置，促进金融体系的发展，但也会给金融企业带来信息安全风险和问题。

然而，挑战与机遇并存。 新的信息技术给人民日报的工作带来了便利，但也存在一定的安全隐患.. 在大数据时代，信息安全风险管理是第一个需要解决的问题。保护大数据除了成为高价值和有吸引力的目标之外，还面临着独特的挑战。它不是那么大的。

数据安全从根本上不同于传统的数据安全。出现大数据安全挑战是因为。额外的差异，而不是根本的差异。大数据环境与传统数据之间的差异。环境包括：收集、聚合和分析数据以进行大数据分析。这些是用于存储和存放大数据的基础架构，也可用于分析结构化和非结构化大数据的技术。

由于主要优先考虑的是为大量数据提供速度，安全性通常是最后要考虑的事项。主要是因为对将要存储和传输的数据没有特定的分类。整合。不同的技术引入了新的安全挑战，

需要妥善解决，通常会被破坏。深入到特定于技术的挑战。如果大数据系统支持关键基础架构。安全性也成为一项要求。由于大数据系统复杂且异构，因此安全性方法必须是整体的，以确保服务的可用性和连续性。为了了解安全挑战，我们决定遵循大数据的使用规范，来探讨大数据金融安全风险。适用的标准是这些领域中的大数据是否成熟，从而从以下方面提供更大的价值。收集到的信息必须考虑到，由于大数据是一个相对较新的概念，因此在确定安全等具体问题的解决方案方面处于早期阶段。

二、大数据金融信息的模式与安全风险

大数据金融主要基于两种模式。一种是平台模式，另一种是互联网供应链财务模式。平台模式的主要代表是阿里巴巴金融和百度金融。互联网供应链金融模式的代表是京东金融。随着人们越来越认识到大数据在社会各个领域的重要性，数据安全已经成为一个必须重视的重要问题。虽然重要的是利用大数据的商业机会，如何防止这些数据被滥用，过度推广和使用违法者是一个大数据分析师需要考虑的问题。同时，大数据时代强调全社会信息资源的开放共享，但其中很多涉及个人隐私，如何平衡数据的使用权和所有权值得思考

（一）平台模式

1.平台模式的特点

企业平台采用平台模式，聚集众多商家。借助多年的交易数据积累，互联网技术和平台为企业或个人提供快捷便捷的金融服务。阿里巴巴金融的信息流（数据）和资金流来源于该平台多年的业务积累，积累了大量的会员信用信息和巨额资金。随后，阿里巴巴金融开始向小微企业提供无担保贷款，并通过余额宝金融服务开展保险业务。百度金融在互联网搜索领域处于领先地位，积累了大量利用百度推广相关信用信息的老客户。并通过引进

百度小额贷款等产品来扶持这些企业，扶持小微企业。

2.平台模式存在的信息安全问题

随着海量数据的不断增加，如何以合理有效的手段备份冷热数据，既保证有用数据的丢失率，又有效降低备份成本，是一个现实问题。此外，用户数据量增加，备份时间窗口小，设备存储容量有限。 如何节省空间，节约成本，提取核心数据将是一个技术难题..

（二）金融领域的网络供应链模型

1.互联网供应链模式的特点

以京东金融(电商平台)或宝钢股份的互联网供应链金融模式，是通过交易为产业链上下游提供融资，通过与银行等机构合作积累丰富的数据或信息提供者或担保人。在这种合作模式下，京东等企业只起到确认、审核、担保或提供信息的作用，不提供实质性资金。

2.互联网供应链金融模式存在的信息安全问题

互联网供应链金融模式积累了大量无差别的用户数据。积累的用户，根据供应链统计，通常只提供担保和信息，而不是资金。 然而，由于一些企业对客户的信用管理能力较低，各企业的实力不同，在交易过程中并不处于完全平等的地位。 在供应链金融的实际运作中，企业难以收集客户信用信息、管理档案、调查管理和信用评级，导致客户信用数据的不对称，并将导致严重的信息安全风险。 这些风险将进一步导致信用风险问题，导致信用风险防范、信用额度审查和财务管理差距。

三、大数据金融信息安全风险的形成过程与原因分析

造成以上信息安全风险的主要原因就是数据量的激增。

（一）平台模式的产生原因

在平台模式上，大数据平台模式是通过以往交易积累的海量数据，总结用户的行为习惯和思维模式，进而预测可能的行为。行为转折点难以把握，造成经济损失。其次，数据源是封闭的、片面的。电子商务企业在平台上获取交易数据，使得平台外的用户数据难以理解。社交网络中有大量的非结构化数据，如用户的思想、爱好等。如果我们从封闭的数据中得出结论，那肯定是片面的。不可避免地，采集到的大数据会与一些错误的数据混在一起。错误的数据会干扰正确的结论。例如，淘宝的刷单行为会导致错误的结论，从而推断商家的信誉。

