无线网络与物联网应用课程期末试题：

一、问答题：

1. 简述 wifi1~wifi7 无线网络通讯性能。（10 分）

wifi1~wifi7 是指无线局域网（WLAN）的七代标准，分别对应 IEEE 802.11 的不同修订版本，如 wifi1 对应 802.11a，wifi2 对应 802.11b，以此类推，wifi7 对应 802.11be。

wifi1~wifi7 的性能主要体现在数据传输速率、频段、带宽、调制技术、多用户接入、多链路操作、多 AP 协作等方面，随着标准的更新，性能也逐渐提升。

wifi1 的数据传输速率为 54Mbps，使用 5GHz 频段，支持 20MHz 带宽和 64-QAM 调制技术，不支持多用户接入和多链路操作。

wifi2 的数据传输速率为 11Mbps，使用 2.4GHz 频段，支持 20MHz 带宽和 CCK 调制技术，不支持多用户接入和多链路操作。

wifi3 的数据传输速率为 54Mbps，使用 2.4GHz 频段，支持 20MHz 带宽和 OFDM 调制技术，不支持多用户接入和多链路操作。

wifi4 的数据传输速率为 600Mbps，使用 2.4GHz 或 5GHz 频段，支持 20MHz 或 40MHz 带宽和 256-QAM 调制技术，不支持多用户接入和多链路操作。

wifi5 的数据传输速率为 6.9Gbps，使用 5GHz 或 60GHz 频段，支持 20MHz、40MHz、80MHz 或 160MHz 带宽和 256-QAM 调制技术，不支持多用户接入和多链路操作。

wifi6 的数据传输速率为 9.6Gbps，使用 2.4GHz 或 5GHz 频段，支持 20MHz、40MHz、80MHz 或 160MHz 带宽和 1024-QAM 调制技术，支持 OFDMA 和 MU-MIMO 等多用户接入技术，不支持多链路操作。

wifi7 的数据传输速率为 30Gbps，使用 2.4GHz、5GHz 或 6GHz 频段，支持 20MHz、40MHz、80MHz、160MHz 或 320MHz 带宽和 4096-QAM 调制技术，支持 Multi-RU 等多用户接入技术，支持 Multi-Link 等多链路操作技术，并引入了多 AP 协作优化等新特性。

2. 简述 Starlink 的原理与当前应用现状。（10 分）

Starlink 是由埃隆·马斯克创办的太空探索技术公司（SpaceX）开发的一项卫星互联网服务，目的是通过在低地球轨道部署数千颗卫星，为全球每个角落，包括覆盖不足的农村地区提供高速、可靠、实惠的互联网接入。

Starlink 的工作原理是利用低地球轨道卫星组成的星座，与地面站和用户终端进行通信。卫星之间使用激光链路形成一个网状网络，可以在全球范围内中继数据。用户终端是碟形的天线，可以自动指向最佳的卫星并接收互联网信号。

Starlink 的目标是为没有互联网连接或连接不稳定的人群提供快速、可靠、实惠的互联网服务，包括农村社区和现有服务过于昂贵或不可靠的地方。SpaceX 表示，它目前在 36 个国家/地区拥

有 40 万用户，主要在北美、欧洲和澳大利亚，包括家庭和企业客户。Starlink 计划在 2023 年将其覆盖范围进一步扩展到非洲、南美洲和亚洲。

Starlink 的收费相对较高，与标准的互联网供应商相比。客户的月费是 99 美元（英国每月 89 英镑）。连接卫星所需的碟形天线和路由器的成本为 549 美元（529 英镑）。而英国 96%的家庭已经可以连上高速互联网，欧盟和美国 90%的家庭也一样。因此，Starlink“依靠一小部分市场份额来获得收入”。

Starlink 不是唯一一个正在开拓近地轨道空间的公司，还有英国的 OneWeb 和 2018 年成立的中国公司银河航天等竞争对手，都在实施各自版本的“星链”，将大量低轨卫星送上天。这种趋势必将带来低轨资源紧张和空间拥挤问题，“使得空间碰撞风险更高”。卫星可能会撞击其他（太空）船只并产生残骸碎片，反过来，这些碎片在高速飞行时可能会造成更大的损害。

Starlink 卫星也给天文学家带来新问题——在日出和日落时，它们可以被肉眼看到，卫星外翼反射太阳，闪闪发光，而这可能导致望远镜图像上出现条纹，模糊恒星和行星的视野。

