

基于指令与描述的文本数据安全业务属性生成机制

李晨皓, 王娜, 刘敖迪

(信息工程大学, 河南 郑州 450001)

摘要: 客体资源的安全业务属性标定是实施基于属性的访问控制机制的基础和关键。传统上, 文本数据安全业务属性标定主要依靠人类专家及机器学习的方法, 其效率及少样本能力过于低, 并且传统方法多以文本数据中的实体作为业务属性, 所提取的属性粒度粗糙、规模及安全管控层级均不可控, 极易导致属性空间膨胀问题。基于此, 提出了一种基于指令与描述的文本数据安全业务属性生成机制 (IDSAM, instruction and demonstration-based secure service attribute generation mechanism for textual data)。具体来说, 首先将安全业务属性生成中的候选业务属性 (即实体) 提取任务由序列标定问题转换为可控生成问题, 利用指令学习和情境学习技术实现对候选业务属性的提取; 然后, 利用 WordNet 实现对候选业务属性的语义泛化及去冗余, 同时通过控制余弦相似度阈值的方法避免语义过于泛化带来的语义丢失问题, 生成业务属性集; 最后, 以集合中初始属性与衍生属性间相似度为边权重, 构建加权有向无环属性图, 实现了能够根据安全管控需求动态生成、规模可控、安全粒度可调的安全业务属性库构建。实验结果表明, 所提机制中候选业务属性提取部分功能在 CoNLL-2003 数据集上的少样本实验中取得的平均 $F1$ 分数较基线模型更高, 并且所提机制能够按照安全管控需求, 动态挖掘出安全管控层级可调、规模可控的安全业务属性。

关键词: 命名实体识别; 基于属性的访问控制; 属性提取; 少样本; 大语言模型

中图分类号: TP391

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2024082

Instruction and demonstration-based secure service attribute generation mechanism for textual data

LI Chenhao, WANG Na, LIU Aodi

Information Engineering University, Zhengzhou 450001, China

Abstract: Attribute-based access control is fundamentally dependent on the secure service attribute calibration of object sources. Traditionally, the calibration of secure service attribute for textual data has been primarily reliant on human experts and machine learning methods, yet the efficiency and few-shot ability are insufficient. Moreover, tra-

收稿日期: 2024-05-29; 修回日期: 2024-08-12

通信作者: 王娜, twftina_w@126.com

基金项目: 国家自然科学基金 (61802436, 62102449); 河南省重点研发与推广专项 (222102210069)

Foundation Items: The Natural Science Foundation of China (61802436, 62102449), The Key Research and Development and Promotion Program of Henan Province (222102210069)

引用格式: 李晨皓, 王娜, 刘敖迪. 基于指令与描述的文本数据安全业务属性生成机制[J]. 网络与信息安全学报, 2024, 10(6): 81-95.

Citation Format: LI C H, WANG N, LIU A D. Instruction and demonstration-based secure service attribute generation mechanism for textual data[J]. Chinese Journal of Network and Information Security, 2024, 10(6): 81-95.

ditional approaches have predominantly utilized entities in textual data as service attributes, resulting in coarse granularity, uncontrollable scale and management level, further leading to the problem of attribute-space explosion. Thus, a secure service attribute generation mechanism for textual data (IDSAM) was introduced. This mechanism addressed the aforementioned challenges by transforming the extraction of candidate service attributes, previously a sequence-calibrated problem, into a controllable-generation problem through instruction learning and in-context learning. Subsequently, WordNet was employed to achieve semantic deduplication and generalization of the candidate service attributes. Concurrently, to prevent semantic loss due to over-generalization, a cosine similarity threshold was regulated, enabling the generation of a service attribute set. Finally, a weighted directed acyclic attribute graph was constructed based on the similarity between initial and derived attributes within the set, facilitating the dynamic construction of a secure service attribute library with a controllable scale and adjustable security granularity, in accordance with security control requirements. The candidate service attribute extraction component of the proposed mechanism achieves an optimal average *F1* score in few-shot experiments on the CoNLL-2003 dataset, surpassing the baseline model. This positions the mechanism as state-of-the-art. Furthermore, the mechanism is capable of dynamically mining secure service attributes with adjustable security control levels and controllable scales to meet varying security management requirements. The experimental results indicate that the proposed mechanism is effective in generating secure service attributes with the desired characteristics.

