

安全GPT大模型对关键基础设施运营商的影响 及应对策略探讨

汇报人：蔡逆水

中国电信研究院安全技术研究所 技术总监

#隐私计算

#数据安全

#数字安全

#国际峰会

#元宇宙安全

#云安全

#区块链

#零信任

目录

CONTENTS



**一.安全GPT助力电信
运营商云网安全的原理**



**二.电信运营商建设安
全GPT的必要性**



**三.电信运营商安全
GPT大模型建设的核心
能力要求和主要策略**



安全GPT助力电信运营商云网安全的原理

1. 各类GPT技术发展迅猛
2. GPT对安全影响深刻

1. 各类GPT技术发展迅猛

ChatGPT 是 OpenAI 于 2022 年 11 月推出的一款聊天机器人，它是基于 GPT-3.5 模型的变体，可以在对话中根据上下文形成类似人类的文本响应。与其他使用预定义的响应或规则生成文本的聊天机器人不同，ChatGPT 拥有更强的语言处理能力和生成能力，会根据接收到的输入生成更自然、更多样化的响应。

ChatGPT 的发布让通用性大模型应用达到新的高潮。它可以完成聊天、撰写邮件、文案、代码等任务，应用于自然语言处理、写作辅助、智能对话、语言学习、创意产业、编程辅助等多个领域。

(1) 资料查询好帮手，随身百科全书

遇到知识盲点，快速得到解答 (以下是 安全持久性内存 知识点)

了解CXL吗 @Albus
6 条回复
Albus应用 14 分钟前

了解，CXL是一种新型的计算机总线架构，用于连接中央处理器（CPU）和其他加速器设备，如图形处理器（GPU）和人工智能加速器。CXL可以在高速数据传输和低延迟之间实现平衡，从而提高系统性能和效率。
Not happy with my response? Share issues and feedback for me to improve via the 3-dots menu > Share feedback.
wind 14 分钟前
CXL和原来的架构有哪些优势? @Albus
Albus应用 14 分钟前

CXL相对于传统的计算机总线架构有以下优势：1. 更高的带宽：CXL可以提供高达32 GT/s的带宽，这比PCIe 4.0的带宽高出近3倍。2. 更低的延迟：CXL可以通过直接内存访问（DMA）实现设备之间的数据传输，从而减少了CPU的干预，降低了延迟。3. 更高的效率：CXL支持内存共享，多个设备可以共享同一块内存，从而提高了系统的效率。4. 更灵活的拓扑结构：CXL支持点对点和多级拓扑结构，可以根据不同的应用场景进行灵活配置。5. 更强的安全性：CXL支持硬件级别的安全特性，如加密和认证，可以提供更高的系统安全性。综上所述，CXL的优势主要在于更高的带宽、更低的延迟、更高的效率、更灵活的拓扑结构和更强的安全性，这些优势可以提高系统的性能和可靠性。

CXL和持久内存有什么关系? @Albus
Albus应用 < 1 分钟前

CXL和持久内存都是新型的计算机技术，它们可以结合使用以提高系统的性能和可靠性。持久内存是一种新型的内存技术，它可以将数据持久地存储在内存中，即使系统断电也不会丢失数据。持久内存可以替代传统的硬盘和固态硬盘，提供更高的性能和更低的延迟。CXL可以连接CPU和其他加速器设备，如GPU和FPGA，以提高系统的性能。CXL还支持内存共享，多个设备可以共享同一块内存。这意味着，持久内存可以作为CXL连接的一种设备，与CPU和其他加速器设备共享内存。这样可以提高系统的性能和可靠性，同时也可以减少数据传输的延迟。综上所述，CXL和持久内存可以结合使用以提高系统的性能和可靠性，持久内存可以作为CXL连接的一种设备，与CPU和其他加速器设备共享内存。