Starlink 也在帮助乌克兰应对俄罗斯军队的威胁，当乌克兰的互联网服务被关闭，社交媒体网站也岌岌可危时，马斯克在冲突开始后立即在乌克兰推出了 Starlink 服务，向该国运送了 1.5 万套天线接收碟和路由器。它也被用于战场。乌克兰军队正在用它进行通信，例如指挥部和前线作战部队之间的通信。Starlink 的信号不像普通无线电信号那样容易干扰，而且只需 15 分钟即可设置完毕。

二、小论文（80 分）：

请撰写一篇无线网络相关小论文，题目自拟。

建议：请结合无线网络或物联网针对研究电子竞赛或物联网大赛完成一个作品及论文并成功参赛。

无线传感器网络数据保护在医疗行业的应用

摘要

无线传感器网络（Wireless Sensor Networks，WSN）是由大量的密集部署在监控区域的智能传感器节点构成的一种网络应用系统，能够实现对目标区域的信息感知、采集和处理。无线传感器网络在医疗行业有着广泛的应用前景，可以为患者提供实时、准确、便捷的医疗监护服务，提高医疗质量和效率。然而，无线传感器网络在医疗行业的应用也面临着数据保护方面的挑战，如数据的敏感性、完整性、可靠性、可用性、可追溯性等。本文综述了无线传感器网络在医疗行业的应用场景、目标和技术，并重点分析了无线传感器网络在医疗行业的数据保护问题及其解决方案，包括加密、认证、访问控制、隐私保护、安全路由、安全聚合等技术。本文旨在为无线传感器网络在医疗行业的数据保护提供一个综合的视角和参考。

关键词：无线传感器网络；数据保护；医疗行业；应用

Abstract

Wireless Sensor Networks (WSN) is a network application system composed of a large number of intelligent sensor nodes deployed in the monitoring area, which can realize the perception, acquisition and processing of information in the target area. Wireless sensor network has a wide application prospect in the medical industry, which can provide patients with real-time, accurate and convenient medical monitoring services, improve medical quality and efficiency. However, the application of wireless sensor networks in the medical industry is also faced with data protection challenges, such as the sensitivity, integrity, reliability, availability, traceability and so on. This paper summarizes the application scenarios, objectives and technologies of wireless sensor networks in the medical industry, and focuses on the analysis of wireless sensor networks in the medical industry data protection issues and solutions, including encryption, authentication, access control, privacy protection, secure routing, security aggregation and other technologies. This paper aims to provide a comprehensive perspective and reference for data protection of wireless sensor networks in the medical industry.

Key words: wireless sensor network; Data protection; The medical industry; application

目录

1 引言

随着微电子技术、通信技术和计算机技术的快速发展，无线传感器网络作为一种新兴的信息获取和处理技术，引起了学术界和工业界的广泛关注。无线传感器网络由大量的廉价微型传感器节点组成，这些节点通过无线通信方式形成一个多跳自组织网络，能够协作地感知、采集和处理网络覆盖区域中被感知对象的信息，并呈现给用户。无线传感器网络具有低功耗、低成本、分布式和自组织等特点，使其能够适应各种复杂和动态的环境，为人类提供更加丰富和精细的信息服务。

无线传感器网络在农业生产、生态监测、工业控制、智能交通等领域已经得到了广泛应用。其中，医疗行业是无线传感器网络最具潜力和价值的应用领域之一。随着人口老龄化和慢性疾病增多等社会问题的出现，人们对于医疗服务的需求和期望越来越高。然而，传统的医疗模式存在着诸多不足，如医疗资源分布不均、医患沟通不畅、医疗成本高昂、医疗质量难以保证等。基于无线传感器网络的医疗监护系统可以为患者提供实时、准确、便捷的医疗监护服务，提高医疗质量和效率，缓解医疗资源的紧张，改善医患关系，提升患者的生活质量和满意度。