Keywords: named entity recognition, attribute-based access control, attribute extraction, few-shot, large language model

0 引言

作为一项遵循预设控制策略,保障资源只能被合法用户执行合法操作的技术,基于属性的访问控制(attribute-based access control, ABAC)技术可以通过更改安全属性对访问决策进行控制,而不需要更改底层规则集的主体/客体关系,进而提供大数据环境下的动态访问控制能力^[1]。显然,对数据资源的安全属性进行合理标定是实施ABAC技术的基础。

数据资源的安全属性包含密级、隶属单位、生成者、业务属性等。其中,业务属性是数据资源内容的体现,它是基于安全需求对一类数据资源内容的某种共性特征的描述。在数据量较少的情况下,由安全管理员对数据资源的业务属性进行人工标定是可行的。然而,进入大数据时代,面对海量的数据资源,单纯依靠安全管理员以人工方式标定数据资源的业务属性显然是不切实际的。因此,迫切需要对业务属性智能化生成技术展开研究,以实现海量数据资源的业务属性的自动化标定。

业务属性智能化生成技术至少需要满足两个需求:①针对不断动态涌现的数据资源和复杂多变的应用场景,业务属性智能化生成技术在少样本(few-shot)场景下应该具有良好的性

能。②业务属性应该满足不同级别的数据安全管控需求。也就是说,面对不同的数据安全管控级别,业务属性的粒度应该不同。例如,对分别具有“直升机”“民航飞机”等内容的数据资源而言,在只对“飞机”敏感的管控级别下,标定业务属性为“飞机”即可,但是在对具体飞机类型敏感的更加细粒度的管控级别下,应该分别标定业务属性为“直升机”“飞机”。

近年来,随着自然语言处理(natural language process, NLP)技术的进步,已有一些使用深度学习技术实现文本数据业务属性生成的解决方案,如Alohaly等^[2]、Liu等^[3]、Heaps等^[4]、Bao等^[5]提出的方案。然而,经分析发现,这些方案一方面存在属性空间膨胀问题,难以满足不同级别的数据安全管控需求,另一方面其依赖于复杂的特征工程和全参数微调(fine-tuning),难以有效应对few-shot场景下的安全业务属性标定需求。

得益于大语言模型(large language model, LLM)技术的进步,本文提出了一种基于指令与描述的文本数据安全业务属性生成机制(instruction and demonstration-based secure service attribute generation mechanism for textual data, IDSAM),以弥补上述方案的不足。该机制将

文本数据的安全业务属性生成分为文本数据的候选业务属性提取和属性语义泛化与聚类两个子问题。针对文本数据的候选业务属性提取问题, 本文将其转化为文本数据的命名实体识别(named entity recognition, NER)问题, 利用LLM技术设计了基于指令与描述的NER模型, 指令(instruction)能够明确指示和约束模型需要执行的操作, 确保模型聚焦任务要求; 描述(demonstration)能够增强模型对任务的理解, 使模型在面对few-shot场景下的有限数据时, 依然能够保持较高的准确性。同时, 为进一步提高模型对实体边界信息的捕获能力, 受Wang等^[6]论文的启发, 本文也提出了“实体提取”这个辅助任务。通过上述方法, 模型将针对特定内容的序列提取任务转换成了文本到文本(text to text, Text2Text)的生成任务, 能够在无须fine-tune的情况下以更高的精度实现few-shot场景下非结构化文本数据候选业务属性的提取。

由于自然语言的丰富性, 从文本数据资源中直接提取的候选业务属性可能存在语义冗余, 直接作为业务属性会带来属性空间膨胀问题。同时, 为了满足不同级别的数据安全管控需求, 本文对候选业务属性进行了语义泛化与聚类, 设计了基于WordNet语义泛化与聚类的安全业务属性生成方法。该方法将提取到的候选业务属性(即识别出的命名实体)语义映射到WordNet词网中, 利用WordNet词网中的同义词集实现候选业务属性的语义去冗余, 利用其中的上位词集实现候选业务属性的语义泛化, 并设置余弦相似度阈值来避免语义过于泛化带来的语义丢失问题, 最终实现了具有语义泛化关系的、安全管控级别可调、规模可控的业务属性库的构建, 为实现满足不同管控级别的安全业务属性标定提供了支撑。

本文主要贡献如下。

1) 将LLM技术与访问控制技术相结合, 为LLM技术在访问控制技术方向的发展进行了初步探索。

2) 提出了一种面向安全业务属性生成的基于指令学习(instruction learning)和情境学习(in-

context learning, ICL)的实体识别模型, 该模型是首个通过指令学习及情境学习技术实现安全业务属性生成中实体识别部分功能的模型。

3) 提出了一种基于WordNet语义泛化与聚类的安全业务属性生成方法, 实现了具有语义泛化关系的、安全管控级别可调、规模可控的业务属性库的构建。

1 相关工作

1.1 文本数据安全业务属性的生成

针对文本数据安全业务属性的生成问题, Alohaly等^[2]提出将属性类型提取视为一个通过关系依存树对文本数据进行关系抽取的任务, 然后通过一个基于CNN的多分类任务提取文本数据客体属性, 将这两个阶段的工作相关联来获取最终的属性信息。Liu等^[3]提出了一种多维混合特征生成的文本数据业务属性提取方法, 其中包括基于TF-IDF(term frequency-inverse document frequency)和BiLSTM设计的非结构文本数据安全业务属性挖掘模型, 以及基于BERT和胶囊网络设计的机构安全业务属性挖掘器。Heaps等^[4]首先通过BERT分类来判定文本数据是否包含访问控制信息, 然后对包含访问控制信息的数据资源继续依托BERT进行命名实体识别及分类并获取属性信息。Bao等^[5]通过句法依存关系抽取文本数据中的属性-观点对, 利用BERT实现结合上下文动态特征的词向量预训练, 并将Attention引入BiLSTM, 实现特征空间降维处理和属性信息的分类提取。

