廣東財經大學
GUANGDONG UNIVERSITY OF FINANCE & ECONOMICS

广东财经大学		

继续教育学院本科毕业论文（设计）

基于 JAVA 的移动电商平台安全性研究

教 学 点	
专　　业	
班　　级	
学　　号	
学生姓名	
指导教师	
提交日期	年　　月　　日

毕业论文（设计）写作成绩评定表

写作成绩（五级记分制）_____

指导教师签名_____

年　　月　　日

内容摘要

2019 年双十一全网成交额为 4101 亿元，超过 2018 年双十一的交易额 3143 亿元。巨大的交易量带来了巨大的并发量，从而对移动电商平台有了更高的安全要求。本文以基于 JAVA 的移动电商平台系统架构出发，探究了基于 JAVA 的移动电商平台的安全机制以及安全风险。总结归纳了基于 JAVA 的移动电商平台的系统层次，对基于 JAVA 的移动电商平台使用的 JAVA 安全机制、数据传输安全机制、访问控制安全策略等安全机制进行了深入的探讨。研究了基于 JAVA 的移动电商平台单点服务故障与缓存失效等安全性风险及其解决方案。通过建立一个知识体系从而灵活有效地使用它们。

关键字：移动电商平台 JAVA 安全性

Abstract

As mobile e-commerce is blossoming, the security is more and more importance. Now, many mobile e-commerce platforms are use JAVA technology, so why and how use JAVA technology is importance. This paper is talk about the security of JAVA-based mobile e-commerce platform, it is include the system framework of JAVA-based mobile e-commerce platform, some bug of the system framework and some safe technology of JAVA-based mobile e-commerce platform. Frist, this paper is talk about the security of JAVA-based mobile e-commerce platform, it is introduce how and why the system is split and role of each layer. Second, this paper is talk about some safe technology of JAVA-based mobile e-commerce platform, it is include the safe technology of JAVA's, data transmission security mechanism and access control security strategy. Third, this paper is table about some bug of the system framework, it is include service failure of single point, cache's failure and why there are happened and how to solve. I wish we could build a knowledge system, and effective use it.

Key words: mobile e-commerce platforms JAVA security

目　　录

一、　绪论 1
二、　基于 JAVA 的移动电商平台系统架构 1
三、　基于 JAVA 的移动电商平台的安全性机制 4
(一)　JAVA 安全机制 4
1.　类装载器结构； 4
2.　class 文件检验器； 4
3.　内置于 JAVA 虚拟机（及语言）的安全特性； 5
4.　安全管理器及 JAVA API。 5
(二)　数据传输安全机制 5
1.　数据加密 5
2.　数字签名 6
3.　SSL 协议 6
(三)　访问控制安全策略 6
1.　基于角色的访问控制模型 7
2.　服务接口的安全设计 7
四、　基于 JAVA 的移动电商平台安全性风险 8
(一)　单点服务故障 8
1.　导致单点服务故障的原因 8
2.　单点服务故障的容错机制 9
(二)　缓存失效 9
1.　缓存穿透 9
2.　缓存雪崩 10
五、　总结 10
参考文献 12
致谢

基于 JAVA 的移动电商平台安全性研究

一、 绪论

电子商务是一种商业模式，它使得企业或个人能够通过网络进行交易。电子商务让企业在市场竞争上更加有优势，可以通过提供商品或服务得到更加快速高效的分销链[1]。随着互联网的快速发展，电子商务这种媒介得以发展壮大。随着移动设备的普及，移动商务已经成为独立的市场。移动电商是“无线的电子商务”，它是指用户通过移动终端如手机、掌上电脑等设备访问网络，进行各种电子商务活动[2]。近几年，移动电子商务平台数量在逐渐的增多，买家和卖家通过移动电子商务平台进行的交易额也在逐年呈现暴涨趋势。移动电商平台是建立在移动互联网基础上电子商务平台，像美团、饿了么、淘宝、拼多多都属于典型的移动电商平台。[3]

JAVA 能够快速、安全、可靠地构建基于分布式的移动电子商务系统，随着移动电子商务平台的不断发展，其体系结构也随着技术和时代的潮流发生了很大的变化，大致经历了三个阶段：

