ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

T/

团 体 标 准

T/XXX XXXX—XXXX

5G 核心网信令数据的采集、处理、传输与隐私保护技术规范

Technical specification for the collection, processing, transmission and privacy protection of 5G core network signaling data

（征求意见稿）

XXXX－XX－XX 发布 XXXX－XX－XX 实施

发 布

目　　次

1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　总体架构 2
5　原理 3
5.1　隐私保护 3
5.2　同态加密算法 4
5.3　威胁流检测分析原理 5
5.4　Hyperledger Fabric 联盟链 5
6　信令数据生成与仿真 6
6.1　正常信令流数据模拟生成 6
6.2　异常信令流数据模拟生成 6
6.3　数据流捕获 7
7　数据加密玉隐私保护 7
7.1　概述 7
7.2　数据加密技术 7
7.3　数据访问控制 9
7.4　身份认证与权限管理 10
7.5　数据完整性验证 10
7.6　零知识证明 10
7.7　数据存储与传输加密 11
8　数据共享与检索 11
8.1　数据共享 11
8.2　共享通道 12
8.3　信令数据管理 14
8.4　身份管理 14
8.5　联盟链管理 14
9　分布式存储管理 15
9.1　分布式存储架构要求 15
9.2　数据存储与访问控制 15
9.3　数据可靠性与完整性 16
9.4　存储性能与效率优化 16
9.5　数据隐私保护措施 16
10　威胁流检测与分析 16
10.1　范围 16
10.2　数据预处理 17
10.3　威胁检测规范 17

10.4 异常行为分析 18
10.5 威胁溯源规范 19
11 建立可视化展示平台 19
11.1 数据库建立 19
11.2 可视化分析平台 20
附录A（资料性） 实验室工作条件 21

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意某些内容可能涉及专利，本文件的发布机构不承担识别这些专利的责任。

本文件由××××提出。

本文件由××××归口。

本文件起草单位：重庆邮电大学、深圳北理莫斯科大学、香港大学、澳门科技大学、广州波奇亚标准及检测技术有限公司、中国检验检疫科学研究院粤港澳大湾区研究院、中山市信裕科技有限公司、中山亿联智能科技有限公司、OrionAI Limited、中山市政达企业管理服务有限公司。

本文件主要起草人：宁兆龙、熊炫睿、王小洁、胡希平、王云帆、关乐淳、吴锡标、邱云翔、张俊林、郭星佑、巩勋、高云利、陈狮雄、吴宇、谢晓刚、Edith C. H. Ngai、田晋宇、Terry H. S. Chu、李喜彤、罗丙燕、钟晓雨。

5G 核心网信令数据的采集、处理、传输与隐私保护技术规范

1 范围

本文件规定了5G核心网信令数据在采集、处理、传输、存储与隐私保护中的技术要求、实验方法、以及数据的采集、加密、共享、分析等内容。

本文件适用于5G核心网控制面和用户面信令数据的处理与保护，包括信令流的模拟生成、数据的加密与访问控制、隐私保护、威胁检测及可信共享等应用场景。本标准同样适用于基于联盟链技术的数据共享平台和基于零知识证明及同态加密的隐私保护系统。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2022 信息安全技术术语

GB/T 22239-2020 信息安全技术 网络安全等级保护基本要求

GB/T 37988-2019 云计算服务安全能力要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

信令数据 signaling data

指5G核心网中的控制面和用户面信令流数据，包括设备间交互的协议消息及流量信息。

3.2

数据采集 data collection

通过探针或其他接口从5G核心网设备中提取信令流数据的过程。

3.3

零知识证明 Zero-Knowledge proof

一种允许证明方在不泄露任何实际信息的情况下向验证方证明某项声明的真实性的密码学技术。

3.4

同态加密 homomorphic encryption

一种允许对加密数据直接执行数学运算的加密技术，解密后结果与对明文执行相同运算的结果一致。

［来源：GB/T 25069-2022］

3.5

联盟链 consortium blockchain

由多个组织共同维护的区块链，仅授权节点参与共识，用于数据共享与访问控制。

3.6

数据完整性 data Intergrity

数据在传输、存储和处理过程中未被篡改的特性，可通过哈希校验或数字签名技术实现。

3.7

数据访问控制 access control

通过技术手段限制对信令数据和系统资源的访问权限的过程，包括基于角色（RBAC）和基于属性（ABAC）的控制方式。

3.8

数据脱敏 data masking

对敏感数据进行伪匿名化或遮盖处理的技术，确保数据内容在共享或存储时不可恢复至原始状态。

3.9

数据共享 data sharing

在授权条件下，在多方之间交换或访问信令数据的过程，需确保数据安全和隐私保护。

3.10

加密 encryption

采用算法将明文数据转换为密文的过程，以保护数据机密性。包括对称加密（如AES）和非对称加密（如RSA）。

［来源：GB/T 25069-2022］

3.11

身份认证 authentication

确认用户身份真实性的过程，常采用密码、数字证书、多因素认证等方式。

3.12

威胁检测 threat detection

通过分析信令流数据，发现和识别潜在网络威胁的技术方法

3.13

威胁检测 threat detection

信令数据在数据库或分布式存储系统中的保存过程，需确保其可用性、安全性和一致性。

3.14

多通道隔离 multi-channel Isolation

一种基于联盟链技术的数据共享机制,通过划分独立的数据通道,实现数据的安全隔离和访问控制。每个通道独立维护成员和数据共享范围,确保不同业务场景下的数据隔离性。通过加密和身份认证技术，多通道隔离可保护敏感数据，防止未授权的访问或数据泄露，同时支持动态调整通道配置，满足复杂的共享需求，如跨组织的敏感数据交换。

3.15

数据传输 data transmission

信令数据在网络中移动或共享的过程，需通过加密协议（如TLS/IPSec）确保安全性。

3.16

分布式存储 distributed storage

将数据分布存储在多个节点中以提高可靠性和可用性的存储方式。

3.17

数据压缩 data compression

采用算法对信令数据进行编码以减少数据存储或传输占用空间的过程。

3.18

数据冗余 data redundancy

通过在多个节点存储相同数据副本来提高数据可靠性和容灾能力的技术手段。该技术广泛应用于分布式存储系统，通过副本策略和地理分布机制，确保即使部分节点故障，数据依然可以被恢复。在5G核心网中，数据冗余可以用于信令数据存储和共享，防止单点故障引发的数据丢失，并保障网络服务的高可用性和持续性。

3.19

区块链 blockchain

分布式账本技术，通过去中心化和不可篡改性实现数据共享和可信记录。

4 总体架构

5G核心网信令数据处理与保护的完整框架如图1所示，涵盖数据生成、存储、保护、分析与平台建设的全流程管理。主要内容包括：正常与异常信令数据的生成；分布式存储的架构优化与数据可靠性管理；通过加密技术、身份认证和零知识证明等手段实现数据访问控制和隐私保护；在确保数据完整性和

安全性的前提下，支持数据共享与检索；通过威胁流检测与分析明确异常行为及潜在风险源；最终构建可视化展示平台，提供安全分析与共享功能，全面保障5G网络数据的安全性、完整性和高效管理。