无线传感器网络在医疗行业的应用主要包括以下几个方面：

（1）医院内部的医疗监护。无线传感器网络可以在患者身上安置多种生理参数传感器，如心电、血压、血氧、体温等，实时采集患者的生命体征数据，并通过无线通信方式将数据传输到医院的中央监控系统，使医护人员能够随时随地了解患者的健康状况，及时发现异常情况，提供及时有效的诊断和治疗。无线传感器网络可以实现对所有住院患者的全面覆盖和持续监测，而不仅仅是重症监护病房的少数患者。无线传感器网络还可以减少医护人员的工作量和压力，降低医疗成本和风险，提高医疗安全性和可靠性。

（2）家庭和社区的远程医疗监护。无线传感器网络可以在患者家庭或社区的生活环境中安装多个环境参数传感器，如温度、湿度、光照、噪音等，实时采集患者的生活环境数据，并通过无线通信方式将数据传输到个人医疗终端，如智能手机、平板电脑等。个人医疗终端可以将数据显示在用户界面上，并根

据设定的阈值或规则进行分析和判断，给出相应的提示和建议。个人医疗终端还可以通过互联网或移动通信网络将数据上传到远程的医疗云平台或专家系统，实现与远程医生或专家的交互和咨询，获取更专业和权威的诊断和治疗方案。无线传感器网络可以实现对居家或社区患者的长期跟踪和监测，而不需要患者频繁地去医院就诊。无线传感器网络还可以提高患者的自我管理能力和主动性，增强患者对自己健康状况的了解和掌控。

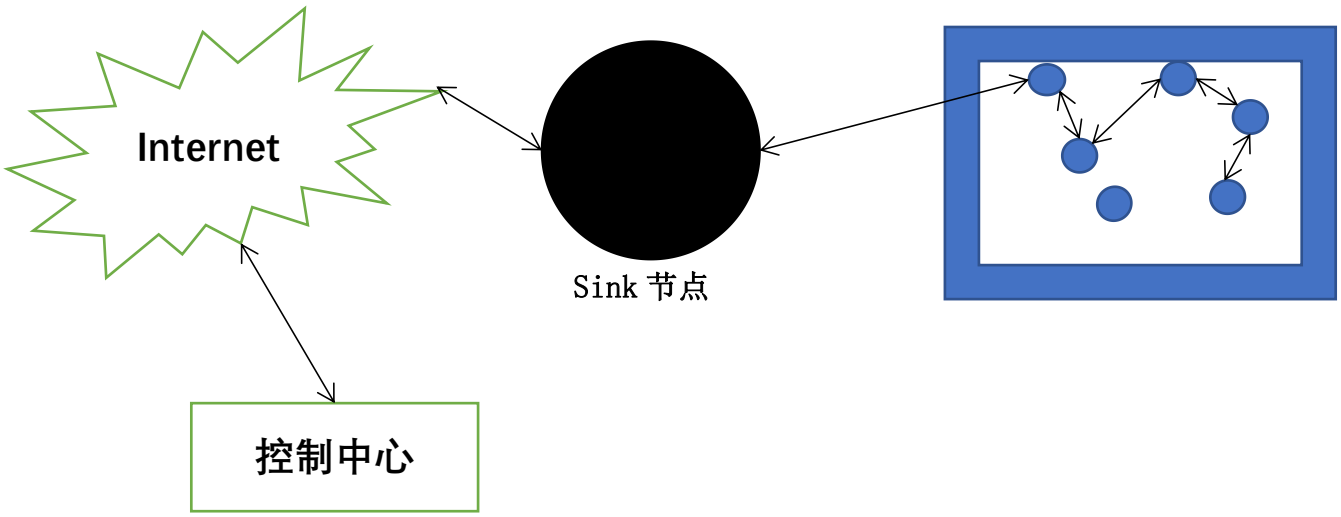
（3）紧急救援和灾难救助的移动医疗监护。无线传感器网络可以在紧急救援或灾难救助现场部署多个移动传感器节点，如无人机、车载节点等，实时采集现场的环境信息和伤员信息，并通过无线通信方式将数据传输到移动指挥中心或救援队伍，使指挥人员或救援人员能够及时了解现场的情况，制定合理有效的救援方案。无线传感器网络还可以在伤员身上安置多种生理参数传感器，实时采集伤员的生命体征数据，并通过无线通信方式将数据传输到移动指挥中心或救援队伍，使指挥人员或救援人员能够及时了解伤员的健康状况，优先救救治重伤员，并提供必要的急救措施。