单点服务阶段：此阶段应用程序、数据库、文件都部署在一台服务器上，或者独立部署。

集群阶段：此阶段应用程序、数据库、文件分别部署，通过增加应用程序以及负载均衡的方式，将请求访问到不同的服务器上。

分布式阶段：此阶段将应用程序中各个业务应用都会使用到一些基本的业务服务，例如用户服务、订单服务、支付服务、安全服务。我们将这些服务从应用程序中抽离出来，利用分部式服务框架搭建分布式服务。

本文主要基于 JAVA 的移动电商平台安全性为研究目标。探讨目前基于 JAVA 的移动电商平台的系统架构、安全性机制、安全性问题及改进方案。

二、 基于 JAVA 的移动电商平台系统架构

随着移动电子商务平台的不断发展，通过移动电子商务平台进行的交易额也在逐年呈现暴涨趋势。为了应对愈发暴涨的流量，网站的系统架构，从最初的单独部署应用服务，到现在大规模集群方式，技术的发展经过了一代又一代的革新。以淘宝为例：最开始使用 LAMP（Linux+Apache+Mysql+PHP）架构，随着业务发展的复杂性，第二阶段使用 MVC 框架和 ORM 框架，实现了前后端分离，第三阶段使用 RPC 架构，把各个系统进行拆分，通过 RPC 进行各个系统之间的通信。JAVA 拥有