持久内存的关键技术有哪些? @Albus
Albus应用 4 分钟前

持久内存的关键技术包括以下几个方面：1. 存储介质：持久内存需要使用一种非易失性存储介质，如3D XPoint、PCM、ReRAM等。这些介质具有较高的存储密度和较低的访问延迟，可以满足持久内存的需求。2. 内存控制器：持久内存需要使用一种特殊的内存控制器，以支持内存的持久性和原子性操作。这些内存控制器需要支持内存映射和内存保护等功能，并且需要与操作系统和应用程序进行兼容。3. 文件系统：持久内存需要使用一种新型的文件系统，以支持内存中数据的持久性和安全性。这些文件系统需要支持快速的数据访问和原子性操作，并且需要与操作系统和应用程序进行兼容。4. 数据管理：持久内存需要使用一种新型的数据管理技术，以支持内存中数据的持久性和安全性。这些技术需要支持数据的快速访问和原子性操作，并且需要与操作系统和应用程序进行兼容。综上所述，持久内存的关键技术包括存储介质、内存控制器、文件系统和数据管理等方面，这些技术需要相互配合，才能实现持久内存的高性能和可靠性。

持久内存目前行业龙头有哪些? @Albus
Albus应用 3 分钟前

目前持久内存领域的行业龙头包括Intel、Micron和Samsung等公司。这些公司都在持久内存领域进行了大量的研发和投资，并推出了自己的持久内存产品。其中，Intel推出的3D XPoint内存和Micron推出的QuantX内存都是比较具有代表性的持久内存产品。这些产品都具有较高的存储密度和较低的访问延迟，可以满足持久内存的需求。同时，这些公司还在持久内存的生态系统建设方面进行了大量的工作，如推出了相应的内存控制器、文件系统和数据管理技术等，以支持持久内存的应用。除了这些公司，还有一些新兴的公司也在持久内存领域进行了研发和投资，如Avalanche Technology、Crossbar和...
查看更多

中国有哪些机构在研究持久内存? @Albus
Albus应用 2 分钟前

中国在持久内存领域也有一些机构在进行研究。以下是一些代表性的机构：1. 清华大学计算机科学与技术系：该系的分布式系统与并行计算实验室一直在持久内存领域进行研究，主要关注持久内存的应用和系统设计方面。2. 中国科学院计算技术研究所：该所的计算机体系结构国家重点实验室也在持久内存领域进行研究，主要关注持久内存的架构和性能方面。3. 上海交通大学计算机科学与工程系：该系的分布式系统与存储实验室也在持久内存领域进行研究，主要关注持久内存的应用和系统设计方面。4. 华为公司：作为一家领先的通信设备和解决方案供应商，华为公司也在持久内存领域进行研究，主要关注持久内存云计算和大数据应用中的应用。5. 阿里巴巴集团：作为一家领先的电子商务和互联网技术公司，阿里巴巴集团也在持久内存领域进行研究，主要关注持久内存云计算和大数据应用中的应用。这些机构在持久内存领域进行了大量的研究和投资，推动了持久内存技术的发展和推广。

中国哪些企业提供持久内存相关产品? @Albus
Albus应用 < 1 分钟前

目前，中国的一些企业也在持久内存领域进行了研究和开发，并推出了相关产品。以下是一些代表性的企业：1. 华为公司：华为公司推出了FusionStorage系列产品，其中包括FusionStorage Flash和FusionStorage Cloud，都支持持久内存技术，可以提供更高的性能和可靠性。2. 浪潮集团：浪潮集团推出了基于3D XPoint技术的持久内存产品，包括PBlaze5 910和PBlaze5 916等系列产品，可以提供更高的性能和可靠性。3. 中兴通讯：中兴通讯推出了基于NVMe-over-Fabric技术的持久内存产品，可以提供更高的性能和可靠性。4. 联想集团：联想集团推出了基于3D XPoint技术的持久内存产品，包括ThinkSystem DM7100和ThinkSystem DM7100F等系列产品，可以提供更高的性能和可靠性。5. 启明星辰：启明星辰推出了基于3D XPoint技术的持久内存产品，包括StarXpand系列产品，可以提供更高的性能和可靠性。6. 中科曙光：中科曙光推出了基于3D XPoint技术的持久内存产品，包括Lightning系列产品，可以提供更高的性能和可靠性。这些企业在持久内存领域进行了大量的研究和投资，并推出了自己的持久内存产品，可以满足不同用户的需求。