2.无线传感器网络的概述

2.1 定义

无线传感器网络是由大量低成本、能耗低、可自组织的节点构成的网络系统，这些节点能够收集环境信息进行处理和传输，实现对物理世界的实时监测、控制和应用。无线传感器网络是一种分布式传感网络，它的末梢是可以感知和检查外部世界的传感器，能够实时地监测、感知和采集节点部署区的环境或观察者感兴趣的感知对象的各种信息，并对这些信息进行处理后以无线的方式发送出去。以无线形式通信的传感器组成的网络，可以采集、处理、发送信息。

2.2 典型场景



传感区域

传感器节点

WSN 一般由传感器节点、Sink 节点、外部网络构成，Sink 节点为汇聚节点，作为传感器区域与外部网络通信的桥梁。

2.3 特征

(1)无线自组网

WSN 是一种无线自组网，而无线自组网有以下特点：

1.自组织

节点自己寻找邻居节点，通过多跳传输的方式搭建整个网络。如果有节点加入或退出，则需要重新组织网络。

2.分布式

网络的感知能力由若干冗余节点共同完成，每个节点具有相同的硬件资源和通信距离，网络的运行不受个别节点加入和退出的影响。

3.节点平等

除 Sink 节点以外，各传感器节点分布随机，以自己为中心，负责通信范围内的数据交换

4.可靠性要求高

由于采用无线信道，且需经过多跳路由，故可靠性不高。易受到干扰、窃听，保密性差。

(2)独特特征

WSN 除作为无线自组网外，还具有以下独特特征：

1.结点资源有限

如能量、通信能力、计算存储能力等

2.网络规模大

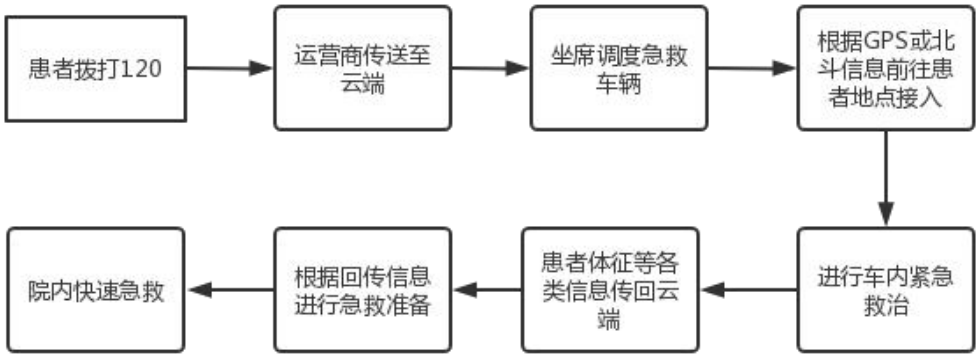
覆盖范围大且部署密集，单位面积存在大量结点

3.时效性

WSN 需要在一定时间内将采集到的信息传递给观察者或数据中心

2.4 无线传感器网络在医疗行业的具体应用

无线传感器网络院前急救的基本原理是通过物联网传感器，将患者的生命体征信息和其他检查结果实时通过 4G 网络传回医院，让医生提前做好诊疗准备具体步骤如下：



这种方式可以有效地节省救治时间，提高急救效果。

3.无线传感器网络在医疗数据传输中面临的问题

无线传感器网络在医疗数据传输中面临的问题主要有以下几个方面：

1.能耗问题。无线传感器网络的节点通常是由电池供电的，因此需要考虑如何降低节点的功耗，延长网络的寿命。一些方法包括使用低功耗的通信协议，采用数据压缩和聚合技术，设计合理的网络拓扑和路由算法，利用节能模式和唤醒机制等。

2.安全性问题。无线传感器网络的数据涉及到患者的隐私和健康信息，因此需要保证数据的机密性、完整性、可靠性和可用性。一些方法包括使用加密和认证技术，采用安全的密钥管理和分发机制，设计抵抗攻击的协议和算法，利用入侵检测和容错技术等。

3.信道干扰问题。无线传感器网络的通信信号可能受到其他无线设备或环境噪声的干扰，导致数据传输的质量下降或丢失。一些方法包括使用动态信道分配技术，采用多跳或中继技术，设计自适应的调制和编码技术，利用多天线和多址接入技术等。