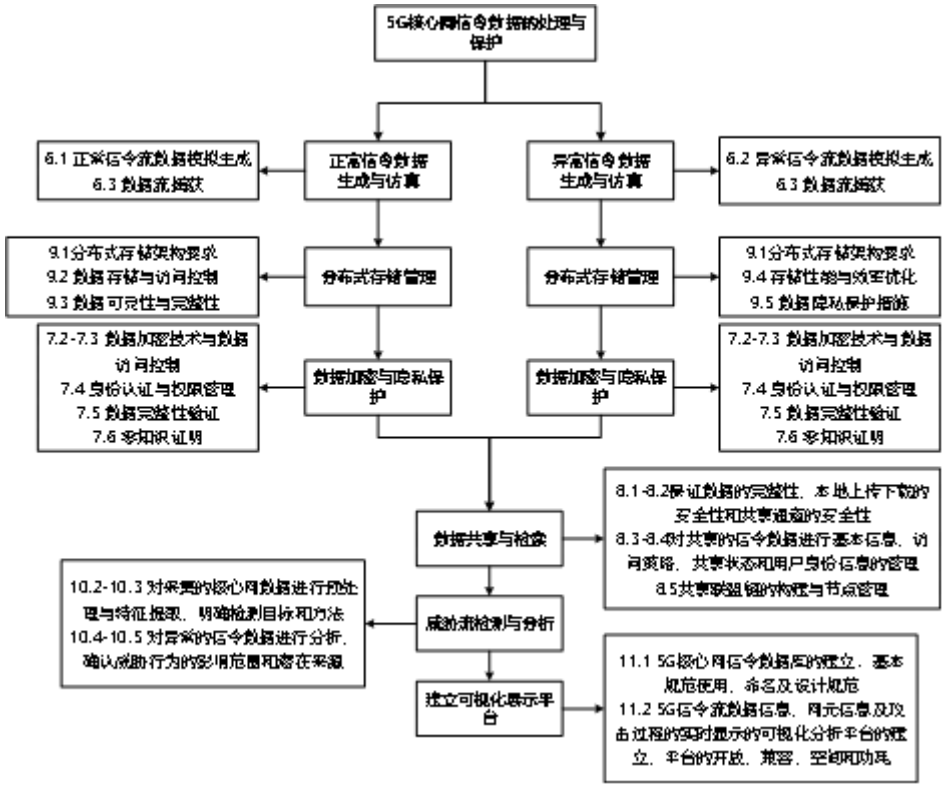

图1　15G 核心网信令数据处理与保护的完整框架图

5　原理

5.1　隐私保护

私保护技术的核心在于确保数据或信息在敏感内容未暴露的情况下，依然能够实现验证、操作或处理。通过数学和密码学方法实现数据的隐私性、安全性和高效性，主要包括零知识证明和同态加密两种关键技术。零知识证明是一种密码学方法，使得证明者可以在不泄露具体信息的前提下，向验证者证明某一声明的真实性。这一技术的核心目标是保护隐私，同时确保信息的真实性和有效性。同态加密是一种允许对加密数据直接进行数学运算的加密技术，运算结果解密后与对明文直接运算的结果一致。这一特性使得数据可以在不解密的情况下进行计算，从而保护数据隐私，如图2、图3所示。

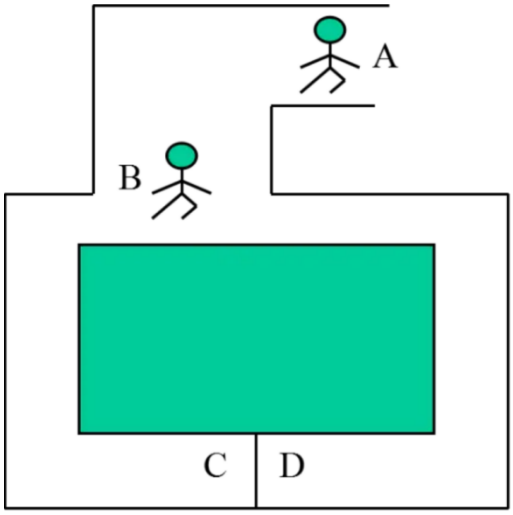

图2　零知识证明

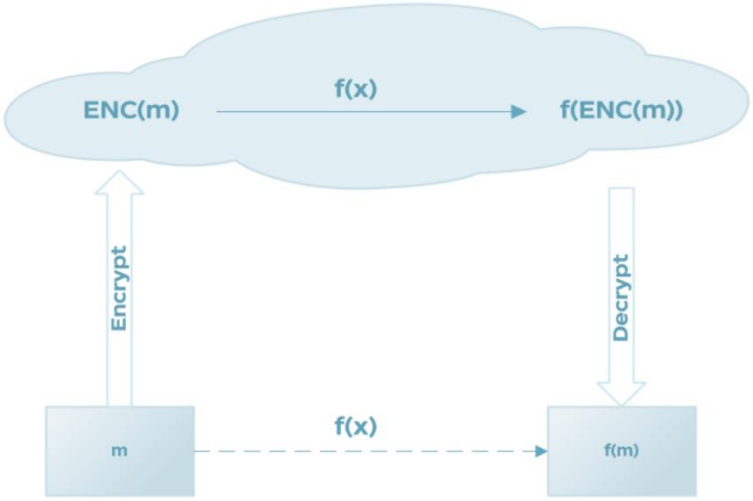

图3　同态加密算法

5.2　同态加密算法

基于联盟链Fabric与多通道机制构建可控的信令网威胁流数据共享环境。联盟链通过认证准入机制建立基础的可控环境，多通道技术在此基础上实现共享数据的隔离，确保数据共享的安全性与可控性。为解决链上存储的高成本和效率低问题，引入IPFS分布式存储系统，构建链上索引与链下数据结合的存储模型，降低存储开销并提升数据管理效率。同时，通过边缘计算技术，将IPFS存储节点动态部署在靠近参与机构的位置，优化数据访问路径，提高数据访问速度和共享效率，从而实现高效、安全、可控的数据共享环境，如图4所示。

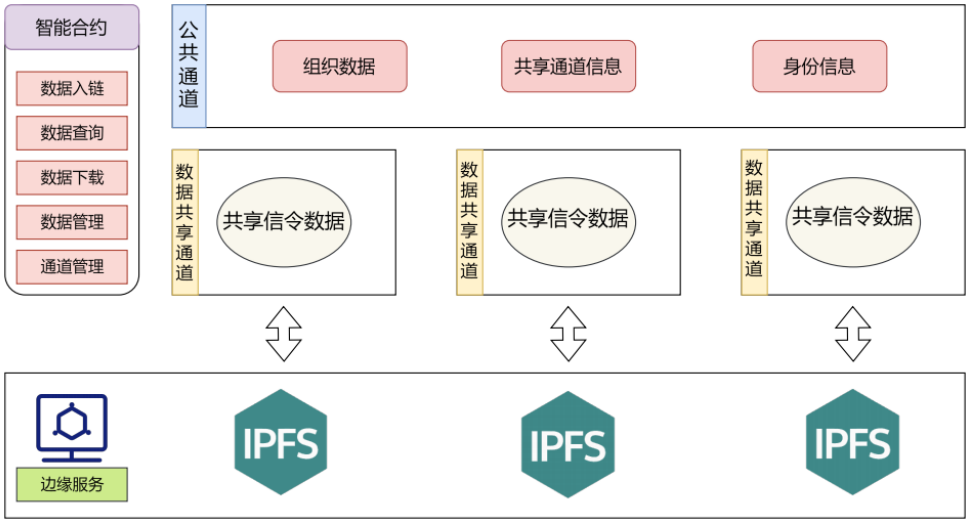

图4　数据共享原理图

5.3　威胁流检测分析原理

基于算法模型和知识图谱技术对信令数据流进行威胁种类检测和行为特征分析。通过比较信令流特征与正常模式的偏离程度或与已知攻击特征的匹配情况，识别异常行为和潜在威胁，生成知识图谱，用于精确描述威胁行为的特性和来源。当信令流表现出异常模式或攻击特征时，将其判断为威胁事件，从而提供有效的技术手段保障5G网络的安全性和稳定性，如图5所示。