面相对象、跨平台、强类型等优秀特性，并且因为开源的原因，拥有良好的生态环境与强壮的生命力。经过调查研究，目前一个基于 JAVA 的移动电商平台架构如下：

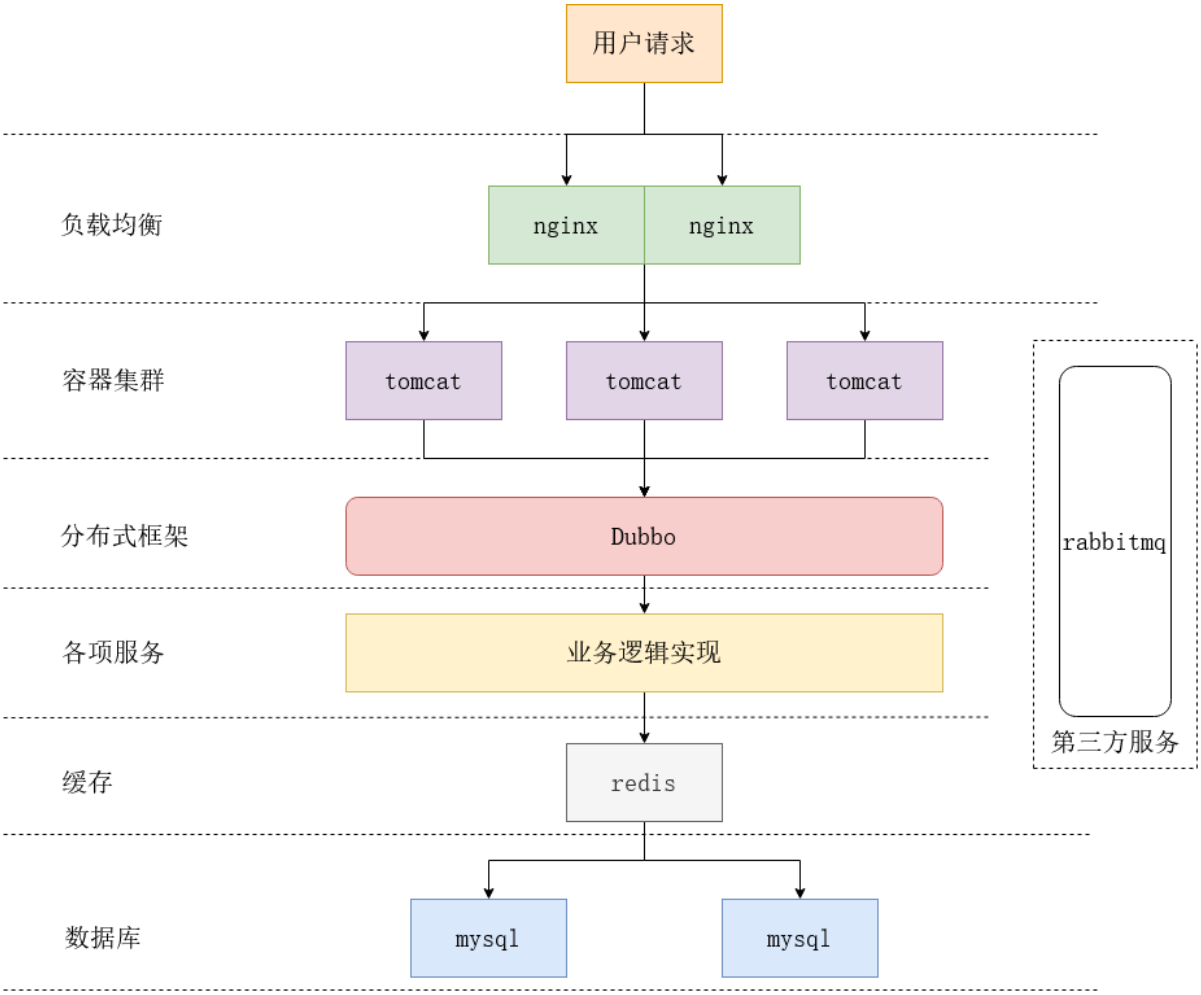

图 1 基于 JAVA 的移动电商平台系统架构

从系统架构来看，一个基于 JAVA 的移动电商平台按照各组成部分可以分为以下几个部分:

- 负载均衡

负载均衡是指有效地将传入的网络流量分布到一组后端服务器上，也称为服务器池。移动电商平台必须为用户提供成百上千的并发请求，并以快速和可靠的方式返回正确的文本、图像、视频或应用程序数据。受限与现代科学技术，一台服务器并不能承载成百上千的并发请求，为了以成本有效的方式处理这些请求，现代计算最佳实践通常是添加更多的服务器来解决。

通过负载均衡，可以将用户请求分发到提供相同功能的不同服务器，降低服务器因并发量过大而导致容器奔溃的几率。也可以将 CSS，JS，HTML，图片等静态资源从容器中分离出来，使得单个容器更易维护，运行效率更高。

现在使用最广泛的负载均衡工具为 nginx。

- 容器集群

Servlet 容器是指使用 JAVA 编写的，一个符合 Servlet 容器规范的程序，该程序封装了包含 HTTP 的网络协议规范，使得开发过程中，不用关注网络部分，从而能更好的专注于业务开发。Servlet 容器的作用是负责处理客户请求，当客户请求来到时，容器获取请求，然后调用某个 Servlet，并把服务的执行结果返回给客户。

容器集群，在一个移动电商平台中，单个容器并不能承载如此庞大的并发量，为了加强整体架构的刚性，承载更大的并发量，在一个移动电商平台中，通常采用多个容器，形成一种容器集群的模式。

- 分布式框架

在一个移动电商平台中，为了拆分业务，更好的使用容器，单个容器并不会拥有太多的功能，随着业务的发展，容器的增多，容器间相互通信与管理成为了一个很大的难题。分布式框架并不是一个程序，它是一段预先编写好的代码，封装了容器与容器之间相互通信的协议，提供了丰富的 API，使得开发过程中，不用过分关注容器与容器之间的通信，每个开发人员可以只关注自己的部分业务。

一个分布式框架通常包括: 服务发现注册、配置中心、消息总线、负载均衡、断路器、数据监控等功能。

- 服务

这里的服务是指由开发人员编写的程序逻辑，一个移动电商平台常见的服务有：登录服务、购物车服务、交易服务、对账服务等。开发人员进行开发时，通常会分为三层：视图层、业务层与持久层。视图层负责页面展示与调整、业务层负责业务模块的逻辑应用设计、持久层负责数据持久化工作。

- 缓存

缓存就是将程序或系统经常要调用的对象存在内存中，以便其使用时可以快速调用，不必再去查询数据库或者第三方服务。在一个移动电商平台中，往往存在着大量的热点数据，这些数据查询的频率很高，但是并不需要实时更新，如商品详情，商品浏览数，以及商品评论等。对这类数据采用缓存，能有效的降低数据库的访问频率，减少由数据库瓶颈对整个移动电商平台的影响。