(2) 编程设计辅助高效率

Algorithm 1: core algorithm of compliance matrix generation based on AI structured interpretation

```
from collections import defaultdict

class PrivacyPolicyRule:
    def __init__(self, category, structured_format, statement_text):
        self.category = category
        self.structured_format = structured_format
        self.statement_text = statement_text

def create_rule_category_library():
    # 添加隐私政策规则类别到类别库
    rule_categories = ['category1', 'category2', 'category3']
    return rule_categories

def create_structured_format_library():
    # 为每个规则类别创建对应的结构化格式
    structured_formats = {
        'category1': 'structured_format1',
        'category2': 'structured_format2',
        'category3': 'structured_format3',
    }
    return structured_formats

def process_privacy_policy_text(text):
    # 将隐私政策文本拆分为单个规则
    privacy_policy_rules = text.split('\n')
    return privacy_policy_rules

def identify_rule_category(rule_text, rule_categories):
    # 判断规则类别
    for category in rule_categories:
        if category in rule_text:
            return category
    return None

def process_rules(privacy_policy_rules, rule_categories, structured_formats):
    rule_base = defaultdict(list)

    for rule_text in privacy_policy_rules:
        category = identify_rule_category(rule_text, rule_categories)
        if category:
            structured_format = structured_formats[category]
            rule = PrivacyPolicyRule(category, structured_format, rule_text)
            rule_base[category].append(rule)
```

In this implementation, we use a class called PrivacyPolicyRule to represent each rule. We have created a category library and a structured format library, and processed the input privacy policy text. Next, we cycle through each rule, determine its category, select the corresponding structured format, and add the rule to the rule library. Finally, we print out the rule library.

Algorithm2: DBSCAN density-based clustering algorithm

```
import numpy as np
from sklearn.datasets import make_blobs
from sklearn.preprocessing import StandardScaler
from sklearn.cluster import DBSCAN

# 创建数据集
n_objects = 1000
centers = [[1, 1], [-1, -1], [1, -1]]
X, _ = make_blobs(n_samples=n_objects, centers=centers, cluster_std=0.4,
                 random_state=42)
X = StandardScaler().fit_transform(X)

# DBSCAN 参数
eps = 0.5
min_samples = 5

def dbscan(X, eps, min_samples):
    db = DBSCAN(eps=eps, min_samples=min_samples).fit(X)
    core_samples_mask = np.zeros_like(db.labels_, dtype=bool)
    core_samples_mask[db.core_sample_indices_] = True
    labels = db.labels_
    n_clusters_ = len(set(labels)) - (1 if -1 in labels else 0)

    cluster_collections = []
    for i in range(n_clusters_):
        cluster = X[labels == i]
        cluster_collections.append(cluster)

    return cluster_collections

# 聚类结果
cluster_collections = dbscan(X, eps, min_samples)
print(cluster_collections)
```

This implementation uses the DBSCAN algorithm from the scikit learn library. Firstly, we created a dataset containing n objects. Then we set the parameters of the DBSCAN algorithm, such as the neighborhood radius parameter eps and the neighborhood density threshold min_samples. Next, we implemented a function called dbscan, which takes the dataset, neighborhood radius parameters, and neighborhood density threshold as inputs and returns a density based clustering set. Finally, we print out the clustering results.

Algorithm 3: Random Forest

```
import numpy as np
from sklearn.datasets import load_iris
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score

# 加载数据集
iris = load_iris()
X = iris.data
y = iris.target

# 划分训练集和测试集
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3,
                                                  random_state=42)

# 随机森林参数
n_estimators = 100
max_depth = None
random_state = 42

# 实现随机森林模型
def random_forest(X_train, y_train, n_estimators, max_depth, random_state):
    rf = RandomForestClassifier(n_estimators=n_estimators, max_depth=max_depth,
                              random_state=random_state)
    rf.fit(X_train, y_train)
    return rf

# 训练模型
rf_model = random_forest(X_train, y_train, n_estimators, max_depth, random_state)

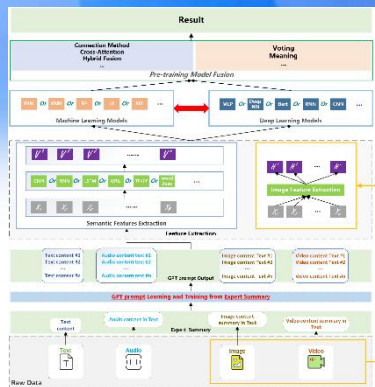
# 预测
y_pred = rf_model.predict(X_test)

# 计算准确率
accuracy = accuracy_score(y_test, y_pred)
print('Accuracy:', accuracy)
```