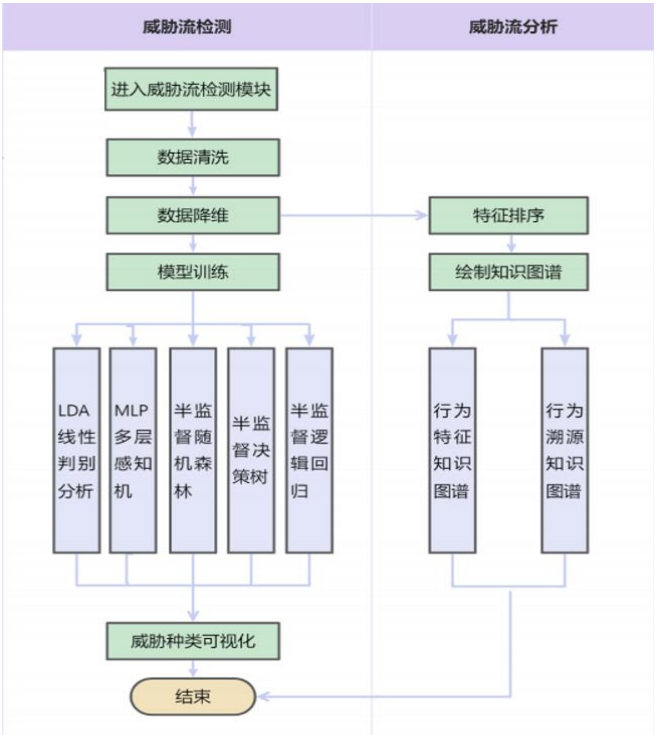

图5　威胁流检测分析原理图

5.4　Hyperledger Fabric 联盟链

Hyperledger Fabric 是一个开源的区块链平台，采用联盟链模式，由一组已知且受信任的参与者共同管理，与公有链和私有链有所不同。其核心是执行-排序-验证（EOV）架构，通过执行、排序和验证三个阶段来高效、安全地处理交易。在执行阶段，交易被模拟和背书；在排序阶段，交易通过共识协

议排序；在验证阶段，根据特定的信任假设进行验证。这种架构不仅提高了性能，还增强了对非确定性和潜在恶意行为的抵抗力。

Fabric 通过访问控制列表（ACL）和成员服务提供（MSP）实现细粒度的权限管理，确保只有授权参与者可以读取或写入账本，同时支持跨组织的数据共享和协作。多通道架构是其显著特点，允许在同一区块链网络上创建多个逻辑隔离的通道，每个通道拥有独立的参与者和智能合约，满足多场景需求。此外，Fabric 采用只追加的区块链和快照机制，保证数据的不可篡改性、高效访问和验证。

Hyperledger Fabric 提供了一种灵活、安全和高效的区块链架构，适用于需要隐私保护、多样化场景和高性能的分布式系统应用。

6 信令数据生成与仿真

6.1 正常信令流数据模拟生成

通过5G 核心网信令风暴仿真测试平台（XPRO 仪表）、开源软件 Free5GC 平台、UERANSIM 模拟器以及 Kali 平台，以模拟生成接近真实的 5G 核心网控制面信令流数据。

正常信令流的模拟生成一方面通过 XPRO 仪表仿照现实网络环境进行配置 AMF、SMF、AUSF、UPF、GNB 网元和 UE，并根据具体需求进行信令负载配置，可以仿真5G 环境；另一方面通过搭建 Free5GC 平台模拟核心网，UERANSIM 模拟网络终端和基站，并通过一定的配置使三者可以互连互通，模拟 UE 、gNB 以及核心网元之间的交互，可以模拟 5G 网络中的各种信令流程，如用户设备 UE 的接入、用户身份的认证、鉴权过程以及数据连接的建立等。这些模拟的信令流数据严格遵循 3GPP 5G 标准，确保了数据的标准化和兼容性。

6.2 异常信令流数据模拟生成

在异常信令流数据的获取方面，主要采用三种方法：

a) 使用 XPRO 仪表可以构建相应的信令风暴业务模型和流量触发，仪表架构如图 6 所示：如 5G UE 上下线、Paging（UE 和网络触发）、多 PDU 会话、Xn 切换、N2 切换、4/5G 互操作以及 PDU Session Modify 等业务组合流程的仿真，如图 6 所示。

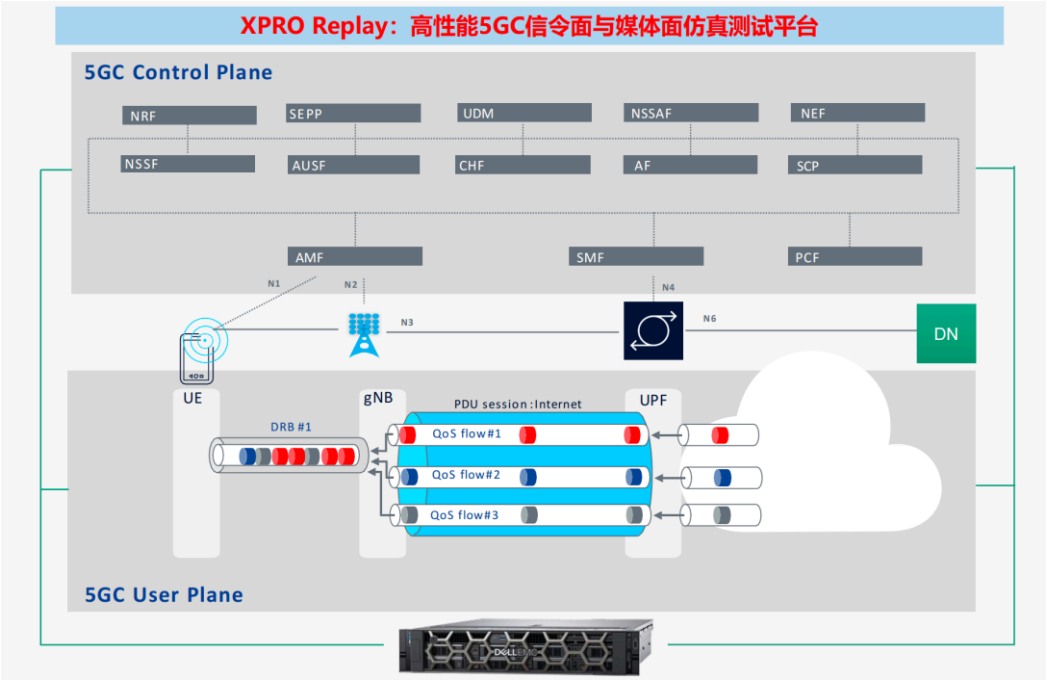

图6 XPRO 仪表架构

b) 基于 Free5GC 和 Kali 攻击系统，在实验环境下模拟外部攻击者发起对核心网的 DDoS 攻击行为，如 ICMP Flood、UDP Flood、SYN Flood 等 DDoS 攻击，并采集分析攻击流量。

c) 基于 Free5GC 实验环境提供的 openAPI，通过深入研究通信信令网的各网元通信机理，对网元通信接口进行分析，利用 5G 通信内部接口间的权限漏洞，推演潜在的逻辑威胁成因，从而发现控制面的异常信令数据。具体的异常信令流数据如下：

1) 基于缺乏身份验证的漏洞，恶意攻击者可以根据此漏洞进行核心网网元数据的窃取。通过伪造一个随机身份，恶意攻击者能够成功冒充合法用户或网元来实现对核心网的非授权访问。访问成功后将会导致网络中的敏感信息和配置数据的曝光，给网络的安全性和隐私保护带来极大威胁。

2) NRF 网元没有实现对请求来源进行有效检查，恶意攻击者根据此漏洞可以冒充 AMF 节点来请求 NRF 网元中存储的关键数据。此类攻击绕过了 5G 核心网的防御机制，攻击者可获得用户数据和网络配置数据。这种敏感信息的获取可能引发用户隐私泄露和网络安全的进一步威胁，同时，攻击者还可将这些数据用于其他恶意活动。

3) 网元接口权限检查缺失的漏洞，会导致恶意攻击者对核心网的虚假 AMF 攻击的风险。通过伪造 AMF 节点加入到网络中并发送删除其他 AMF 节点的请求，攻击者能够绕过权限控制，对核心网实施破坏性操作。此类攻击可能导致核心网的服务中断、网络故障或数据丢失，严重威胁了信令网的可用性和稳定性。