虽然这些方法在特定场景下表现较出色, 但是它们将从文本数据中提取的实体直接作为属性, 自然语言语义的丰富性不可避免会带来属性空间膨胀问题。同时, 这些方法提取的业务属性粒度固定, 难以满足不同级别的数据安全管控需求。此外, 这些方法依赖复杂的特征工程设计来实现较优的业务属性提取性能, 在本质上仍属于“狭隘的任务专家”, 应用场景受限; 同时, 其依赖fine-tuning, 在面对few-shot场景下的安全业务属性提取需求时, 性能往往受到限制。

1.2 提示学习、指令学习与情境学习

文献[7-8]提出了提示学习 (prompt learning) 技术, 各类下游任务被整合为预训练任务, 通过自然语言的形式进一步释放了模型的潜在能力。之后, Brown 等^[9]在训练 GPT-3 的过程中发现, 随着模型参数规模的不断扩大, 模型开始展现出对上下文知识的捕获能力, 即 ICL。通过向模型提供一系列与特定任务紧密相关的描述性语句作为 prompt, 模型能够更加精准地理解任务需求, 并生成更加精确的预测结果。在若干基准测试中, 经过 ICL 处理的模型在性能上已经能够与 fine-tuning 后的模型相媲美, 在某些情况下甚至实现了超越。这一发现为模型的发展和应用开辟了新的路径。

ICL 的形式化描述如式(1)所示:

$$Y = P(X|X'_1, X'_2, \dots, X'_n; \theta) \quad (1)$$

其中 Y 表示模型输出, $P(\bullet)$ 表示模型, X 表示模型输入, $X'_i (1 \leq i \leq n)$ 为描述性语句, θ 表示模型参数。例如, 在情感分类任务中, 若要判断语句 “The movie is so thoughtlessly assembled.” 是积极还是消极的, 传统方法往往涉及复杂的特征提取过程, 并结合统计方法 (如支持向量机或朴素贝叶斯分类器等) 进行处理。而借助 ICL 技术, 只需在 LLM 输入端枚举多个情感倾向明确的示例语句, 如 “It’s a wonderful movie and I like it. This is positive” 表示积极情感, “The drama discloses almost nothing. This is negative” 表示消极情感, 再将目标语句添加到这一上下文中, 并通过 prompt 询问 LLM 该语句的情感倾向, 即可快速得到分类结果。

Wei 等^[10]于 2021 年提出了一种名为 “指令调优 (instruction tuning)” 的新方法, 由此引出了指令学习技术。指令调优是通过在模型的输入前端添加自然语言形式的 “指令”, 指导模型学习并执行特定的任务。这种指令化的方式, 使得模型能够更准确地理解任务要求, 并按照指令进行相应的操作。这种方法不仅将下游任务与自然语言进一步对齐, 还显著提高了模型在 zero-shot (零样本) 和 few-shot 场景下的泛化能力。本文所提机制在实体识别部分便采用了指令学习与情

境学习技术。

指令学习的形式化描述如式(2)所示:

$$Y = P(X|\text{Ins}; \theta) \quad (2)$$

其中 Y 表示模型输出, $P(\bullet)$ 表示模型, X 表示模型输入, Ins 表示指令, θ 表示模型参数。例如, 在情感分类任务中, 针对语句 “This movie is amazing and I like it.”, 只需在 LLM 输入端加入指令如 “Please judge the sentiment of the this sentence and output 1 if it is positive and 0 if it is negative.”, 即能得知当前语句的情感态度, 而无须进行其他复杂计算。

上述技术能力只有在模型参数达到一定量级时才会 “涌现” 出来, 其在简化模型训练过程、提高模型的灵活性和易用性方面具有显著优点。然而, 这些技术能力的高低会受到模型输入长度限制、输入信息的敏感性, 以及上下文示例和指令质量的影响。在实际应用中, 需要综合考虑以获得最佳效果。

1.3 命名实体识别

传统上, 命名实体识别任务主要是通过通过在编码器的基础上增加分类器或条件随机场 (conditional random field, CRF) 来实现序列标定^[2, 3, 11]的。然而, 这类方法主要适用于平面实体识别任务, 难以应对更复杂的嵌套实体识别问题。为解决嵌套实体识别这一难题, 研究者 (如 Straková 等^[12]、Yan 等^[13]、Liang 等^[14]) 提出了 LSTM-CRF、TENER、BOND 等多种基于序列到序列 (sequence to sequence, Seq2Seq) 的方法, 然而这些方法仍存在依赖已标定数据集, 无法满足 few-shot 场景需求等局限性。

随着大语言模型技术的发展, 特别是在应对 few-shot 场景时, 生成式方法逐渐成为 NER 任务新的有效实现途径。2020 年, Li 等^[15]提出将 NER 任务转换为一个机器阅读理解 (machine reading comprehension, MRC) 任务。通过使用 query prompt 方法, 将 NER 转化为 MRC 中的问答类模式, 从而用一个统一的框架来处理平面和嵌套 NER 任务。2021 年, Yan 等^[16]提出了 BARTNER, 该模型通过将源句中的跨度逐个填充到预设模板中进行评分, 以判断其是否为实体。这种方法在 few-shot 场景下的表现显著超