In this implementation, we used the RandomForestClassifier class from the scikit learn library. Firstly, we loaded the iris dataset and divided it into training and testing sets. Then, we set the parameters of the random forest algorithm, such as the number of decision trees n_Estimators, maximum depth of decision tree max_Depth and Seed Random of Random Number Generators_state. Then, we implemented a method called random_Forest receives training data, number of decision trees, maximum depth and seed of random number generator as input, and returns a trained random forest model. Next, we use the training set to train the model and use the test set to predict the classification results. Finally, we calculate and print out the accuracy of the prediction.

(3) 与通用GPT融合后，提升数据集质量和检测精度

融合



Introduction to commonly used public datasets and GPT extension fusion

No.	Input	Model	Accuracy
201	statement+user information+evidence	Single channel	0.603
202	statement+user information+gpt_evidence	Single channel	0.639
203	statement+evidence+gpt_user_predict	Single channel	0.651
204	statement+user information+evidence+gpt_evidence+gpt_user_predict	Single channel	0.666
205	statement+gpt_user_predict+gpt_evidence	Single channel	0.673
211	statement+user information+evidence	Fusion	0.720
212	statement+user information+gpt_evidence	Fusion	0.743
213	statement+evidence+gpt_user_predict	Fusion	0.781
214	statement+user information+evidence+gpt_evidence+gpt_user_predict	Fusion	0.744
215	statement+gpt_user_predict+gpt_evidence	Fusion	0.786