6.3 数据流捕获

在数据流捕获与分析方面，通过使用Wireshark网络协议分析工具对模拟生成的信令流数据进行实时捕获和深入解析。Wireshark能够全面记录网络中的数据包，包括协议类型、源地址、目标地址、数据包长度以及时间戳等信息。在捕获数据的基础上，进一步分析异常信令流中的具体行为特征，例如数据包重复、丢失、异常长度或非法请求等。同时，在模拟的攻击环境下，通过对DDoS攻击流量特征的提取，识别了ICMP Flood、UDP Flood和SYN Flood等攻击的关键模式。这些捕获的数据为后续的异常检测算法开发和安全防护机制的优化提供了高质量的数据支撑。

7 数据加密玉隐私保护

7.1 概述

数据加密与隐私保护是保障数据安全的重要技术手段，贯穿数据的采集、传输、存储及使用的全生命周期。在大数据和云计算等复杂数据环境中，数据加密技术、访问控制策略和隐私保护算法共同构成了防范数据泄露、篡改及未经授权访问的关键防线。本章规定了数据加密与隐私保护的技术要求和应用规范，并明确了适用于不同场景的具体实施方案。

7.2 数据加密技术

7.2.1 加密目标

数据加密技术的主要目标是确保数据在采集、传输、存储和使用过程中的机密性、完整性及不可抵赖性。通过有效的加密手段，防止未经授权的访问，保护数据不被篡改和泄露。如下图所示，数据隐私保护模型结合了AES加密、Paillier加密算法和区块链节点，以确保数据的安全性。业务层使用AES加密保护数据的机密性和完整性，计算层通过Paillier加密算法保护数据隐私，并支持加密计算。区块链节点通过智能合约管理加密数据,确保数据不可篡改,并提供可验证性。此模型有效防止未经授权的访问，确保数据的机密性、完整性与安全性，如图7所示。

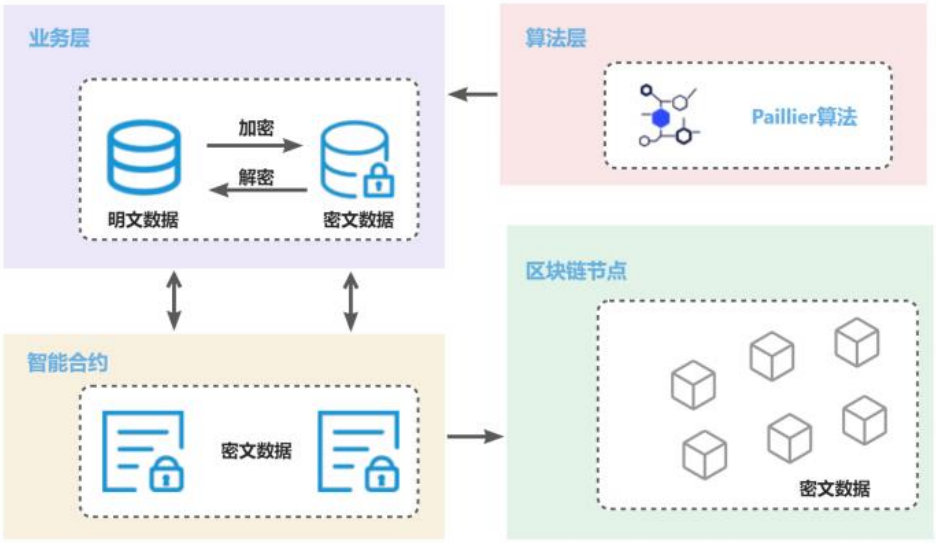

图7　数据隐私保护模型图

7.2.2　加密算法

推荐采用经国家密码管理机构批准的加密算法，以保证安全性和合规性，具体包括以下几种：

——对称加密：推荐使用 AES 算法，用于高效加密大规模数据。AES 算法具有加密速度快、资源占用少等特点，适用于文件存储和批量数据传输的场景。

——非对称加密：推荐使用 RSA 算法，适用于密钥交换和敏感数据加密。非对称加密因其高强度安全性，常用于加密敏感信息如身份凭证。

——同态加密：支持在加密状态下直接对数据进行计算，适用于隐私保护计算和多方协作计算场景。

Paillier 加密算法作为一种同态加密算法，能够在不解密数据的情况下进行计算，非常适合隐私保护计算场景。Paillier 加密算法首先从公钥中提取和，生成随机数，确保它是在范围内的整数，通过下面公式计算密文：

$$C = (g^m \ ?r^n)\bmod n^2 \quad \text{.....(1)}$$

式中：g 为公钥中的参数

M 为明文信息

C 为加密后的密文

密文可以发送给接收方，进行解密操作以获得原始的明文消息。基于 Paillier 的加密算法见示例 1 和示例 2。

示例 1：

Algorithm 7.1 基于 Paillier 加密算法

Input: 明文m ,公钥(n,g)

Output: 密文 C

1：**procedure** $\mathrm{P}_{\mathrm{AILLIER}}\mathrm{E}_{\mathrm{NCRYPT}}(m\ public\_key)$

2:　　$(n,g)\neg\ public\_key$

3:　　Choose a random r such that 1 < r < n and r is coprime with n

4: Compute ciphertext $C \quad (g^m \quad r^n) \bmod n^2$

5: **return** C

6: **end procedure**

示例 2：

Algorithm 7.2 基于 Paillier 加密的单个属性加密算法

Input: 属性名称 attr_name，属性值 attr_value，公钥(n, g)

Output: 加密后的属性值 enc_attr_value

```
1：procedure PAILLIERATTRIBUTEENCRYPTION (attr_name, attr_value, public_key)
2：    if attr_name = “Src IP” then
3：        enc_attr_value ← PaillierEncrypt(attr_value, public_key
4：    else if attr_name =“Dst IP” then
5：        enc_attr_value ← PaillierEncrypt(attr_value, public_key)
6：    else if attr_name =“Dst Port” then
7：        enc_attr_value ← PaillierEncrypt(attr_value, public_key)
8：    else if attr_name =“Protocol” then
9：        enc_attr_value ← PaillierEncrypt(attr_value, public_key)
10：   else if attr_name =“Timestamp” then
11：       enc_attr_value ← PaillierEncrypt(attr_value, public_key)
12：   end if
13：   return enc_attr_value
14：   end procedure
```

7.2.3 应用要求

数据在传输和存储过程中应全程加密，以防止信息泄露。

系统应支持加密算法的动态更新，以应对新型安全威胁。

密钥管理需采用分布式密钥管理机制，确保密钥的高安全性和高可用性，避免单点失效。

7.3 数据访问控制

7.3.1 控制目标

实现对信令数据访问的严格控制，确保只有授权用户或系统模块能够访问特定数据，防止数据泄露和非法使用。

7.3.2 数据访问控制

基于角色的访问控制（RBAC）：按照用户在系统中的角色分配权限，例如系统管理员、数据分析员、普通用户分别具有不同的数据访问权限。

基于属性的访问控制（ABAC）：通过用户属性和数据属性动态调整权限，适应更复杂的访问需求场景。

区块链智能合约：结合区块链技术，利用智能合约记录和验证访问行为，实现访问过程的透明性和不可篡改性。

7.3.3 应用要求

系统应支持访问权限的动态调整，以适应用户角色和业务需求的变化。
所有访问行为必须记录在系统日志中，并定期对访问记录进行审计。
对敏感数据的访问应支持双重认证或审批流程，进一步提升安全性。