（二）互联网供应链金融模式的产生原因

与平台模型相比，互联网供应链金融模型主要通过大数据技术信息处理实现有效的风险管理。 与传统供应链融资相比，进一步降低了中小企业的融资门槛。 然而，由于大数据采集和处理的复杂性、数据真实性保证的难度和侵犯用户隐私和安全的敏感性，削弱了这种方法的效果。 此外，互联网供应链金融和社交网络难以实现深度融合，大数据核心处理能力尚未培养，使得大数据的获取和处理成本高，数据的真实性难以保证。 在信息处理过程中，形成潜在的数据安全风险，大大降低了用户的隐私程度。

四、有效防范大数据金融信息安全风险的对策

金融信息化的实质是基于信息技术对传统金融服务和产品进行调整和创新。然而，随着金融服务的日益多样化和业务规模的不断扩大，金融业的信息安全风险逐渐暴露出来，成为影响和制约金融业发展的重要因素之一。银行系统信息安全风险管理一旦存在依赖于海量信息数据的脆弱性，就会造成客户信息泄露、资金流失等诸多问题。因此，大数据信

息的安全问题亟待解决。经过多年的发展，信息技术几乎涵盖了金融业的所有业务和流程，也有利于金融网络信息技术的发展。

（一）平台模式的信息安全风险对策

1.风险识别

规规划和组织流程、对系统组件进行分类、列出程序和数据、分类、识别威胁和识别易受攻击的数据。基于互联网技术的发展，互联网金融的信息安全技术需要重视和加强。传统的信息安全防护体系很难提供可靠的安全防护，尤其是对企业内部的APT攻击、零日漏洞攻击或网络攻击。 互联网金融企业要从信息系统全生命周期(ESLC)的角度，结合安全开发、安全产品、安全评估、安全管理等，加大对信息安全技术的投入，实现互联网金融的长效安全。

信息是对组织有价值的资产。对于组织的业务与其他重要业务资产一样。因此需要适当地受保护。实际上这在日益增长的互联互通的商业环境中发布了各种有效的标准。如国际标准化组织等。安全作为保护机密性、完整性和信息的可用性；此外，其他属性，如真实性、责任性、不可否认性和可靠性。为了获取信息安全性，组织需要首先确定什么是。需要保护并执行风险评估的资产，并通过实践练习以确定风险级别，直到控制以将这些风险降至最低，最终确保资产的安全。对于在线生产系统来说，通过防火墙、数据库审计、数据容灾等手段提高用户和数据的安全性是当务之急。

部署操作和维护审计和风险控制系统越来越多的巨大的金融信息系统提高财务信息的安全操作。维护管理系统通过账户管理、身份验证、自动密码更改、资源授权、实时阻塞,检测并行、回放审查,维护运行自动化、对过程进行管理等功能。为了预防与探查紧急事件响应、跟踪审查流程、统一控制与其他目的，研究的特点必须与自身信息系统相吻合，例

如安全预防的策略和规律;开展安全审计、强制门禁、系统架构、多层次系统安全互联门禁、产品符合性检查等相关技术;研究开发保护环境、安全区域边界、安全通信网络、安全管理中心等关键信息系统核心技术产品的安全计算;研发一些用户可以控制的模拟环境、操作系统、位于间接步骤的软件、资料仓库等其他产品，实现对代替国外软件，搭建软件模拟使用环境，通过可靠的软件检测产品实现电子金融系统的安全模拟，保证减少软件环境在使用时发生信息风险事故。

对目前需要维护的资产与虚拟产品进行细化与归类，从集体利润考虑并精确到大部分的虚拟电子资产或虚拟电子环境，将限制性的资料放到保护重要的虚拟电子资料中。中国金融信息系统的核心安全建设和保障，需要有一支具有专业信息安全服务能力和应急响应能力的安全服务队伍，并通过权威机构认证，具备一定规模和专业的扫描检测和渗透测试产品。

以信息安全水平为保障进行防护和风险管控，充分利用网络算力和数据挖掘优势，搭建适用于互联网金融信息系统自身的建筑规范和信息安全管理规范，将目前的安全防护方式多样化，并发展虚拟金融环境安全全面防护系统，确定并行算力和数据安全预防维护规范制度，补充协调规约，具有较强的协同发展能力。金融机构在实施外包前，应根据外包程度、风险集中度和多项业务外包给同一服务商的风险，制定具体的外包政策和标准。同时，在服务外包过程中，也需要进行内部金融风险预测。

搭建风险管理部门，用于直接向当事人报告，并与其他业务部门分开，单独的进行风险的估测与分析过程；根据自身的业务特点建立完整的工作过程制度。根据工作过程中的各环节产生的的安全风险，以大体上预估自身的安全中心；为了保障相似的工作能够精确地被分析，需要依据在工作过程中产生的安全问题，来使自己建设出的间接控制运作项目