- 数据库

数据库是一个长期存储在计算机内的、有组织的、有共享的、统一管理的数据集合。在一个移动电商平台中，单个数据库不会存储所有业务的数据，而是会根据业务进行划分，单个数据库只存储与单个容器相关的业务数据。如果需要表与表之间的关联查询，往往是通过业务逻辑来实现的。

- 第三方服务

第三方服务是指由第三方实现的程序，它封装了一系列的功能，只要按照程序的

API 给与入参，程序就能使用相关功能，节约了开发者开发相关功能的时间。目前在移动电商平台中用的比较多的第三方服务有：消息队列服务（rabbitmq），工作流服务（actoviti），搜索引擎（solr）。

三、 基于 JAVA 的移动电商平台的安全性机制

系统越复杂，也就越容易发生问题，这是恒古不变的真理，对于基于 JAVA 的移动电商平台，常使用以下机制保证其安全性。

(一) JAVA 安全机制

JAVA 是基于 JAVA 的移动电商平台的基石，如果 JAVA 不安全，则系统的安全性则无从谈起。JAVA 通过的沙箱安全模型保证了其安全性，JAVA 提供的沙箱组件有以下几种：

1. 类装载器结构；

- 防止恶意代码去干涉善意的代码。

这是通过为不同类加载器提供不同的命名空间来实现的，在 JAVA 虚拟机中，在同一个命名空间内的类可以直接进行交互，而不同的命名空间中类甚至不能觉察彼此的存在，除非显式地提供允许它们交互的机制。

- 守护了被信任的类库的边界

虚拟机通过使用不同的类装载器装载可靠的包和不可靠的包，即所谓的双亲委派模式：在某个特定的类装载器试图以常用方式装载类型之前，它会先默认将这个任务“委派”给它的双亲，这个双亲再依次请求自己的双亲来装载这个类型。这个委派的过程一直向上继续，直到达到启动类加载器（boostrp classloader），如果一个类加载器的双亲类加载器有能力装载这个类型，则这个类加载器返回这个类型，否则这个类装载器试图自己来装载这个类型。

- 将代码归入某类（称为保护域），该类确定了代码可以进行哪些操作。

2. class 文件检验器；

和类加载器一起，class 文件检验器保证了装载的 class 文件内容中有正确的内部结构，并且这些 class 文件相互间协调一致，如果 class 文件检验器在 class 文件中发生了问题，它将抛出异常。

JAVA 虚拟机的 class 文件检验器在字节码执行之前，必须完成大部分检验工作。class 文件检验器需要经过四趟独立的扫描来完成其工作。

第一趟扫描：class 文件结构检查。对每一段被当做类型导入的字节序列，class 文件检验器都会确认其是否符合 class 文件格式。

第二趟扫描：类型数据的语义检查。检验一些 JAVA 语言应该在编译时遵守的强制规则。

第三趟扫描：字节码验证。它确保局部变量在赋值之前不可访问，类的字段中总必须赋予正确类型的值等等。

第四趟扫描：符号引用验证。在这趟检查中，JAVA 虚拟机将追踪那些引用，从被验证的 class 文件到被引用的 class 文件，确保这个引用是正确的。

3. 内置于 JAVA 虚拟机（及语言）的安全特性；

JAVA 虚拟机装载了一个类，并且对它进行了第一到第三趟的 class 文件检验，这些字节码就可以被运行了。除了对符号引用的检验（class 文件检查的第四趟扫描），JAVA 虚拟机在执行字节码时，还进行了一些内置的安全机制的操作。这些机制大多数是 JAVA 类型安全的基础：

1.类型安全的引用转换；

2.结构化的内存访问（无指针算法）；

3.自动垃圾收集；

4.数组边界检查；

5.空引用检查。

4. 安全管理器及 JAVA API。

安全管理器定义了沙箱的外部边界，保护虚拟机的外部资源不被虚拟机内运行的恶意或者有漏洞的代码侵犯。JAVAAPI 在进行一个可能不安全的操作前，总是会检查安全管理器，所以 JAVAAPI 不会在安全管理器建立的安全策略下执行被禁止的操作。