Data fusion with GPT: a new method for multimodal detection of false information

1 个通用GPT大模型 + 1 个专用GPT大模型

(4) GPT对国家关键基础设施运营商的影响

电信运营商，作为国家关键基础设施运营商，遭遇的安全攻击也是最严重，承载了更多做好安全防护的社会责任和要求

一方面，GPT 应用于安全攻击带来了新的安全威胁，如对于深度伪造的舆情安全威胁。

另一方面，GPT 应用于安全防御展示了 GPT 可以极大提高安全运营的效率，增强企业的安全能力。

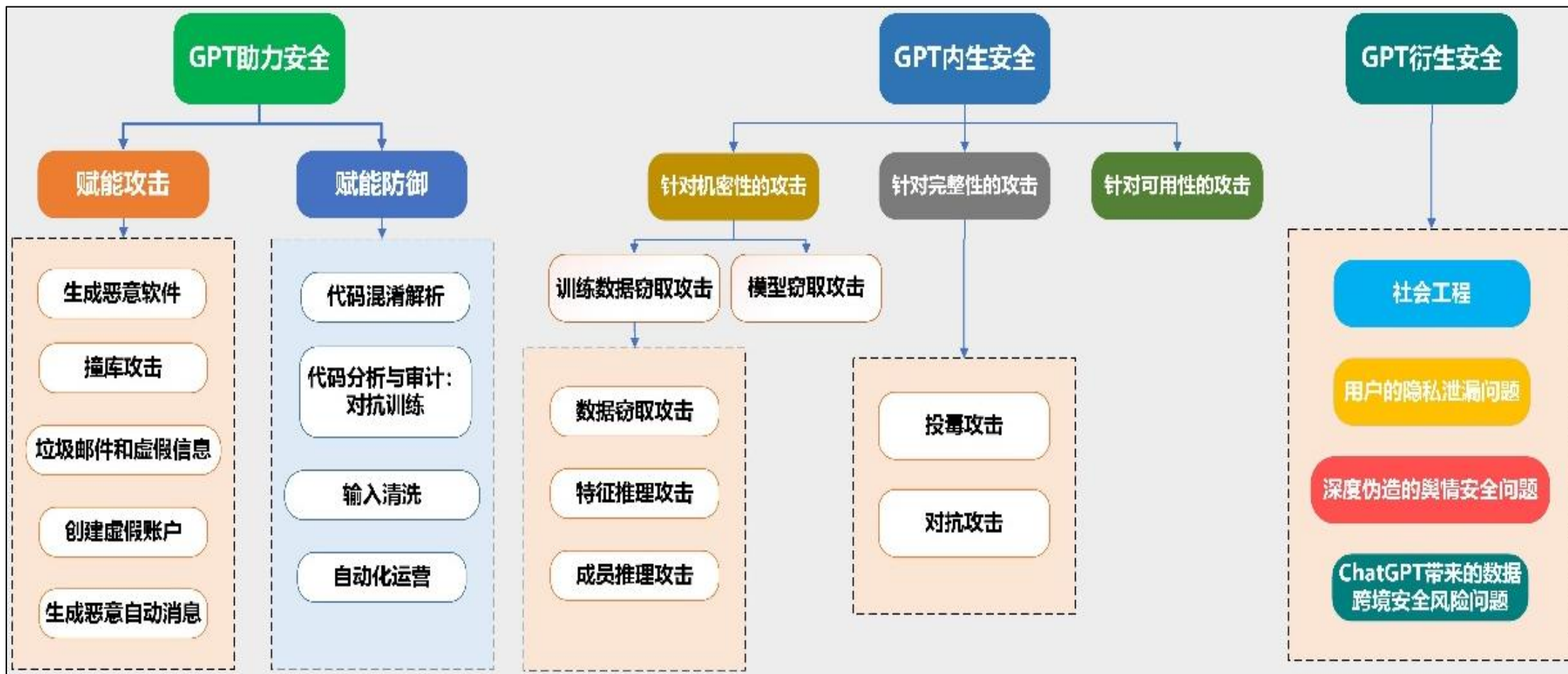
(5) 安全GPT应用产品

在安全领域，GPT 也已经有了较为成熟的应用产品。

国际，2023年3月28日，微软第一个发布了名为**Security Copilot**的新产品，该产品是基于GPT-4和自家训练的安全模型而开发的，旨在为安全人员提供快速、有效的网络安全事件信息收集、潜在威胁挖掘和常见漏洞查找工具。

国内，2023年5月18日，安全厂商深信服发布了国内首个企业级安全GPT云端大模型技术应用深信服安全GPT (**Security GPT**)，通过学习海量网络安全垂直领域专业知识和威胁情报，大幅提升安全检测效果，增强安全运营效率和交互体验。在现场，深信服工作人员演示了安全GPT技术应用在XDR平台上的效果，包括高级威胁检测、安全监测调查、热门漏洞排查等。

2.GPT 对安全影响深刻



(1) GPT 助力安全

GPT技术在网络安全方面具有双重影响。

一方面，利用GPT技术，攻击者能够提升针对性的网络攻击能力：

- **生成恶意软件：** GPT有二进制逆向能力和代码生成能力，攻击者可以利用ChatGPT编写恶意软件说明和指令，从而逃避防病毒软件的检测。
- **撞库攻击：**
- **垃圾邮件和虚假信息：**
- **创建虚假账户：**
- **生成恶意自动消息：**

另一方面，在对抗网络攻击中，合理使用ChatGPT可大幅减少安全运营工作量，作为辅助工具实现以下防御机制：

- 代码混淆解析
- 代码分析与审计
- 对抗训练
- 输入清洗
- 自动化运营

(2) GPT 内生安全

GPT 内生安全围绕着模型安全展开，自身模型安全问题主要包括针对机密性的攻击、针对完整性的攻击和针对可用性的攻击。

1.针对机密性的攻击模型，针对机密性的攻击可以分为训练数据窃取攻击和模型窃取攻击。其中，训练数据窃取攻击可以分为数据窃取攻击、特征推理攻击和成员推理攻击。

数据窃取攻击：在训练阶段，可能会选到由攻击者设计的恶意模型，将训练数据编码到模型参数中，攻击者通过解码参数窃取用户的隐私。在推理阶段，通过原始模型的模型接口进行查询，得到相应的预测结果，利用查询输入和预测结果训练得到一个与原始模型近似的替代模型，基于替代模型逆向恢复原始模型的训练数据。