越了传统方法，但其需对源句进行大量枚举和分类，因此较耗费算力。2022年，Chen等^[17]提出了一种基于风格迁移的数据增强模式，该模式能够将高资源域数据迁移到低资源域，实现few-shot场景下的NER任务。但是，其首先需要将T5模型^[18]作为生成器与鉴别器来实现数据的增强，然后利用BERT和一个线性层进行序列分类，实现方式依然较复杂，且耗费计算资源。

随着指令学习和ICL在人工智能领域的崛起，研究者开始积极探索将这两种学习方法应用于NER任务。Wang等^[6]于2022年提出了InstructionNER，其利用任务特定的指令来指导模型，并加入了两个特定辅助任务进行多任务学习，实现了few-shot场景高质量的NER。同年，Lee等^[19]在序列标定方案的基础上结合了prompt技术，提出了DemonstrationNER方法。通过在源输入后拼接示例模板，DemonstrationNER方法有效提升了模型对源文本中实体的识别能力。2023年，Chen等^[20]提出了MetaNER方法，通过加入特定示例，该方法在实体识别效果上取得了显著提升。Zhang等^[21]在前人的基础上，结合指令学习和ICL，提出了2INER方法，实现了更优的few-shot场景NER效果。

本文在解决安全业务属性生成的候选业务属性提取问题时，受InstructionNER和2INER的启发，也采用了指令学习与情境学习技术策略。不同之处在于，InstructionNER和2INER是完全的NER任务，本文机制更注重对候选业务属性（即实体）本身的提取。本文机制所采用的技术策略在访问控制领域尚属首次，有望为相关领域的研究带来新的突破。

1.4 WordNet词库

WordNet^[22]是一个大型英语词汇数据库，它根据词汇的字符串表示和语义进行精细的分类和组织。WordNet的核心是同义词集（synset），即具有相同或相似语义的词汇被聚集在一起。这种分类方式不仅便于用户查找和理解，还为计算机提供了识别词汇间细微差别的基础。此外，WordNet通过上/下位（hypernymy/hyponymy）词集展示了词汇之间的层次关系。这种

层次关系不仅有助于构建词汇之间的语义网络，还为所提机制的候选业务属性泛化任务提供了有力支持。

2 机制详述

本节首先对业务属性生成任务进行形式化说明，并对所提业务属性生成机制的整体架构进行介绍；然后分别对面向候选业务属性提取的基于指令与描述的实体识别模型和基于WordNet语义泛化与聚类的安全业务属性生成方法进行详细阐述。

2.1 任务描述与架构设计

本文的安全业务属性生成任务可以描述为：给定文本数据集 $Txs = [tx_1, tx_2, \dots, tx_n]$ ，首先采用候选业务属性提取方法分别从文本数据 $tx_i (1 \leq i \leq n)$ 中提取出候选业务属性集合 $Y_i = [y_1^i, y_2^i, \dots, y_{m_i}^i] (1 \leq i \leq n)$ ， $y_j^i (1 \leq j \leq m_i)$ 表示候选业务属性；其次，采用基于语义泛化与聚类的业务属性生成方法，基于候选业务属性 $Y = [Y_1, Y_2, \dots, Y_n]$ 生成业务属性集 A 和满足安全管控级别 α 要求的业务属性集 $A(\alpha)$ ， $A(\alpha) \subset A$ 。

IDSAM的整体架构如图1所示，其中基于指令与描述的实体识别（instruction & demonstration-based entity recognition, IDE）模型负责提取候选业务属性。IDE模型根据指令对嵌合了示例描述的原始输入文本进行实体提取，获得候选业务属性。同时，IDE模型通过执行“实体提取”辅助任务实现多任务学习，进一步优化模型对候选业务属性的提取性能。基于WordNet语义泛化与聚类的安全业务属性生成方法——WGA（WordNet-based semantic generalization and clustering mechanism for generating secure service attributes）运用WordNet对候选业务属性进行语义泛化及去冗余，采用基于余弦相似度的聚类方法避免语义过于泛化带来的语义丢失问题，并采用有向无环图（directed acyclic graph, DAG）方法构建业务属性库的加权属性图，以便根据安全管控级别生成相应的安全业务属性库。