4.兼容性问题。无线传感器网络的节点可能使用不同的通信协议或标准，导致数据传输的不兼容或冲突。一些方法包括使用统一的通信接口和协议栈，采用开放式的平台和架构，设计灵活的网络层次和功能模块，利用中间件和网关技术等。

4.无线传感器网络数据保护

4.1 无线传感器网络数据保护的方法

无线传感器网络在医疗行业中通常会遇到数据冗余、数据丢失的情况，那么这个时候就要进行数据保护，常见的数据保护有以下几种：

1.密码技术。密码技术是保证数据机密性和完整性的基本手段，主要包括对称加密、非对称加密和哈希函数等。对称加密使用相同的密钥进行加密和解密，适用于节点之间的通信，但需要解决密钥分发和管理的问题。非对称加密使用不同的公钥和私钥进行加密和解密，适用于节点和基站之间的通信，但计算量较大，需要优化算法和参数。哈希函数可以将任意长度的数据映射为固定长度的摘要，用于验证数据的完整性，但需要防止重放攻击和伪造攻击。

2.密钥管理。密钥管理是无线传感器网络数据保护的核心问题，主要涉及密钥生成、分发、更新、撤销等过程。密钥管理的目标是在保证安全性的同时，尽量降低节点的能耗、存储和通信开销。常见的密钥管理方案有基于预分配的方案、基于概率的方案、基于组合设计的方案、基于位置信息的方案等。

3.安全路由。安全路由是保证数据可靠传输的重要手段，主要考虑如何在不可靠的网络环境中，选择合适的路径和中继节点，避免或抵抗各种攻击，如虫洞攻击、黑洞攻击、灰洞攻击、拒绝服务攻击等。常见的安全路由协议有SPIN、LEACH、SPEED、ARAN、SEAD等。

4.数据融合。数据融合是利用多个节点收集到的相关数据，通过一定的算法进行处理和分析，得到更准确和有效的信息，并减少数据传输量，从而节省能耗和带宽。数据融合可以在不同层次进行，如物理层、链路层、网络层、传输层或应用层等。数据融合需要考虑如何在保证数据质量和隐私的同时，实现高效率和低开销。

5.数据查询。数据查询是指用户或基站向无线传感器网络发送查询请求，

获取感兴趣区域或感兴趣事件的相关数据。数据查询可以分为单点查询和多点查询，也可以分为快照查询和持续查询。数据查询需要考虑如何在保证查询正确性和完整性的同时，实现低延迟和低能耗。

6.入侵检测。入侵检测是指监测无线传感器网络中是否存在异常或恶意行为，并及时采取相应措施，防止或减轻对网络造成的损害。入侵检测可以分为基于异常的检测和基于规则的检测，也可以分为主动式检测和被动式检测。入侵检测需要考虑如何在保证检测准确性和及时性的同时，实现低误报率和低漏报率。

本文主要使用的是方法是密钥管理协议在医疗数据保护中的应用。

4.2 密钥管理协议来实现数据的保护

密钥管理协议在医疗数据保护应用，主要是为了保证医疗数据的安全性、完整性和可用性，防止数据的泄露、篡改和丢失，同时满足数据的合法合规共享和使用。

4.2.1 密钥协议的特点

密钥管理协议应该具备以下特点：

1.可靠性：能够确保密钥的正确生成、分发、更新和销毁，防止密钥被伪造、篡改或重放。

2.安全性：能够确保密钥的机密性、完整性和不可否认性，防止密钥被窃取、泄露或滥用。

3.高效性：能够尽量减少密钥管理所需的通信开销、计算开销和存储开销，提高密钥管理的效率和可扩展性。

4.灵活性：能够适应不同的网络环境和应用场景，支持多方参与者之间的动态协商和变更。

4.2.2 密钥的基本概念

加密包括两个元素：算法和密钥。一个加密算法是将消息与密钥（一串数字）结合，产生不可理解的密文的步骤。密钥是结合密码算法一起使用的参数，拥有它的实体可以加密或恢复数据。

密钥可以分对称密钥和非对称密钥。

1. 密钥分层管理结构如下所示：

2. 密钥生成

密钥的建立包括密钥的生成和分发。

①生成如下：

PBKDF2 是一个基于口令的密钥导出函数，导出密钥的计算公式:

DK = PBKDF2(HashAlg, Password, Salt, count, dkLen)