模型窃取攻击：

特征推理攻击：

成员推理攻击：

2. 针对完整性的攻击模型，常见的针对大模型系统完整性的攻击包括投毒攻击和对抗攻击。

投毒攻击：攻击者通过将精心制作的样本插入训练集中来操纵训练数据分布，以达到改变模型行为和降低模型性能的目的。

对抗攻击：通过向正常样本中添加精心设计的、人类无法感知的噪声来构造对抗样本，从而达到不干扰人类认知而促使机器学习模型对精心构造的对抗样本进行错误判断的目的。

3. 针对可用性的攻击模型，通常发生在系统的推理或运行阶段。由于在推理阶段，系统可能会接收并处理大量的异常输入甚至恶意输入，因此模型的可用性可以成为攻击者的攻击目标，以迫使系统无法提供正常的服务。

(3) GPT 衍生安全

1.社会工程问题，数据安全角度来看，攻击者可以利用从社交媒体或其他来源收集的大量文本数据来训练模型，生成极具说服力的网络钓鱼电子邮件或消息，诱骗受害者泄露敏感信息。

2.用户的隐私泄漏问题，ChatGPT的正常使用需要收集用户账户信息、对话相关的所有内容、以及交互中网页内的各种隐私信息，这些信息在被共享给供应商、服务提供商以及附属公司的过程中，有可能被攻击者截获，导致模型相关的隐私数据泄露，进而泄露用户隐私数据。

3.深度伪造的舆情安全问题，GPT类技术一旦被滥用，可能制造出较传统更以假乱真的文字，图片、声音、音视频等数据类型被深度伪造与合成，导致真实信息被严重歪曲，网络谣言四处传播，安全以及网络公共安全秩序造成极大的冲击。

4.ChatGPT带来的数据跨境安全风险问题

目录

CONTENTS



**一.安全GPT助力电信
运营商云网安全的原理**



**二.电信运营商建设安
全GPT的必要性**



**三.电信运营商安全
GPT大模型建设的核心
能力要求和主要策略**



电信运营商建设安全 GPT的必要性

1. 建设安全GPT有利于快速提升安全能力
2. 电信运营商建设安全GPT大模型的优势

1. 建设安全GPT有利于快速提升安全能力

(1) 提升态势感知能力

威胁情报收集和分析： ChatGPT可以通过分析恶意软件、黑客活动、网络攻击等数据源，生成关于威胁情报的报告，帮助网络安全专家了解当前的威胁和趋势。

安全漏洞挖掘和修复： ChatGPT可以通过对已知的安全漏洞、代码缺陷和配置错误等进行分析和学习，帮助识别和修复类似的问题，提高系统的安全性。

自然语言处理安全： ChatGPT可以用于自然语言处理安全，例如识别和防止恶意语言、欺诈和网络钓鱼等攻击，保护用户的隐私和安全。

网络流量分析和安全监测： ChatGPT可以对网络流量进行分析和学习，识别异常流量和攻击，帮助网络安全人员及时发现和应对安全威胁。

(2) 安全运营机器人

智能安全辅助决策：ChatGPT可以通过学习历史安全事件和安全策略，帮助网络安全团队进行智能决策，提高安全响应的速度和效率。

2. 电信运营商建设安全GPT大模型的优势

在建设安全GPT方面，电信运营商拥有一体化的云网融合技术与综合智能的信息服务能力，在产业数字化演进方面具备丰富的安全技术手段与安全能力。

首先，知识优势。现有的态势感知系统拥有漏洞库、威胁情报库、安全风险判断规则库、AI智能安全模型和算法、重要数据分类分级规则库等，多类型的规则库为安全GPT提供了丰富的训练数据。

其次，数据优势。基于电信运营商的关键基础设施拥有实时流量数据、安全日志数据等，可作为安全GPT模型的优化依据，利用真实的现网流量信息将GPT模型进一步完善。

此外，行业优势。各类垂直行业的差异化应用丰富了现有的安全框架与安全解决方案，为安全GPT模型提供了面向2B的安全能力，增强了安全GPT的覆盖范围与应用场景；在智能化网络方面，电信拥有组网智能、响应智能、管理智能等成果。