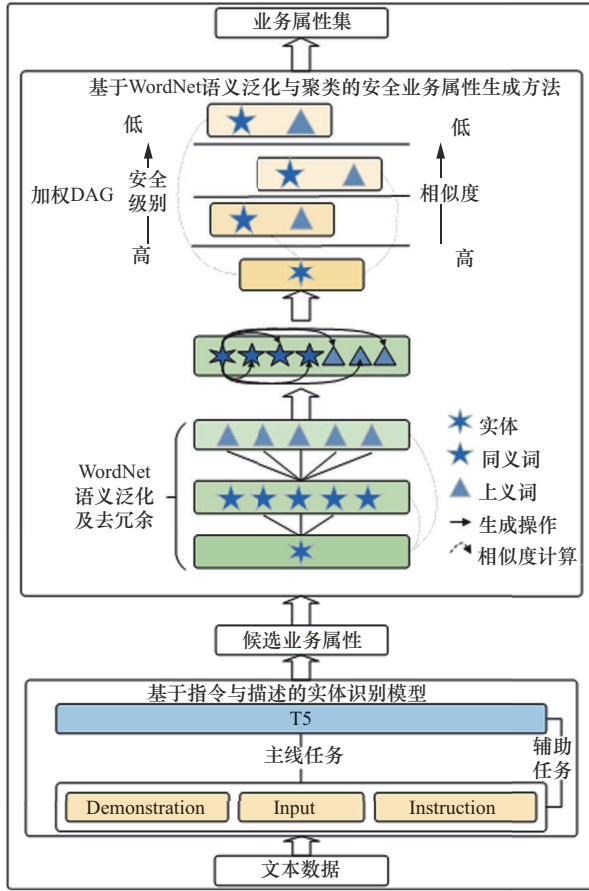


图1 IDSAM的整体架构

Figure 1 Overall architecture of IDSAM

2.2 基于指令与描述的实体识别模型

2.2.1 基于指令与描述的生成

受 Wang 等^[6]和 Zhang 等^[21]的研究启发, 本文所提机制将命名实体的识别问题重构为一个通过 T5 模型实现 Seq2Seq 的生成问题。T5 模型的预训练任务聚焦于恢复被损坏的“词元”, 这与本文所提机制实体提取部分的模式相吻合。同时, T5 模型的参数规模较适中 (7.7 亿个), 易于实际场景应用部署。基于上述考虑, 所提机制采用 T5 模型作为基干模型。

模型的输入结构可抽象为 $X = [T, D, I]$, 其中 T 表示原始输入文本、 D 表示上下文描述、 I 表示指令。IDE 的主线任务与辅助任务示意如图 2 所示。

T : 需要进行实体提取的原始输入文本。

D : 本文所提机制遵循的研究设置^[23], 从训练集中随机抽取不同类型的示例文本, 将其转化为形如 “<entity> is a/an <entity_type>” 的描述性

语句。针对每种实体类型, 从训练集中随机选取 N 个示例。以 CoNLL-2003 数据集为例, D 中各类型实体的部分示例可为 “XXX is a person” “XXX is an organization” “XXX is a location” 及 “XXX is a miscellaneous”。模板统一的 D 不仅有助于 IDE 模型理解上下文示例, 还能起到规范化模型输出以便后续提取操作的作用。

I : 由一句自然语言构成, 用来指示模型当前需要执行的操作。针对主线 NER 任务, 以 CoNLL-2003 数据集为例, I 为 “Please extract all the entities and their types in Sentence based on knowledge in Examples. All types are in options: PER, LOC, ORG, MISC.”。

考虑到 IDE 模型对输入端文本的位序具有极高的敏感性^[21, 24-25], IDE 模型最终的输入形式确定为 $\text{input} = [T, D, I]$ 。

本文所提机制的框架采用 “问答 (question-answer, QA) 模型” 的形式来实现。

对于数据集中的数据 $S = \{(x_i, y_i)\}_{i=1}^N$, 其中 x_i 和 y_i 分别是第 i 个数据的 “句子” 和 “标签”。本文使用 $\Phi(\bullet)$ 和 $\Gamma(\bullet)$ 分别将 x_i 和 y_i 转换成自然语言形式。

以 CoNLL-2003 数据集为例, 对于 $x_i = \text{'By steps Kent had reached 108 for three.'}$ 和 $y_i = \text{'Kent, ORG, span = (10,13)'}$, 有

$$\Phi(x_i) = (\text{Sentence} = x_i) \oplus (\text{Examples} = D) \oplus (\text{Question} = I)$$

$$\Gamma(y_i) = \text{'Answer: Kent is an ORG.'}$$

其中 $\oplus$ 表示内容的串联操作。有了 I 的指示, 再加上 D 与 $\Gamma(y_i)$ 的提示与约束, IDE 模型就能够按照特定格式 “<entity> is a/an <entity_type>” 进行结构化输出, 从而方便后续操作。