(二) 数据传输安全机制

基于 JAVA 的移动电商平台容器众多，数据传输过程中，安全性十分重要，尤其是对于一些敏感的用户信息，其安全性保证更应当被重视。保证传输数据的安全性，主要有以下方法：

1. 数据加密

数据加密一直是数据安全的重要部分，数据加密也就是利用技术手段对重要数据进行加密，然后把加密过后的数据进行传输，到达目的地后再用相同或不同的手段进行解密。对数据加密的技术分为两类，即对称加密技术和非对称加密技术。

- 对称加密

对称加密的特点是加密与解密时采用相同的密钥。对称加密算法简单快捷，密钥较短，且破译困难。对称加密以数据加密算法（DES， Data Encryption Standard）为

典型代表。对称加密在使用中会存在以下几个问题：

1.通讯双方在首次通讯时需要一个安全的通道协商一个共同的密钥；

2.密钥的数目难于管理；

3.对称加密算法一般不能提供信息完整性的鉴别；

4.对称密钥的管理和分发工作是一件具有潜在危险的和烦琐的过程。

- 非对称加密

非对称加密算法需要有两个密钥，公开密钥和私有密钥。一般来说，公钥并不需要对任何人保密，是公开的。私钥并不公开，只有其所有者知道。如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。

非对称加密算法的保密性比较好，它消除了最终用户交换密钥的需要，但加密和解密花费时间长、速度慢，不适合于对文件加密而只适用于对少量数据进行加密。

2. 数字签名

数据加密只解决了传输数据机密性的问题，如果需要确认发信者的身份，则需要使用数据签名的技术。数字签名是建立在公开密钥体制基础上，它是公开密钥加密技术的另一类应用。它的主要方式是，报文的发送方从报文文本中生成消息摘要，发送方用自己的私有密钥对这个消息摘要进行加密来形成发送方的数字签名，然后，这个数字签名将作为报文的附件和报文一起发送给报文的接收方。报文的接收方首先对接收到的原始报文生成消息摘要，接着再用发送方的公开密钥来对报文附加的数字签名进行解密。如果两个值相同、那么接收方就能确认该数字签名是发送方的。

使用数字签名，能确认以下两点：第一，信息是由签名者发送的；第二，信息自签发后到收到为止未曾作过任何修改。

3. SSL 协议

SSL（安全套接字）协议利用对称加密技术和公开密钥加密技术，在两点之间交换私钥建立了安全的连接。该协议提供了以下的安全服务：

1.认证用户和服务器，确保数据发送到正确的客户机和服务器；

2.加密数据以防止数据中途被窃取；

3.维护数据的完整性，确保数据在传输过程中不被改变。

(三) 访问控制安全策略

访问控制是给出一套方法，将系统中的所有功能标识出来，组织起来，托管起来，将所有的数据组织起来标识出来托管起来， 然后提供一个简单的唯一的接口，

这个接口的一端是应用系统一端是权限引擎。权限引擎所回答的只是：谁是否对某资源具有实施 某个动作（运动、计算）的权限。返回的结果只有：有、没有、权限引擎异常了。

1. 基于角色的访问控制模型

传统的强制访问控制和自主访问控制由于各自的缺点均不能满足移动电商平台对访问控制的需求。在基于角色的访问控制模型中，将资源与角色相关联，角色与用户关联，将角色设置成资源的集合，从而使得整个模型系统设计的简易性和安全控制的灵活性。同时允许角色进行重用、继承和派生操作。这样，不仅可以对资源进行访问控制，而且派生角色可以继承父角色的访问控制设置，这对于信息量巨大、内容更新变化频繁的移动电商平台非常有益，可以减轻由于信息资源的派生、演化和重组等带来的分配、设定角色权限等的工作量。

2. 服务接口的安全设计

在一个移动电商平台中，资源的形式通常是以接口的形势存在的，它需要相应的参数，程序执行完成后，返回对应的输出。基于角色的访问控制模式仅仅能保证用户是否能访问接口，但是却没有对接口的入参进行校验，因此，如果想要更高的安全性，往往还需要对服务接口进行以下设计：