PBKDF2 ：密钥导出函数名

输入：

HashAlg ：哈希算法（SHA256）

Password ：用户输入的口令或者读取的一串字符串

Salt ：盐值，为安全随机数，至少为 8 字节

count ：迭代次数，正整数

dkLen ：导出密钥的字节长度，正整数。

输出：

DK ：导出的密钥，长度为 dkLen 个字节的字符串。

②分发如下：

密钥的分发是将密钥通过安全的方式传送到被授权的实体，一般通过安全传输协议或者使用数字信封等方式来完成。

数字信封加解密接口

接口	IpSI	OpenSSL
加密	CRYPT_sealInit()	EVP_SealInit()
加密	CRYPT_sealUpdate()	EVP_SealUpdate()
加密	CRYPT_sealFinal()	EVP_SealFinal()
解密	CRYPT_openInit()	EVP_OpenInit()
解密	CRYPT_openUpdate()	EVP_OpenUpdate()
解密	CRYPT_openFinal()	EVP_OpenFinal()

3. 密钥备份

密钥丢失将导致密文数据无法解密，这样便造成了数据的丢失。特别是在医院，有大量的重要数据包括病人的病情情况，患者以及在职员工的身份信息等都需要对密钥提供备份与恢复机制。

4.3 详细设计

4.3.1 信息采集

健康数据通常包括血压、体温、心率和血糖等，如表所示：

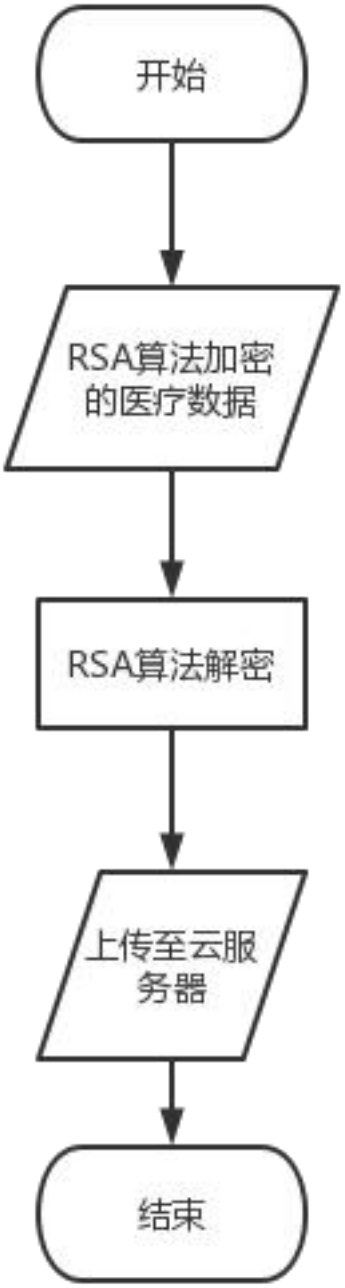
名称	用途
心电数据	患者疾病跟踪
血氧数据	睡眠检测
血糖数据	糖尿病检测及治疗
体温	疾病预防和治疗
血压数据	高血压检测和治疗