能够标准化。

2.风险评估

风险评估时，应用策略和技术来规避尚未发生的风险或扭转已发生风险的趋势。主要评价方法有：网络金融信用、小微贷款管理、财富管理评价、高频交易分析、反欺诈预警、客户识别和损失预警、理赔审核评估、精算。

网络金融征信：由于P2P网贷市场快速增长，个人征信业务需求不断增加。通过大数据对客户征信记录进行实时分析，即实时分析客户征信记录并提供贷款依据，提升了企业价值。

小微贷款管理：需要大数据分析提供业务支撑，实时数据处理信息管理、交叉营销信用模型分析和业务风控需要不断完善。大数据提供交叉营销和信用模型分析。

财富管理评估：利用大数据分析为用户提供有价值的财富管理组合。广泛应用于银行、金融机构/券商/保险。利用内部和外部的大数据来分析有价值的财富投资组合。

高频交易分析：量化投资快速增长，结构化/结构化数据使用量增加。实时准确的数据模型，提供有价值的行业建议，提高客户满意度。利用数据对投资组合进行量化，建立了有效的数据模型。

反欺诈警告:泄漏和欺诈风险增加，控制不足，手段缺乏先进的分析能力，“实时和有效的”识别可疑索赔。通过大数据实时分析渗透欺诈的风险。客户识别与损失先入之见:分析识别潜在客户群体，维护老客户，降低客户开发成本成为主要需求，利用外部和内部大数据有效管理客户关系。

理赔审核与评估:已成为保险行业最大的问题识别难点。分析和评估索赔数据，有效降

低风险，为保险赔偿提供依据。数据审核数据评估，有效减少异常赔付和欺诈性保险。保险精算:利用大数据建立保险类型和赔付率模型，准确预测和提高保险行业核心业务需求的盈利能力。实时垂直支付率模型根据客户分析确定风险分类。在风险评估过程中，由于金融工程项目的特点，计算量大，可以依靠现有的分布式大数据计算来解决。数据采集:通过爬虫技术、数据治理和行业数据集成。

存储容量:通过列数据库、内存数据库、Hadoop键值数据存储，从TB到PB。计算能力:通过MPP (SHARE NOTNHING)的IOE可伸缩性，跨越硬件、代和供应商。分析技能:数据价值挖掘，统计样本扩展，专业工具，专业模型，行业模型。应用功能:信息可视化、管理精细化、预防向预测转化、精细系统等。

3.风险转移

目前互联网中存在的金融风险安全问题，大部分都来自互联网的攻击者系统。他们通常通过系统漏洞或者木马侵袭的方式，造成用户信息泄露。攻击者在几年前，往往都是单独进行攻击，且目的性较弱。但是近年来，攻击者之间逐渐形成一种体系，并且有很强的目的性，这使金融网络安全风险防范形式变得更加严峻。从大量采集与销售私人信息，到仿制银行卡，一些攻击者甚至会单独制作电子银行的系统安全病毒，在网络上都可以轻而易举的找到 病毒的提供者，因此，以金融领域互联网犯罪的灰色产业已经形成。他们通常通过系统漏洞或木马攻击泄露用户信息。袭击者从单打独斗转变为以经济利益为目标的集体袭击。

最近的案例表明，大部分的银行都在面临着各种各样的的DDoS攻击，包括DNS洪流攻击、DNS放大攻击、应用层DDoS攻击、应用层DDoS攻击和内容攻击难以防御。如今的互联网充斥着病毒、蠕虫、僵尸网络、间谍软件和DDoS，这些或多或少都或多或少地绕过了互

联网业务支撑系统的漏洞。例如，一些公司的远郊无线互联网络瘫痪可能会直接导致国内许多银行因遭受同样网络攻击而瘫痪。直到现在，网络安全病毒依然在更新，网上银行的安全也因客户信息被盗而损失惨重。如果用户没有在自己的计算机上安装相应的木马检测软件，则很容易受到感染。

当不可抗力导致风险无法有效规避或逆转过程无法生效时，应将风险转移到其他资产、其他过程或其他机构。风险转移包括提供服务、修改部署模型、外包给其他机构、购买保险以及与提供商签订服务合同。如果风险转移成功，则尝试通过提前规划和准备来减少风险，以减少漏洞的影响。在Internet环境中，交易信息是通过网络传输的。一些交易平台没有建立一个完整的机制来保护敏感信息在“传输、存储、使用、销毁”等环节，大大增加了信息披露的风险。尽管对于非法网站对金融领域资料安全的的行为，大部分金融机构的应对政策都十分积极，但是由于许多含有病毒的非法网站并不是建立在中国大陆网络，因此安全监管的难度大大增加。另一方面，由移动应用软件的信息安全隐患和用户防范意识的缺失，这使暴露出来的移动金融的信息风险给用户造成了严重的经济损失，阻碍了移动金融的发展。