- 时间戳机制

因为移动电商平台的数据经常在公网上传输，容易被抓包，虽然经过加密，加签处理，攻击者拿不到真实数据，但是攻击者仍然可以基于此，进行恶意请求。这时候可以使用时间戳机制，在每次请求中加入当前的时间，服务器端获取当前时间和消息中的时间比较，看看是否在一个固定的时间范围内，这样恶意请求的数据包是无法更改里面时间的，所以不在固定时间范围内的请求就视为非法请求了；

- 限流机制

因为移动电商平台对外开发，攻击者能合法的拿到账号数据，并且对移动电商平台进行正常请求。但是，如果出现频繁极高重复调用接口的情况，这个时候就需要限流。限流机制是基于计数器方法，当一定时间内，用户请求数超过设定的阈值时，进行限流，拒绝该次接口调用的请求。

- 黑名单机制

如果一个账号多次进行非法操作，比如多次请求访问不属于自己角色接口时，此时考虑黑名单机制。黑名单机制通常使用标记法来实现，即当一个用户进行多次非法操作时，更改该用户状态，下次用户在进行请求时，验证状态，如果状态异常，则拒绝该次请求，或者进行账号封停操作。

- 数据合法性校验

数据合法性校验对于移动电商平台尤为重要，数据合法性校验是指对请求的入参

精选校验，常规的校验有身份证长度，电话号码长度等；安全性的校验有特殊字符，特殊标签等。常见的攻击手段往往都是通过使用非法的请求参数对系统进行攻击。比如 XSS 攻击，就是使用非法字符，向页面中植入一段脚本，使得其他用户访问这个页面时，信息泄露至脚本处。严重的情况可导致整个移动电商平台奔溃，无法正常服务。

四、 基于 JAVA 的移动电商平台安全性风险

即使有着相应的安全机制，也难以避免系统故障，与发生风险，以下是两种在基于 JAVA 的移动电商平台比较常见的系统安全性问题：

(一) 单点服务故障

单点服务故障是指在整个移动电商平台的系统架构中，容器集群中的单个容器无法提供正常服务，即接口不能提供正确的返回结果。对于移动电商平台来说，一次完整的调用需要多个容器协同工作，一个容器故障，无法正常提供服务，就可以导致这次调用链的失败。如果没有使用有效的容错机制，请求链接不能有效地关闭，错误的请求会积压到调用方，从而降低整个移动电商平台的吞吐量。

1. 导致单点服务故障的原因

- 配置错误

配置文件是平台中一些需要预定义变量的集合。配置文件编写错误即预定义的变量与正确变量不符。配置错误通常包括容器配置文件编写错误，或程序配置文件编写错误。容器配置配件编写错误会导致容器无法正常启动，对外提供服务；或能正常提供服务，但是容器里的资源接口无法正常访问。容器与容器之间的通信主要通过分布式框架的注册中心与分布式框架协议。注册中心负责服务的注册与发现。如果分布式配置文件编写错误，会导致程序无法正常启动，或程序正常启动，但是调用方无法找到被调用方的情况。

此外，程序中还有一些第三方服务，或者程序框架的配置文件。如果这些配置文件出错，均会导致单点服务故障。

- 程序异常

在 JAVA 里，异常被分为检查异常和非检查异常。检查异常是指编写程序时，class 文件检验器校验 class 文件，并非提示的异常，这类异常会在编写程序期间处理并解决。非检查异常是指程序的瑕疵或逻辑错误，并且在运行时无法恢复，class 文件检验器无法校验，在异常发生时，由 JAVA 虚拟机捕捉异常，并输出到控制台。

非检查异常无法在编译期解决，它对于整个移动电商平台有着更大的危害。导致

非检查异常的原因多种多样，有一种非检查异常是在程序编写递归服务时，递归服务没有定义结束递归的边界，从而无限调用，产生内存异常。还有一种非检查异常是空指针异常，这里的指针并不是 C 语言中的指针，它是在 JAVA 虚拟机中，指向内存区中的对象的指针。程序运行时，该句柄指向的对象为空时，调用这个空对象的方法或属性时，就会抛出空指针异常。