7.4 身份认证与权限管理

7.4.1 认证目标

通过身份认证和权限管理，确保信令数据的安全访问和操作合规性。

7.4.2 身份认证机制

包括以下方式：

a) 单因素认证：采用密码或数字证书的方式进行基础身份验证。
b) 多因素认证：结合密码、生物特征和物理设备，增强认证的安全性。
c) 基于零知识证明的认证：允许用户证明其身份合法性，而无需透露具体的身份信息，从而保护用户隐私。

7.4.3 权限管理

权限分配应遵循最小权限原则，仅授予用户完成其工作所需的最低权限。
系统应支持权限的分级管理和动态调整，满足多层次权限需求。
定期审查权限分配情况，撤销不再需要的权限以减少安全风险。

7.5 数据完整性验证

7.5.1 验证目标

数据完整性验证的主要目标是确保数据在传输、存储和使用过程中的一致性，防止因攻击、错误或意外操作导致的数据篡改或损坏。

7.5.2 验证技术

包括以下方式：

a) 哈希算法：使用 SHA-256 等哈希函数生成数据摘要，用于快速检测数据完整性。
b) 数字签名：结合非对称加密技术，验证数据来源的合法性及数据内容的完整性。
c) Merkle 树结构：在分布式存储环境中，利用 Merkle 树实现多层次的数据完整性校验。

7.5.3 应用要求

对存储和传输的关键数据应定期进行完整性校验，并形成自动化流程。
数据完整性异常时，系统需实时告警并记录异常日志，便于后续追溯。

7.6 零知识证明

7.6.1 原理

零知识证明是一种密码学技术，允许证明方在不透露具体数据内容的情况下，向验证方证明某一声明的真实性。例如，证明用户的身份符合要求，而无需透露具体的身份信息。

7.6.2 应用场景

包括以下场景：

a) 用户身份验证：用户可在不披露个人详细信息的前提下完成身份验证，适用于隐私保护要求较高的场景。
b) 数据共享：在数据共享场景中，数据提供方可证明数据合法性，而无需暴露数据的具体内容。
c) 敏感计算：在医疗、金融等行业，零知识证明可以验证计算结果的正确性，而不泄露输入数据。

7.6.3 技术要求

零知识证明算法应支持交互式和非交互式协议，以适应不同的应用场景。

认证过程需具备高效性，能够满足实时性要求。

7.7 数据存储与传输加密

7.7.1 数据存储安全

数据存储过程中应采用静态加密技术保护其机密性，推荐使用AES算法对静态文件进行加密。

为提高存储可靠性和抗灾难能力，应采用分布式存储系统（如IPFS）存储数据，并设置多副本冗余策略。

7.7.2 数据传输加密

数据传输层应采用TLS或IPSec协议进行加密，确保传输过程中的数据安全性。

传输过程中应支持动态密钥更新机制，避免因密钥泄露导致的安全风险。

在高敏感性场景下，可结合量子安全加密算法，增强数据的抗破解能力。

8 数据共享与检索

8.1 数据共享

8.1.1 数据上传

系统需提供数据上传功能，允许具有共享权限的用户将本地数据上传至共享系统中，以实现数据共享。上传接口应支持多种文件格式，如 .pdf、.docx、.csv、.jpg、.png 以及大文件的上传，单个文件最大支持 1GB。同时，系统应支持多文件批量上传功能，总大小限制可根据业务需求调整。

上传时序图如图8所示上传过程中应对数据进行 AES-256 实时加密，每次上传生成唯一密钥用于文件内容的加密处理，密钥需通过 RSA 公钥加密后安全存储。传输过程需采用 HTTPS 协议，使用 TLS 1.3 或更高版本确保数据传输安全性。上传文件完成后，系统需对文件生成 SHA-256 哈希值，用于后续完整性校验，并对上传记录进行日志化存储，包括上传时间、用户 ID、文件名称和大小等信息，便于后续管理与追踪。如图8所示。

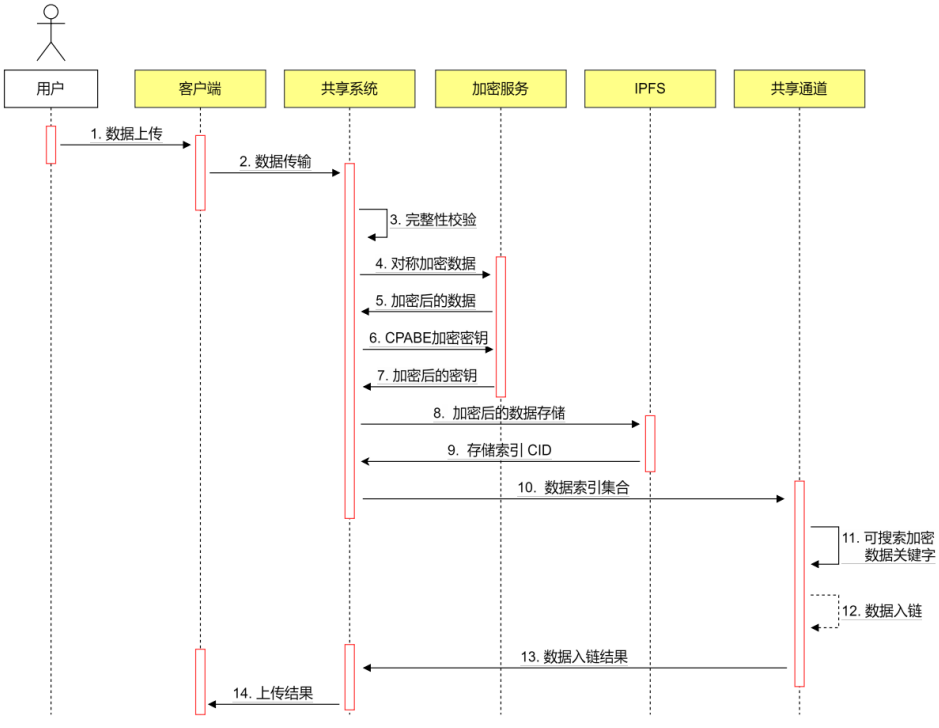

图8 数据上传时序图

8.1.2 数据下载

系统需提供数据下载功能，允许具有访问权限的用户从共享系统中选择并下载所需数据文件至本地。下载接口和界面应支持按需选择文件，并可显示文件基本信息（如文件名称、大小、格式和上传时间）。

为保证数据安全性，下载过程中需对文件内容进行传输加密（使用 HTTPS/TLS），并验证下载数据的完整性，确保文件未被篡改。系统应根据访问者的权限控制下载范围，未授权用户无法下载文件。每次下载需生成访问日志，包括访问者 ID、下载时间、文件名称和大小等信息，供数据提供者了解其共享数据的使用情况。

8.1.3 数据检索

系统需提供多种方式的数据检索功能，以方便用户快速定位所需的数据文件。检索方式包括但不限于：

a) 通过数据 ID 检索：用户可通过文件的唯一标识符（ID）直接精确定位到单项数据，避免检索误差。
b) 通过关键词检索：系统应支持基于文件名称、描述、上传者、日期或其他标签的关键词模糊检索功能，并按相关度返回符合条件的多项数据。
c) 权限限制： 检索功能应基于用户权限，仅返回用户有权访问的数据文件，屏蔽无权限数据。

系统还需在每次检索成功时生成访问日志，记录访问者 ID、访问时间、检索关键词及结果等信息，便于数据提供者监控其数据的访问和使用情况。

8.1.4 完整性校验

系统需提供完整性校验功能，以确保数据在上传、下载和存储过程中未被篡改。具体实现包括：

a) 文件上传校验：在上传完成后对文件内容生成 SHA-256 哈希值，并与本地文件的哈希值进行比对，确认文件内容一致性。
b) 文件存储校验：系统定期对存储中的文件进行哈希校验，确保存储过程中数据未被修改或损坏。
c) 文件下载校验：在用户完成下载后，系统需生成下载文件的哈希值并与存储中的哈希值比对，确保下载数据的完整性。