在训练阶段, 将 $\Phi(x_i)$ 输入模型 $M(\bullet)$, 得到输出:

$$y' = \arg \max M(\Phi(x_i) | \theta)$$

其中 θ 表示模型参数。

训练损失 L 为:

$$L = \text{Loss_function}(y', \Gamma(y_i))$$

最后, 对 y' 执行匹配操作 $p(\bullet)$, 提取出最终

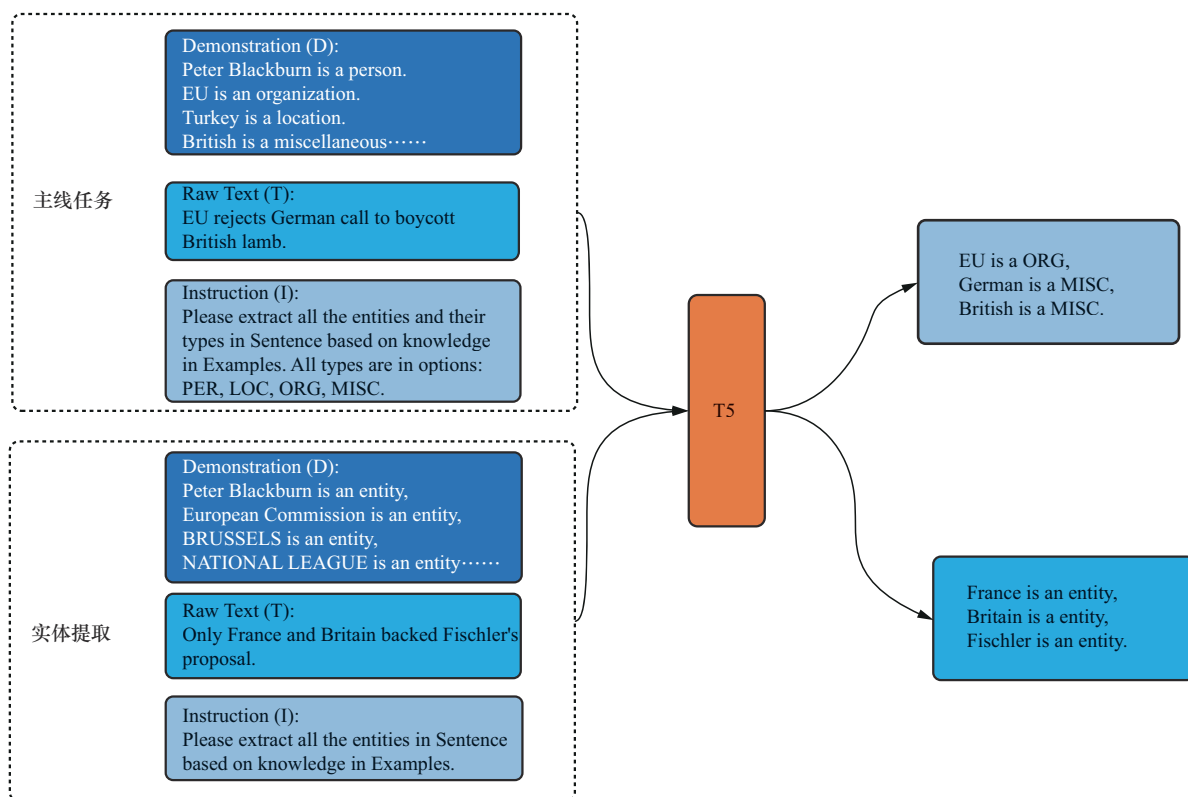


图2 IDE的主线任务与辅助任务示意

Figure 2 Schematic of IDE main tasks and auxiliary tasks

实体、类别及跨度为

$$(\text{Kent}, \text{ORG}, (10, 13)) = p(y', x_i)$$

上述机制能够以自然语言的形式使IDE模型更深入地理解Text2Text的实体识别任务。

2.2.2 辅助任务

为了进一步优化IDE模型的性能, 本文借鉴了InstructionNER方法提出的“实体提取”辅助任务。辅助任务通过Text2Text的形式与主线任务共同进行训练。辅助任务的主要目标是从实体识别方面提高IDE模型的性能。因为业务属性生成的核心可以分解为两个方面, 一方面是从文本数据中准确地识别候选属性(即实体), 另一方面是对实体的属性信息进行提取。引入“实体提取”辅助任务, 可使IDE模型更加聚集于从文本数据中准确地识别候选属性, 从而提高IDSAM的整体性能。

针对“实体提取”辅助任务, 设置 I 为“Please extract all the entities in Sentence based on knowledge in Examples.”, D 为“ y_1 is an entity, y_2 is an

entity, ..., y_i is an entity.”。

有了 I 的指示及 D 提供的上下文示例, IDE模型只需关注输入句中的实体信息, 而无须在意实体的具体类型, 即只考虑实体及其跨度 (y_i, s_p) 。

实体提取的效果直接关系到IDE模型从句子中准确识别实体的能力。通过对此能力的评估, 可以明确了解其在提升IDE模型实体识别性能方面的潜力。“实体提取”辅助任务的性能可使用Span-F1来进行评估。

IDE模型在部署和测试时, 仅需运行主线任务, 而在训练时需要主线任务与辅助任务共同参与。

2.3 基于WordNet语义泛化与聚类的安全业务属性生成方法

针对提取到的候选业务属性 $Y = [Y_1, Y_2, \dots, Y_n]$, $Y_i = [y_1^i, y_2^i, \dots, y_{m_i}^i] (1 \leq i \leq n)$, 首先分别将 $y_j^i (1 \leq i \leq n, 1 \leq j \leq m_i)$ 语义映射到WordNet中, 得到同义词集集合 $\text{Syns} = [\text{syns}_1, \text{syns}_2, \dots, \text{syns}_k]$ 。若存在多个候选业务属性资源共享同一同义词,