最后，科研与创新能力是构建电信运营商的安全GPT大模型的有力支撑。

目录

CONTENTS



**一.安全GPT助力电信
运营商云网安全的原理**



**二.电信运营商建设云
网安全GPT的必要性**



**三.电信运营商安全
GPT大模型建设的核心
能力要求和主要策略**



电信运营商云网安全 GPT大模型建设的核心 能力要求和主要策略

1. 电信运营商安全GPT大模型建设的核心能力要求
2. 主要策略：多模态安全能力 深度融合

1. 电信运营商安全GPT大模型建设的核心能力要求

(1) 目标定位 — 确保关键基础设施安全运营

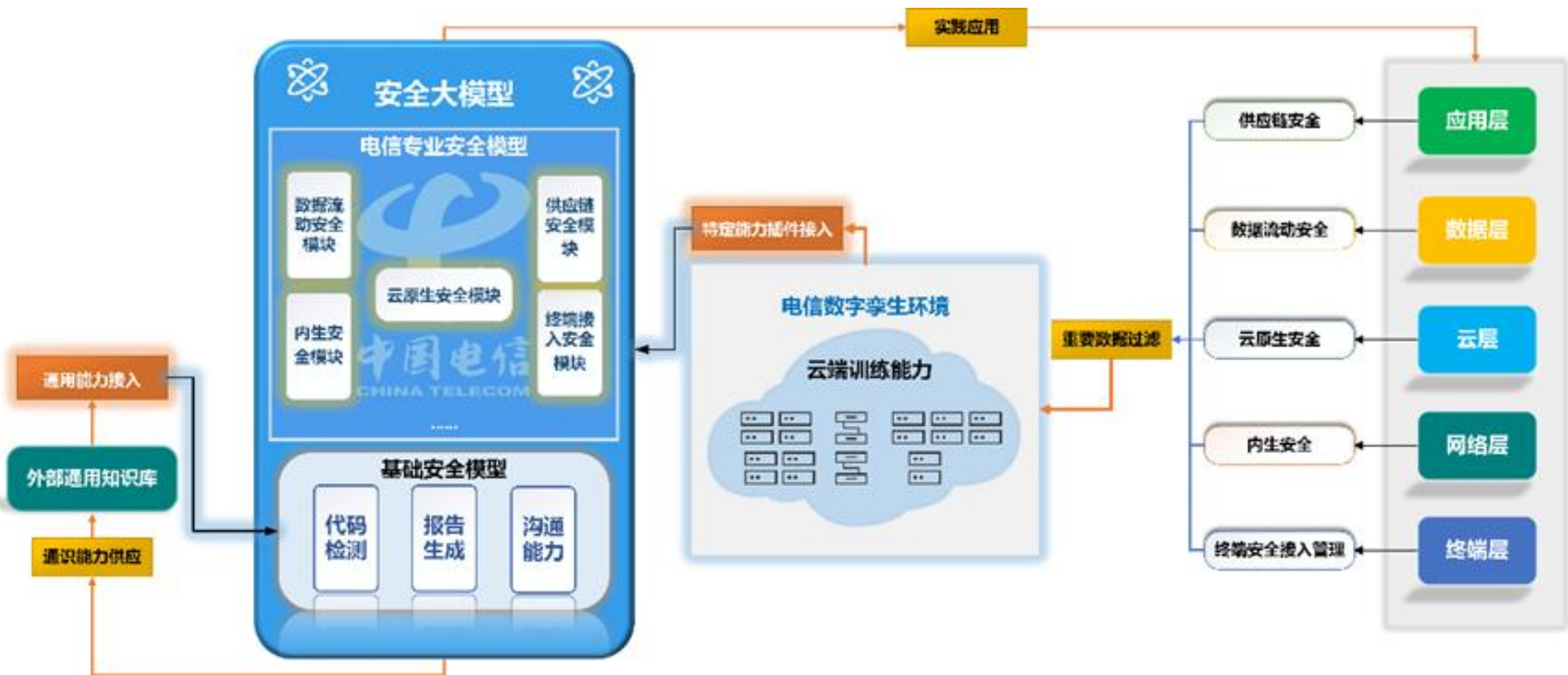
安全GPT大模型利用电信运营商的云计算能力，支持业务中台、数据中台和安全中台在多个场景下的运作，并能进行多场景分析，推动云网融合安全运营。它还能保障AI和元宇宙的安全性和可靠性，具备自动化威胁检测的能力，监管和预警数字资产安全风险，保障元宇宙的数据资产和数字孪生资产安全。