若发现完整性校验失败，系统需立即向管理员发送警告通知，记录相关文件信息和操作详情，并在用户界面提示操作失败，避免使用被篡改的数据。

8.2 共享通道

8.2.1 创建通道

多通道技术是实现信令数据可控共享的重要标准。用户可以根据自身需求创建多个独立的数据共享通道，每个通道都允许用户定义数据共享范围和相关规则，以确保数据的安全性和隐私性。

标准要求通道的创建应具备以下能力：

a) 支持独立配置：每个通道可独立设置共享范围、参与节点、共识规则和出块策略，以满足不同的业务需求。
b) 严格权限控制：在创建通道时，需明确规定通道成员的访问权限，避免数据被未授权的成员访问。
c) 配置透明：通道的配置应可记录并公开在联盟链的公共部分，以便其他授权成员了解通道存在及其基本配置信息。

每个通道应被视为一个独立的逻辑区块链，通道成员在其中共享数据的同时，不会对通道外的成员产生信息泄露的风险。通道创建的流程图如图9所示。

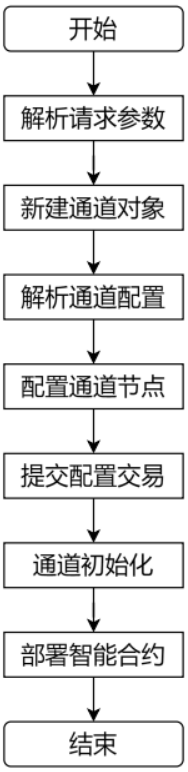

图9　创建共享通道流程图

8.2.2　通道管理

通道的灵活管理是数据共享标准的重要部分。用户应能动态调整通道配置，以适应数据共享需求的变化。标准要求通道管理包括以下功能：

a) 成员管理：用户可动态调整通道成员，包括添加或移除成员，以及调整成员的访问权限级别。
b) 共识规则修改：系统应支持通道共识算法的动态调整，例如从 RAFT 改为 PBFT，以满足不同业务场景下的性能要求。
c) 配置变更记录：所有对通道配置的修改操作（如成员调整、共识规则修改等）应生成完整的日志，记录操作时间、操作人及变更内容。

通道管理功能应具备高适应性，满足不同业务规模和需求场景的调整能力，同时确保变更操作的安全性和可追踪性。

8.2.3　通道配置查看

系统提供实时可视化的通道配置查看功能，方便用户全面了解通道的运行状态。用户应能随时查看通道的基本信息、参与成员、共识算法以及共享数据范围等详细配置。此外，通道还需支持区块数据的解析与查询功能，帮助用户获取通道内的区块信息和交易记录。通过直观的可视化界面，用户能够快速了解当前通道中的数据共享情况，掌握通道运行的整体状况。

8.2.4　通道数据查看

基于联盟链的技术特点，在共享通道中采用双重认证机制。首先，组织需获得公共通道的授权，才能进入系统并了解网络中的基本配置信息。其次，组织需获得数据共享通道的授权，方可访问通道内的共享数据。这种机制确保了数据共享权限的分级管理，仅加入公共通道的组织可查看网络公共信息，而只有加入特定数据共享通道的组织才具有获取相关数据的权限。通过双重认证和通道隔离技术，标准为信令数据的可控共享提供了高效、安全的解决方案。

8.2.5　智能合约管理

智能合约是数据共享和业务逻辑自动化的核心。系统提供智能合约的部署、升级和管理功能，确保智能合约在通道中的一致性和有效性。用户可以通过界面方便地管理智能合约的生命周期，包括安装、实例化、升级和版本控制。同时用户还可以自定义部署智能合约，实现个性化的业务逻辑和数据共享。

8.3 信令数据管理

8.3.1 基本信息管理

需提供对共享数据的基本信息进行管理的功能，用户可以维护共享的信令数据的元数据信息，包括数据名称、类型、关键字、描述等，确保数据的完整性和可追溯性。

8.3.2 访问策略管理

需支持数据访问策略的定义和管理，用户可以根据不同信令数据的共享需求，制定细粒度的访问控制策略。通过配置访问权限，用户可以控制谁可以访问数据，确保数据的安全性和合规性。

8.3.3 共享状态管理

需支持数据访问策略的定义和管理，用户可以根据不同信令数据的共享需求，制定细粒度的访问控制策略。通过配置访问权限，用户可以控制谁可以访问数据，确保数据的安全性和合规性。

8.3.4 访问日志

系统需记录所有信令数据访问的日志信息，包括访问时间、访问者、访问操作、访问结果等。用户可以通过访问日志进行审计和分析，追踪数据访问行为，检测异常访问活动，确保数据的安全性。

8.4 身份管理

8.4.1 身份注册

身份注册功能要求用户提交正确的身份材料，并确保材料的真实性和合法性。系统管理员负责审核用户提交的身份材料，核实用户身份的真实性和完整性。审核通过后，系统将基于预设定的程序为用户生成身份证明，该证明可用于后续的身份验证，并且该身份证明不会泄露用户的隐私信息。

8.4.2 身份验证

身份验证功能是用户在共享系统中进行操作前验证自己身份的过程。用户需使用身份注册时得到的身份证明进行验证，系统将通过验证身份证明的有效性来确认用户身份。此功能旨在确保系统中的操作只能由合法身份的用户执行，提高系统的安全性和可信度。

8.4.3 身份更新

身份更新功能允许用户在需要时可以更新自己的身份信息。用户可以通过系统界面修改信息并提交更新请求，并提供新的身份材料进行验证。权威身份验证机构的管理员将对更新请求进行审核，核实用户提交的新身份信息的真实性和合法性。审核通过后，系统将更新用户的身份信息，并重新生成相应的身份证明，以确保用户身份的及时更新和有效性。

8.4.4 身份信息管理

系统应提供安全高效的身份信息管理功能，并且不能泄露用户隐私，因此身份信息管理功能主要是针对验证身份的材料进行管理。系统应确保这些信息的安全存储和访问控制，防止未经授权的访问和信息泄露。

8.5 联盟链管理

8.5.1 公共通道管理

用于创建和管理联盟链中的公共通道。系统管理员可以定义通道的参与组织、共识算法和出块策略等配置，并动态调整通道的配置参数。公共通道记录的是共享系统的参与组织、数据共享通道现状等公共信息，以帮助用户对共享系统的现状进行全面的了解。

8.5.2 联盟组织管理

组织管理功能用于管理参与联盟链的各个组织。系统管理员可以添加、删除或更新组织信息，分配组织的角色和权限，确保每个组织在联盟链中的合法参与。通过有效的组织管理，可以保证共享系统的稳定性和安全性。

8.5.3 节点管理

节点管理功能用于管理联盟链中的节点，包括节点的注册、配置和监控。系统管理员可以添加新节点、更新节点配置，并监控节点的运行状态和性能。通过节点管理，可以确保联盟链的高可用性和可靠性。