用户在上传数据之前，可以使用 RSA 算法对数据进行加密，然后将加密好的数据上传到云服务端。具体加密公式如下所示：

$$m^e \equiv C \pmod{n}$$

其中，m 表示待加密的数据，（n，e）表示由 RSA 算法生成的公钥，C 表示生成的密文。经过加密的数据，就不会泄露信息了，从而保护传输过程中的隐私安全。

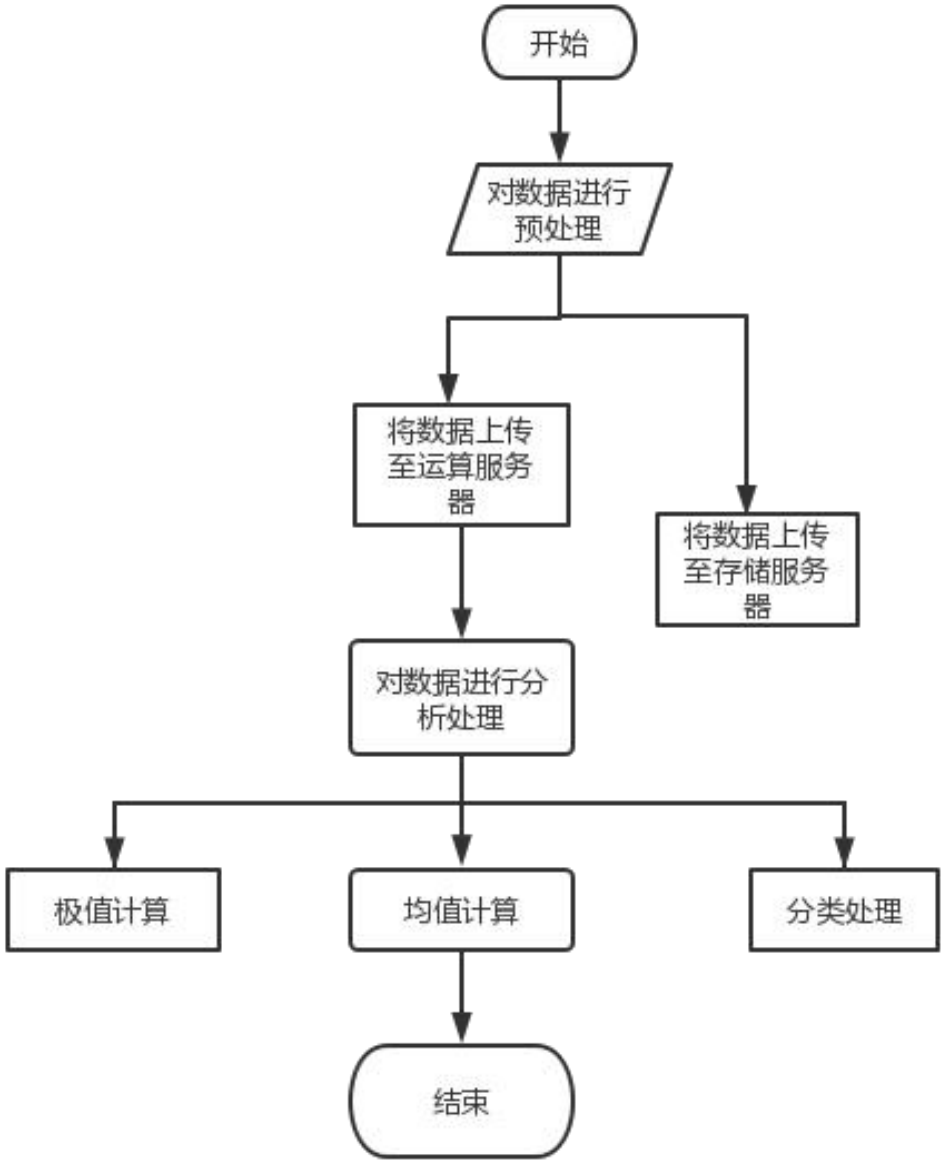
4.3.2 预处理流程图



为了更好地了解用户的健康状态，可以通过云服务器来分析计算加密的健康数据，主要是计算数据的平均值和极值。因为数据的平均值能表示数据的整体水平，根据平均值就能评估用户 基本的健康状态是否正常。而且计算数据的极值能知道数据中是否存在一些异常值，从而在用户数据超出正常值时，做出

提醒。

云服务器处理密文数据的流程图如下所示：



5.结论

随着互联网技术的发展和医疗信息化的普及，医院和其他健康机构产生了大量的医疗数据。这些医疗数据集大体可以根据获取的来源不同分为两类：一类是在医院就医过程中产生的医疗数据；另一类是健康机构通过可穿戴设备收集到的健康医疗数据。其中医疗数据是存放在医院信息系统中，有专门的部门进行管理，对数据的隐私性具有一定保护。而健康医疗数据的隐私保护措施则相对薄弱，但健康医疗数据中含有大量的用户敏感数据，如果发生数据泄露可能会侵犯用户的隐私，甚至会导致财产损失。

本文着眼于医疗数据的隐私保护，主要是指通过采集到的健康医疗数据。结合 RSA 加密算法方案，该方案既能保证用户数据在传输和存储过程中的隐私安全，又能对用户数据进行分析与处理。

对今后工作的建议：

通过对医疗数据的基础应用研究，发现数据加密仅是保护隐私安全的一种途径。本文需要进一步完善的问题：本文仅是通过数据加密方法来对医疗数据进行隐私保护，保护医疗数据隐私安全的方法还有很多，可以在后续的时间中对其进行学习和研究。