安全GPT大模型的能力分为以**通用安全知识为主的基础安全模型和偏用户服务为主的专业安全模型及专业能力插件两部分**。通用安全知识部分由互联网公开信息语料搭建而成，可以支持代码检测、报告生成和沟通能力对集团工作起到支持作用。专业能力插件实现模块化的数据流动安全、云原生安全等安全能力，并在关键数据脱敏后作为插件集成到安全大模型中。专业插件化的大模型具有实时获取最新能力、减少更新模型成本和增加可拓展性等优势。

(2) 核心功能及模型架构

多模态网信安全保障AI安全和元宇宙安全，如下图所示





第一阶段能力规划

在第一阶段，收集大量中英文语料和公开安全数据集，并结合目前已经开源的**通用大型模型（例如MOSS和ChatGLM）**进行微调训练。经过微调训练后，模型将具有成体系的网络安全知识和安全检测能力，如恶意行为检测、威胁情报分析、弱点扫描和漏洞管理等。此外，大型模型还可以与操作专家进行自然语言对话，从而显著降低安全人员的工作门槛。

第二阶段能力规划

在第二阶段，整合电信现有的安全资源，并借鉴相关厂商的服务能力。使用电信的计算资源能力对各专业能力进行插件化处理，并最终形成 **“1+1+N的安全GPT大模型目标体系”**。

这个体系以一个通用的大模型为基础，同时训练一个通用的安全专业大模型，并辅以N个专业能力插件。通过这个体系，安全大模型可以根据用户侧的实际情况自动调用专业插件，实现自动化处理。

这个阶段的安全大模型已经具备了相当于一个专业安全公司的能力，其中集成了各种不同的安全能力，并可以在不同的场景下自动组合使用。

2. 主要策略：多模态安全能力 深度融合

电信运营商已经在建设多模态安全能力深度融合的云网安全方面取得了初步成果。基于移动网、固网、无线网等，融合元宇宙终端设备，已初步构建大安全产品体系，包括云网安全、AI安全、元宇宙安全、量子安全、公共安全、信创、特殊通信等板块的两百多个安全产品。

尽管已经建立了如此庞大的安全产品体系，但是不同模态之间的安全能力深度融合仍然存在一定的不足，安全差异化优势尚未完全显现。

因此，电信运营商规划建设安全GPT大模型，发挥**多模态融合安全能力核心优势**，继续加强多模态安全网络的协同作用和融合能力，并不断优化云网安全GPT大模型，持续提高云网安全性能。

最后提出4点建议，与同仁们共同探讨：

- 1. GPT对于关键基础设施运营商的安全影响巨大。**需要快速做出反应，采取一系列的措施来应对这种威胁。只有这样，才能更好地保障企业网络和信息安全。
- 2. 采用“1+1+N”模式建设多模态安全GPT大模型。**安全GPT大模型是一种基于多模态网络的综合性安全模型，可以通过多种技术手段对网络安全进行全方位的保障。融合云计算、人工智能、元宇宙等先进技术，通过多种手段对网络进行实时监控和防护，提高网络安全的可视化和可感知性，为企业提供更加安全、稳定的网络环境。
- 3. 与行业内多模态安全GPT大模型开放服务能力提供商建立深度合作。**强强联合开发安全GPT产品，提高安全产品的质量、稳定性和安全性。

- 4. 加快多模态安全GPT大模型能力融合的核心技术创新，确保关键核心技术自主掌控。**随着人工智能、大数据等新技术的快速发展，网络安全面临着更加复杂和严峻的挑战，为了更好地应对这些挑战，需要加快安全融合需求的核心技术创新。其次，搭建多模态融合安全服务平台是实现内外能力紧耦合的关键。整合多种安全技术，提高安全防护能力。最后，构建多模态网信安全能力，保障AI安全和元宇宙安全是当前网络安全工作的重点。需要加强技术研究和创新，构建完善的安全保障体系，提高网络防护能力和应对能力。

THANKS

#云安全

#数字安全

#国际人才认证

#数据安全

#国际峰会

#隐私计算

#元宇宙安全

#区块链

#零信任