4.风险接受

如果在上述操作之后风险无法避免，你只能选择接受风险，即在一系列操作之后，不采取针对漏洞的防护措施，接受漏洞的结果。操作包括确定风险级别、评估攻击的可能性、评估供应造成的潜在损害、进行全面的成本效益分析、评估使用每个控件的可行性，以及确定某些功能(服务、信息)或资产不值得保护。

风险本身的定义。它包括风险发生的程度、风险的持续影响间隔、风险发生位置和关键风险坐标。风险行为模型的定义。包括对企业的影响是直接影响还是间接影响的;是否会

引起其他相关风险;企业的风险范围等。风险后果的定义。亏损:如果存在风险，企业将遭受巨大的损失。如果能避免或降低风险，企业将付出巨大的代价。在风险承担的好处方面:如果企业承担风险，它可以获得很少的利润。如果能够避免或降低风险，对企业的效益仍然很小。

（二）互联网供应链金融模式的信息安全风险对策

互联网金融的持续必须依靠大数据作为底层支持。互联网供应链金融可持续发展的基础是银行信息平台的建立健全。⑴加强互联网供应链金融与社交网络深度融合，培育大数据核心处理能力，通过建立用户信息库降低大数据采集处理成本。⑵通过机器学习的方式，加强对原始数据的检查，可以保证数据的真实性，并根据实际需要将原始数据转化为专业知识资产，确保数据在交付过程中的安全。⑶为保护用户隐私，最好使用第三方数据脱敏产品进行数据脱敏。一方面需要加强供应链金融平台的互联互通能力，这包括数据嗅探、数据加工、数据可视化和维护数据有序性，为了提升全行业运行效率，还需要整合各企业数据基础资料。

五、展望

尽管金融服务公司仍然坚持改善大数据的安全环境，以实现自身利益的最大化，但仍有很长的路要走。银行家们仍在起草大数据的安全策略、切入点和后续使用案例。对银行而言，大数据金融主要通过加强监管来规避信息安全风险。在可预见的未来，第一类大型金融集团将继续在大数据的金融信息安全领域开展各种行动。在市场低端，一些中小企业(券商、资管、区域银行、顾问等)。可以更快的适配大数据的金融安全监控平台(云平台和本地部署)。这可以帮助他们建立能够抵御黑客攻击的大规模网络系统，他们和这些系统将不得不面对更大的竞争对手。对于大数据软件提供商和服务商来说，安全问题已经成为

银行业必须接受的热点。

每个人都应该在低风险、大规模、内控和以客户为中心的活动中有所作为。同时，这些内容也与我们看到的云技术发展路径不同。供应商和服务商要强化大数据技术的应用范围，以网络安全技术为支撑，建立一套完善的大数据金融安全保障机制，加强与客户、银行的长期合作关系。系统防范大数据金融信息安全风险。在大数据时代，互联网金融数据具有可视化优势。在大数据时代，人工智能、云计算、移动互联网等技术与金融服务深度融合，达到互联网金融数据可视化的目的。大量的数据检索变得容易，解决了以往数据获取困难、检索过程复杂等问题，使数据在全面的基础上更加直观，可以呈现简单的逻辑分析，提供更加准确的决策依据。在大数据时代，互联网金融数据具有便捷优势。

在大数据时代，互联网金融数据在数据采集、数据查询、数据共享等方面具有极大的便利优势。它改变了过去搜索和分享的困难。在互联网和信息技术的基础上，金融企业获取信息更加方便。

参考文献

[1] 傅少川，徐成贤.金融信息风险的防范对策研究 [D].《 中国安全科学学报 》， 2005

[2] 常文广，牛朋英，张云.基于商业银行视角的供应链金融信息风险研究 [D].《 价值工程 》， 2014

[3] 翁跃明.金融信息风险决策中的熵应用 [D].《 上海金融学院学报 》， 2012

[4] 丁昱.互联网金融信息风险与防范 [D].《 青海金融 》， 2015

[5] 高华.直击金融信息风险-深信服为北京银行构建互联网安全屏障 [D].《 网管员世界 》， 2008

[6] 刘振海，马征，缪凯．大数据在金融行业的应用现状与发展对策[J].《金融电子化》，2018(9):20-21.

[7]石勇，陈懿冰．大数据技术在金融行业的应用及未来展望[J].《金融电子化》, 2014(7):22-23.

[8]许伟，梁循，杨小平．金融数据挖掘:基于大数据视角的展望[M]．知识产权出版社, 2013.

[9]沙莎．大数据在金融行业的应用[J].《中国金融电脑》, 2014(6):34-34.

[10]魏国雄．大数据与银行风险管理[J].《中国金融》, 2014(15):25-27.