2. 单点服务故障的容错机制

对于单点服务的故障，一般有以下的容错机制：

- 重试机制

重试机制是当发生单点服务故障时，调用方或者被调用方居然进行重新调用的情况。但是并不是所有情况都需要进行重试，当被调用方出现异常时则需要进行重试，如：程序异常、调用超时、网络中断等。符合程序安全机制的部分则不进行重试，如：数据不合法、用户处于黑名单中、消息中的时间戳不符合等。在分布式框架中通常有着自己的重试机制，在 dubbo 中可以设置 retries=1，timeout=500，即调用失败只重试 1 次，超过 500ms 调用仍未返回则调用失败。

- 服务熔断

服务熔断是当该单点服务多次发生故障，多次重试后均返回错误异常，此时对该服务进行熔断。服务熔断的作用可类比成家用保险丝，当服务不可用的情况发生时，为防止系统架构雪崩，暂停该服务的应用。但是与家用保险丝不同的是，服务熔断会间隔一段时间进行服务调用测试，如果服务正常，则恢复该服务应用，如果服务异常，则继续保存熔断状态，等待下一次的服务调用测试。

(二) 缓存失效

缓存使用流程：服务先从缓存中取数据，取到数据直接返回结果，取不到数据时从数据库中取，数据库取到更新缓存，并返回结果，数据库也没取到，直接返回空结果。当缓存失效时，用户请求无法使用缓存，导致请求压力直接积压到数据库，从而导致整个系统失效。以下是缓存失效的原因以及常用的处理方案。

1. 缓存穿透

缓存穿透，是指用户请求缓存和数据库中都没有的数据。在使用数据库时，会采用一个自增长的正整数作为主键，缓存中获取数据的依据通常含有主键，以正整数主键为例，正整数主键从 1 开始，步长为 1，那么此时多次请求主键-1 时，或者超过数据库整数类型长度时，这时就会发生缓存穿透，请求直达数据库，并且数据库中无相应数据。

因为缓存穿透是缓存以及数据库中都没有对应数据，对于缓存有以下处理方法：

第一种处理方法：将数据库中所有数据导入至缓存，更新数据库时同时更新缓存，直接减去查询数据库的步骤。对于这种方法来说，少量的配置类型的数据是可以的，但是对于移动电商平台来说，数据量过于庞大，不可能将内存作为第二数据库，因此该方案在移动电商平台中无法应用。

第二种处理方法：查询数据库时，如果数据库中没有数据，就将一个空对象插入到数据库中，下次再有同样的请求，则将缓存中的空对象返回。这种处理方法的缺陷在于，可以执行缓存穿透的主键极多，使用这种方法，缓存中会存在着大量的无用的空对象，使用这些空对象，有可能也会造成程序的异常。对于此，人们又对这种方法做了一些改进，即使用布隆过滤器。布隆过滤器的工作方式是：定义一个数组，每个位置都保存为 0；定义一系列 HASH 函数；当键入缓存数据时，对缓存数据的键进行 HASH 运算，将数列中对应的元素置为 1；获取数据时，对缓存数据的键进行 HASH 运算，如果数据中的元素为 0，则说明数据不存在。因为受限于队列大小，存在 HASH 碰撞的可能性，即使当数据中的元素为 1 时，数据也不一定存在，依然要从数据库中获取。但是使用布隆过滤器，能大大的减少了从数据库中获取数据的几率。

2. 缓存雪崩

缓存雪崩，是指缓存中数据大批量同时过期，导致大量数据直接请求数据库，从而导致系统失效。在移动电商平台正式服务前，会把热点数据键入缓存中，从而减少正式上线后直接查询数据库的频率，如果这部分热点数据设置了同样的缓存过期时间，那么在缓存将会同时过期，发生缓存雪崩。对于缓存雪崩，解决方法也比较简单，每个缓存设置不同的过期时间即可，或根据需要，让该缓存永不过期。

五、 总结

人们从很多安全事件和专家的警告中，渐渐地认识到应用程序安全性的重要性。现在，它也成为信息安全中的一个重要课题，成为大家关注的一个焦点。一个移动电商平台，难以避免存在安全性问题。目前任意一个移动电商平台，每时每刻都有黑客在公司网站上扫描。有的是寻找 SQL 注入的缺口，有的是寻找线上服务器可能存在的漏洞，大部分都是使用黑客检测工具来扫描，如 Linux 发行版 KALI，就集成了大量的黑客工具，当然更高级一点的入侵需要很多人工协助。