9 分布式存储管理

9.1 分布式存储架构要求

9.1.1 架构设计目标

9.1.1.1 高可用性

分布式存储系统需支持高可用架构，确保数据存储和访问的连续性，避免单点故障。

9.1.1.2 扩展性

系统应支持按需扩展，满足5G核心网日益增长的数据存储需求。

9.1.1.3 容错性

具备强大的容错能力，通过数据副本和节点冗余保障数据的可靠性。

9.1.2 架构设计要求

1.多节点分布：数据应分布存储于多个节点，避免因单节点故障导致数据丢失。

2.数据分片与副本：系统应采用数据分片和副本策略，确保数据的高可靠性；建议副本数量不少于3个。

3.元数据管理：元数据需集中存储，确保对数据分布信息的快速访问与管理。

4.存储类型支持：系统应支持多种存储类型，满足不同应用场景需求。

9.2 数据存储与访问控制

9.2.1 存储权限管理

9.2.1.1 角色分级权限

不同角色应设置不同的存储访问权限，避免越权访问。

9.2.1.2 细粒度权限控制

基于用户、数据类型和操作类型实现不同权限分配。

9.2.2 访问控制机制

9.2.2.1 身份认证

访问存储数据时需通过强身份认证（验证用户身份。

9.2.2.2 访问加密

所有访问操作需通过安全传输协议（如HTTPS、TLS）进行加密，防止数据被窃取或篡改。

9.2.2.3 零信任机制

数据存储和访问需基于零信任原则，动态验证用户身份和操作权限。

9.2.3 访问日志与审计

9.2.3.1 访问日志记录：

记录所有存储数据的访问行为，包括访问时间、用户、数据对象及操作类型。

9.2.3.2 日志审计：

定期对访问日志进行审计，发现异常访问行为并及时处理。

9.3 数据可靠性与完整性

9.3.1 冗余与容灾策略

为了确保数据的高可靠性，系统设计了多副本冗余存储策略，将同一数据分片存储至多个节点。结合地理位置分布的跨区域容灾方案,即使某一区域的存储节点出现故障,也能快速从其他区域恢复数据。

9.3.2 篡改检测技术

基于区块链技术，系统通过存储数据的哈希值实现篡改检测。每次文件变更都会更新其哈希值并记录至区块链中,同时结合数字签名技术记录修改者的身份信息,确保数据变更过程的透明性和可追溯性。

9.3.3 完整性校验方法

系统定期运行哈希值校验算法，检查存储数据的完整性。采用Merkle树结构验证数据的完整性，配合分布式一致性校验机制，确保多节点环境下的数据同步与一致。

9.4 存储性能与效率优化

9.4.1 检索性能优化

为提升加密数据的检索效率，系统采用公钥可搜索加密技术和分布式索引机制。在分布式环境中，分层索引结构能有效减少跨节点查询的延迟。

9.4.2 吞吐量与延迟优化

系统通过智能负载均衡技术优化数据请求的分配策略，确保每个节点的处理负载均匀。结合边缘缓存技术减少远程存储访问次数，从而降低数据访问延迟。

9.4.3 资源利用效率

结合数据压缩与分片存储技术优化资源使用效率,节点间的协同调度算法可动态调整存储任务分配,避免资源浪费。

9.5 数据隐私保护措施

9.5.1 加密与隐私技术

同态加密技术用于数据加密存储，实现加密数据的直接计算操作，避免解密过程中的隐私泄露。差分隐私技术则用于数据统计分析，保护敏感数据免受推断攻击。

9.5.2 安全传输保障

传输过程中采用TLS/SSL协议，确保数据的机密性与完整性。同时支持量子安全加密算法，以应对未来量子计算的威胁。

10 威胁流检测与分析

10.1 范围

包括数据预处理、威胁检测流程、异常行为分析、威胁溯源等内容，其流程图如图10所示。

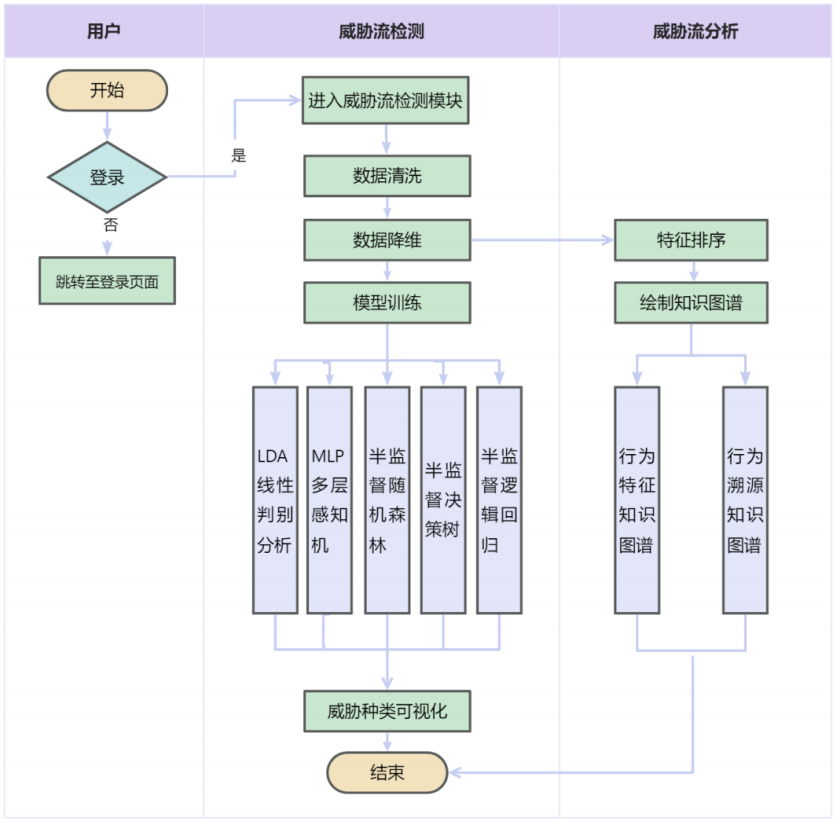

图10　威胁流检测分析模块流程图

10.2　数据预处理

10.2.1　数据采集要求

10.2.1.1　正常数据采集

使用仿真工具XPRO和Free5GC模拟真实网络环境，生成标准化信令流数据，需涵盖控制面和用户面网元的交互数据。

采集数据应包括但不限于以下信息：协议类型、源地址、目标地址、时间戳、数据包大小等。

信令流数据需符合3GPP相关协议标准。

10.2.1.2　异常数据采集

基于仿真平台模拟攻击流量，比如DDoS、中间人攻击等，并捕获攻击特征数据。

使用合法实验环境下的攻击工具Kali Linux生成并记录常见攻击数据。

10.2.2　数据清洗要求

清除数据中的重复记录和噪声数据，确保数据集的质量。

针对缺失字段的数据记录，明确处理方法，可选补全或剔除。

数据时间戳需同步至统一的时钟参考，保证时间序列一致性。

10.3　威胁检测规范

10.3.1　检测目标

通过信令数据威胁检测技术，识别和定位潜在的网络威胁，包括但不限于：

a)　网络流量异常行为，如超高频请求或异常数据包格式。

b)　非法访问信令数据，如未经授权的信令操作。

c)　攻击行为特征，包括 DDoS 攻击、伪造身份、伪造信令流量等。

10.3.2 检测方法

10.3.2.1 基于规则的检测方法

定义规则库，需覆盖以下维度，如流量特征、协议特征、时间特征等。

规则库需定期更新，以应对新的威胁特征。

10.3.2.2 基于机器学习的检测方法

建议引入经过训练的分类或聚类模型，如监督学习模型随机森林或无监督学习模型K-Means，以提升异常检测的准确性。

所选模型应定期更新和校准，确保检测效果。

10.3.2.3 自定义检测方法与模型规范

10.3.2.3.1 小波模型

要求如下：

a) 适用场景：适用于捕捉信令流量的时频特性变化，如突发异常和频率波动；
b) 模型原理：利用小波变换对信令流数据进行分解和重构，从时域和频域识别潜在威胁；
c) 实现要求：对信令流数据采用固定时间窗口，进行小波分解。通过多分辨率分析定位信令流的突变点，并标记潜在异常行为，然后对检测出的异常信令进行特征分类和进一步分析。

10.3.2.3.2 小样本模型

要求如下：

a) 适用场景：针对数据样本不足的场景，尤其是稀有攻击类型的检测；
b) 模型原理：基于迁移学习和数据增强技术，使用小样本训练模型，并通过特征提取提升检测效果；
c) 实现要求：在小样本条件下，利用已知数据的相似特征构建迁移学习模型，并使用对抗生成网络生成更多样本以弥补数据不足。