可使用该同义词表示上述属性, 实现语义去冗余。因为存在语义冗余的候选业务属性都合并到

一个同义词集 $\text{syns}_i (1 \leq i \leq k)$ 中, 所以 $k < \sum_{i=1}^n m_i$ 。

然后, 基于 WordNet 的上/下位词集关系, 对 Syns 中同义词集分别进行泛化处理, 提取所有的上位词, 生成集合

$$A' = \{ y | (y' = \text{syns}_i) \vee (y' = \text{hy}(\text{syns}_i)), 1 \leq i \leq k \}$$

其中, $\text{hy}(\text{syns}_i)$ 表示同义词集 syns_i 的某个上位词。最后, 依次计算 syns_i 与其每个上位词间的余弦相似度 cs_{ij} 。

$$\text{cs}_{ij} = \text{sim}_{\cos}(\text{syns}_i, \text{hy}_j(\text{syns}_i))$$

其中 $\text{hy}_j(\text{syns}_i) \in \text{Hy}(\text{syns}_i)$, $\text{Hy}(\text{syns}_i)$ 表示同义词集 syns_i 在 WordNet 中所有上位词构成的集合。 $\text{Hy}(\text{syns}_i)$ 是个有序集, 按上位词间层次关系对 $\text{Hy}(\text{syns}_i)$ 中元素进行排序, $\text{hy}_j(\text{syns}_i)$ 表示 syns_i 的第 j 个上位词。

设存在语义泛化阈值 δ , 则生成业务属性集合:

$$A = \{ y | (y = \text{syns}_i) \vee (y = \text{hy}_j(\text{syns}_i) \wedge (\text{cs}_{ij} \geq \delta)), 1 \leq i \leq k \}$$

只选取集合 A' 中语义相似度大于阈值 δ 的元素生成业务属性集合 A , 可避免语义过于泛化带来的语义丢失问题。将集合 A 中元素 syns_i 称为初始属性, 元素 $\text{hy}_j(\text{syns}_i)$ 称为 syns_i 的衍生属性。

为了得到满足安全管控级别 α 要求的业务属性集 $A(\alpha)$, 本文所提生成方法采用了加权 DAG 思想来生成集合 A 的加权有向无环属性图 $\text{DAG}(A)$ 。具体来说, 将集合 A 中属性作为节点, 根据属性间的语义泛化关系生成节点间的有向边, 如 $\text{hy}_j(\text{syns}_i)$ 是 syns_i 的上位词, 则存在从节点 syns_i 到节点 $\text{hy}_j(\text{syns}_i)$ 的有向边, cs_{ij} 为该边权重, 通过重复上述步骤实现集合 A 的加权 $\text{DAG}(A)$ 的构建。其次, 设安全管控级别 $\alpha \in [1, 2, 3, \dots]$, 数值越大, 表示管控级别越低, 属性粒度越粗, 属性库规模越小。按照边权重从大到小的顺序输出 $\text{DAG}(A)$ 中每个 syns_i 属性的第 $\alpha - 1$ 个衍生属性, 从而得到满足安全管控级别 α 要求的业务属性子集 $A(\alpha)$ 。

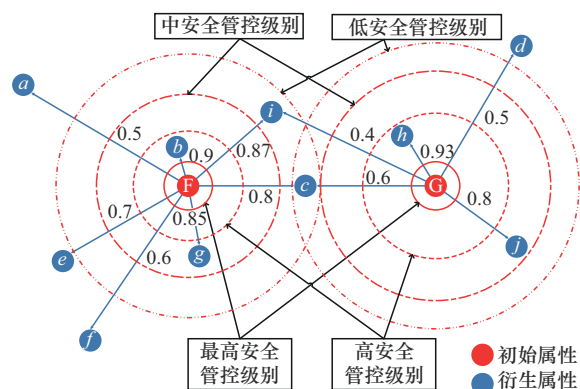
候选属性集 Graph_{CA} 示意如图 3 所示, 红色节点表示初始属性, 蓝色节点表示由初始属性语义泛化得到的衍生属性, 边权重表示初始属性与其对应衍生属性间的相似度。较高的安全管控级别应具备较细粒度的属性。当 $\alpha = 1$, 则 $A(1) = \{ F, G \}$; 当 $\alpha = 2$ 时, 则 $A(2) = \{ b, h \}$; 当 $\alpha = 3$ 时, $A(3) = \{ g, j \}$; 当处于低安全管控级别, 即 $\alpha = 4$ 时, 候选属性节点 F 、 G 具有共同的衍生属性节点 c , 节点 i 因低于节点 G 的最低管控级别而被舍弃, 因此 $A(4) = \{ c \}$ 。表 1 给出了安全业务属性集生成伪代码。