一般情况下，系统被攻击是因为开发人员平时没有安全意识导致的，厉害的黑客往往会对平台的业务和内部流程非常熟悉，很多漏洞是从逻辑上分析出来的。所有的攻击行为都是有目的，99% 都是因为其中隐藏着暴利。比如 2015-2017 年，很多互联网金融公司遭遇黑客敲诈，最后都是打钱了事。不仅如此，网站的漏洞还有可能被竞争对手利用。这里分享一段美团趣事，美团曾经被 12306 禁止爬取票务信息，这对美

团抢票业务照成很大影响，此时美团通过爬取市场上相同功能的竞品的票务信息作为备用，维持自身业务，但是这却对竞品造成了异常请求，影响了竞品的使用用户的体验。

安全其实就是一个矛盾的问题。任何保障安全的措施实际上都是一种无形的屏障，会带来一定的运行效率损失。所以在开发中加入应该更全面的考虑。如何在效率和安全之间做出权衡？首先，我们需要知道哪些工具是用于安全的，使用它们的本质是什么，使用它们的优缺点是什么。本片论文提及的基于 JAVA 的移动电商平台系统架构、基于 JAVA 的移动电商平台安全性机制、基于 JAVA 的移动电商平台安全性风险，仅仅只是抛砖引玉。对于安全性问题，我们应该对其有一定了解，建立起相应的知识体系，这样当面对安全性问题时，我们才能更好也更加有效的解决。

参考文献

[1] Strzębicki D. The Development of Electronic Commerce in Agribusiness – The Polish Example ☆[J]. Procedia Economics & Finance， 2015，（23）:1315-1321.

[2] 唐兴家.移动电商安全问题探析[J].中山市技师学院（科技经济导刊），2016，（2）：33-34.

[3] 李婷婷.快消品移动电商平台消费者购买意愿影响因素分析[D].大连工业大学，2016.

[4] 刘梦飞. 基于 JAVA 平台安全性的分析与研究[D].山东师范大学，2008.

[5] 赵文奎. 电商平台分布式架构设计与实现[D].重庆大学，2008.

[6] 熊厚仁，陈性元，杜学绘，王义功. 基于角色的访问控制模型安全性分析研究综述 [J]. 计算机应用研究，2015，32（11）：3201-3208.

[7] 崔鹏. JAVA 平台及应用 JAVA 技术的安全问题[J].辽宁轻工职业学院（信息与电脑），2019，（15）：160-161.

[8] 裴得志. 基于 J2EE 的 WEB 安全研究 [D].武汉理工大学，2006.

[9] 李俊. B2B 电子商务平台系统关键技术研究[D].山东大学，2018.

致 谢

我历时近两个月的时间终于把完成了这篇论文，在这段充满奋斗的时间里，带给我的学生生涯无限的激情与收获。在论文写作的过程中遇到了无数的困难与障碍，都在老师和朋友的帮助下度过了。尤其要强烈感谢我的论文指导老师--李志勇老师，没有他对我不厌其烦的指导与帮助，就没有我这篇论文的最终完成。在此，我向指导过帮助过我的老师们表示最衷心的感谢！

同时，我也要感谢本论文所引用的各位学者的著作，如果没有这些学者的研究成果的启发与帮助，我将无法完成本篇论文。至此，我也要感谢我的朋友和同学，他们在我写论文的过程中给予了我很多有用的素材，也在论文的排版和撰写过程中提供了热情的帮助！金无足赤，人无完人。由于我的学生水平有限，所写论文难免有不足之处，恳请各位老师和同学批评和指正！

广东财经大学成人高等教育毕业论文（设计）指导记录表

<table>
<tr><td colspan="2">教学点</td><td></td><td>姓名</td><td></td><td>学号/考号</td><td></td></tr>
<tr><td colspan="2">专业</td><td></td><td>联系方式</td><td colspan="3"></td></tr>
<tr><td>论文选题</td><td colspan="6">指导意见：

指导教师签名：　　年　　月　　日</td></tr>
<tr><td>论文初稿</td><td colspan="6">指导意见：

指导教师签名：　　年　　月　　日</td></tr>
<tr><td>论文定稿</td><td colspan="6">指导意见：

指导教师签名：　　年　　月　　日</td></tr>
</table>