10.3.2.3.3 SGM-CNN 模型

要求如下：

a) 适用场景：高维度、多样化信令数据的复杂威胁检测；
b) 模型原理：使用卷积神经网络提取信令数据的深层特征；结合 SGM 生成特征优化表示，利用改进的分类层实现对异常信令的高精度检测；
c) 实现要求：数据输入需标准化，格式为固定时间窗口内的流量矩阵。模型参数需通过交叉验证方式优化，确保检测准确率达到 90%以上。

10.3.2.3.4 多解释方法融合模型

要求如下：

a)适用场景：检测结果解释与特征排序，用于辅助决策和威胁溯源；

b)模型原理：通过融合 SHAP、LIME 和 ELI5 方法，生成特征重要性排序。通过融合不同解释方法的结果，避免单一方法的偏差，形成综合可信的解释；

c)实现要求：输出需包括特征重要性排序及其对应分数。特征排序应以可视化方式呈现，辅助研究人员理解模型结果。

10.3.2.4 检测流程

流程包括：

a) 数据采集与预处理；
b) 多模型检测；
c) 结果输出与分析。

10.4 异常行为分析

10.4.1 分析目标

通过对检测出的异常信令数据进行分析，确认威胁行为的性质、影响范围和潜在来源，为后续处置提供依据。

10.4.2 分析步骤

包括：

a) 行为模式分析：比对异常信令流与正常信令流的统计特性，提取关键行为模式。
b) 协议字段分析：深入解析信令数据的协议字段，定位可能的异常字段。
c) 历史数据比对：将异常信令数据与历史攻击特征数据进行比对，判断是否匹配已知威胁模式。

10.4.3 输出要求

分析报告需包含威胁行为描述、可能的影响范围、建议的应对措施等。

10.5 威胁溯源规范

10.5.1 溯源目标

通过分析异常数据和网络日志，定位威胁事件的发起源、攻击路径以及涉及的关键节点。

10.5.2 溯源方法

基于区块链记录的溯源：依托区块链技术，对信令数据的操作日志进行回溯，确定异常行为的触发源。

关联分析：利用网络拓扑数据、时间戳和异常事件特征，逐步追踪威胁来源。

10.5.3 输出要求

溯源报告需包括：

a) 威胁源的详细描述，IP 地址、设备信息等。
b) 攻击路径示意图。
c) 相关异常行为的分析说明。

11 建立可视化展示平台

11.1 数据库建立

使用标准化工具 PowerDesigner 或 ERwin进行 ER 模型设计，明确实体与关系。

信令数据的字段设计遵循驼峰命名法或下划线分隔法，确保字段名语义清晰。

表名使用简洁、明确的命名规则（如模块_功能名），避免歧义。并且需要添加必要的主键、外键及唯一性约束，确保数据完整性。

数据库须配置自动备份策略，建议每日定时全量备份及每小时增量备份。确保定期进行备份恢复演练，确保数据恢复的有效性与完整性。

建议使用UTF-8 字符集。万国码，无需转码，无乱码分险，节省空间。

数据结构应根据实际使用场景选择合适类型。使用分层命名规则，确保键名唯一且具备可读性。

建议禁止在更新十分频繁、区分度不高的属性上建立索引。更新频繁的字段建立索引会大大降低数据库性能。

建议采用分表分库策略。水平分表可根据 ID 或时间字段拆分数据，垂直分表则可将非核心字段拆分至独立表中。分库建议按照模块划分，如用户数据库和订单数据库。

禁止使用 SELECT * 查询，必须明确指定需要的字段，以减少数据传输量。避免嵌套查询，建议使用联表查询优化性能。在 WHERE 子句中避免对字段使用函数处理（如 WHERE YEAR(date) = 2025），以提升查询效率。

数据库连接需通过连接池HikariCP、Druid管理，设置合理的连接池参数：最大连接数、空闲超时时间及最大等待时间，以提高连接复用效率并减少资源消耗。

采用最小权限原则分配用户权限。普通用户仅允许 SELECT 操作，数据管理用户可拥有 INSERT、UPDATE 和 DELETE 权限,而只有管理员可进行数据库 schema 修改。关键操作需经过严格的权限审核。

启用数据库日志功能，记录所有数据变更操作。日志需定期归档，建议保留至少 6 个月的历史数据。启用审计功能，分析访问记录和变更日志，排查潜在的安全隐患。

建议启用表分区功能RANGE 或 LIST 分区。分区策略应根据业务场景设计，如按日期或 ID 范围分区，以提高查询性能和管理效率。

定期清理历史数据，建议将 6 个月前的无用数据归档至备份库。归档表设置只读权限，防止误操作，并减少主表存储压力。

定期设置任务校验数据库数据的一致性。通过事务机制确保多表更新操作的数据一致性，避免因意外中断导致数据出错。

建议使用数据库监控工具Prometheus、Zabbix监控数据库状态，重点监控查询延迟、连接数、索引使用率及锁等待时间等指标，确保数据库的稳定运行。

本标准以“5G核心网信令数据”作为数据库的具体例子，该数据库应兼具为5G核心网信令数据提供快速分析的工具，例如识别正常与异常的信令流量、信令数据的特征导出、信令数据的共享。

11.2 可视化分析平台

11.2.1 信令流数据信息实时显示

系统需支持以高刷新率展示信令数据，确保实时性。

数据展示需提供多维度信息，包括时间戳、来源IP地址、目标IP地址、端口号、协议类型、数据大小等。

平台界面需具备交互性，支持用户点击信令流数据条目，展开查看更详细的信令信息，如完整的消息体内容及其解析结果。

实时异常信令检测：平台集成威胁检测模型，对信令流进行实时分析，识别如非法信令、丢包、延迟过高等异常活动，并自动生成告警。

11.2.2 网元信息实时显示

系统需实时采集并显示每个网元的关键信息，包括但不限于：网元名称、IP地址、端口号、连接状态、处理时延、CPU利用率、内存使用率等性能指标。

平台需支持对每个网元的活动日志进行实时记录和存储，日志内容需包括事件类型、发生时间、影响范围等详细信息，用户可通过时间轴功能快速回溯特定时间段内的网元行为。

支持将网元信息集成到网络拓扑视图中，通过可视化手段展示网元之间的关系与状态，方便快速了解整体网络运行状况。

11.2.3 攻击过程实时显示

攻击过程建议通过分阶段的进度条展示，包括攻击启动、目标发现、信令操控、数据注入等阶段。

在攻击过程中，建议实时捕获所有与攻击相关的信令数据包，并支持信令数据包的分类与标记，便于后续用于威胁发现模型进行分析。

攻击结束后，平台应自动生成攻击分析报告，包含攻击目标、阶段耗时、涉及网元、影响范围及潜在风险等信息。

用户需能够下载攻击过程中捕获的数据包文件，并结合威胁发现特征提取工具进行详细分析。

11.2.4 网元监控

平台需实时获取所有网元的状态信息，包括连接状态、数据吞吐量、处理时延等。当某个网元的状态出现异常时，系统需立即标记，并通过视觉提示告知用户。

平台需具备自动化的安全响应能力，包括隔离受攻击的网元、限制恶意流量、重新分配网络资源等措施，以最大限度降低攻击对核心网的影响。

所有网元的监控数据及安全事件记录需支持长时间存储，便于用户事后进行深度分析或审计。

基于网元的历史运行数据，平台需能够预测未来的状态变化趋势。

附 录 A
（资料性）
实验室工作条件

A.1 实验环境要求

A.1.1 实验软件环境

应安装支持5G核心网仿真的软件环境，包括Free5GC、Open5GS、UERANSIM。要求使用Free5GC版本v3.0及以上，Open5GS版本v2.0及以上，UERANSIM版本v2.0及以上，以确保对最新3GPP中对5G协议的兼容性和支持。

A.1.2 操作系统要求

所有实验设备应运行Linux操作系统，推荐使用Ubuntu 20.04或CentOS 7/8版本，确保软件的兼容性和稳定性。