表 1 安全业务属性集生成伪代码

Table 1 Pseudo-code for the generation of security service attribute set

输入: y_j^i // 候选业务属性 输出: A // 安全业务属性集

- 1) $\text{Syns} = \text{set}()$ // 初始化同位词集合
- 2) $\text{Syns} = \text{Synonyms}(y_j^i)$ // 通过 WordNet 获取 y_j^i 的同义词集合, 并去除冗余词
- 3) $\text{Hyps} = \text{set}()$ // 初始化上位词集合
- 4) For si in Syns :
- 5) $\text{hy}_i = \text{Hypernyms}(si)$ // 获取同义词集中每个元素 si 的上位词集合
- 6) For hy in hy_i :
- 7) $\text{cs_value} = \text{Cos_Sim}(\text{hy}, y_j^i)$ // 依次计算 y_j^i 与 hy 间的余弦相似度
- 8) if $\text{cs_value} > \delta$: // 当相似度大于阈值时
- 9) $\text{Hyps.add}(\text{hy})$ // 将符合条件的上位词添加到上位词集合中
- 10) $A = \text{Union}(\text{Syns}, \text{sort}(\text{Hyps}))$ // 将依据相似度大小排序后的上位词集与同位词集相融合, 构建业务属性集
- 11) $\text{DAG}(A) = \text{build_attribute_graph}(A)$ // 利用 Neo4j 建立属性集 A 的加权 DAG 属性图谱
- 12) $A = \text{infer_attribute}(\text{DAG}(A), \alpha)$ // 按照安全需求 α 从属性图中推理出子属性图
- 13) return A

图3 候选属性集 Graph_{CA} 示意Figure 3 Schematic of candidate attribute set Graph_{CA}

3 实验

本节将从机制和功能的角度对比分析IDSAM与前人工作的差异，并从全监督实验和 few-shot 实验两个方面评价IDSAM的候选业务属性（即实体）提取性能，并验证WGA的属性提取能力。

3.1 实验设置

(1) 评价指标

本文采用了常见的精确率（Precision）、召回率（Recall）及 $F1$ 分数（ $F1$ -score）作为评价指标。本文计算了实验所得的真阳性（TP）、假阳性（FP）、真阴性（TN）及假阴性（FN）的数量。这些评价指标的计算方法如式(3)~式(5)所示。由于 $F1$ 分数能够更加综合地反映模型的精确率与召回率，因此本文主线任务以 $F1$ 分数为基准进行评价。“实体提取”辅助任务采用 Span- $F1$ 为基准进行评价（即忽略结果中的“实体类别”部分后进行指标计算）。每个实验重复5次取平均结果进行评价。

$$\text{Precision} = \frac{TP}{TP + FP} \quad (3)$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad (4)$$

$$F1\text{-score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \quad (5)$$

(2) 数据集

为评价所提机制在安全业务属性挖掘方面的效果，本文选用NER研究领域广泛应用的新闻类CoNLL-2003标准数据集进行实验。该数据集包含了实体类别和实体位置信息，其中实体类别包括下列4类。

1) 人名（PER）：人员名称。

2) 地名（LOC）：地理位置或地点。

3) 组织名（ORG）：涵盖公司、机构、团体组织等。

4) 其他（MISC）：除前3类以外的其他类型实体。

CoNLL-2003数据集的详细信息如表2所示。

表2 CoNLL-2003数据集的详细信息

Table 2 Details of the CoNLL-2003 dataset

数据集	领域	标签	训练集	测试集
CoNLL-2003	新闻	4	1.4×10^4	3.5×10^3

(3) 实验环境

实验采用Windows 10系统、Pytorch工具包和Pycharm作为开发平台，依托Nvidia Titans GPU进行测试。

(4) 参数

实验采用T5-large作为基干模型进行测试。实验批次规模分别设定为2、4、6，模型采用AdamW优化器，并采用交叉熵 CrossEntropy-Loss作为损失函数，学习率设置为 2×10^{-5} ，波束搜索尺寸设置为2，以获得更多的抽取结果。在全监督实验中，热身步数设置为200步。

3.2 对比分析

本文从技术路径、技术特点、机制效果等方面将IDSAM与前人工作进行了对比分析，如表3所示。本文所提机制采用了与前人工作完全不同的技术路线，并且实现了安全管控层级可调的属性提取。同时，本文机制采用无须耗费大量算力的 fine-tuning，能够适应不同的应用环境。综合而言，本文机制各方面的能力均优于前人所提机制。

3.3 全监督实验评估

在IDSAM实体提取部分的全监督实验中，本文实验的比较模型如下。

1) 基于序列标定的方法，包括Yang等^[26]、BOND^[27]、TENNER^[13]、LC-BERT^[28]与LC-BART^[29]。

2) 基于BART构建prompt模板的TemplateNER^[23]。

3) 采用参数高效微调（PEFT，parameter-efficient fine-tuning）机制的LightNER^[30]。

4) 基于BART的生成式方法BARTNER^[16]。

5) 基于“指令+情境学习”的2INER^[21]机制。

表 3 IDSAM 与前人工作对比

Table 3 Comparison between IDSAM and previous works

机制	模型	技术路径	few-shot	fine-tuning	属性粒度	属性库规模
Alohaly 等 ^[2]	CNN	分类	不具备	需要	固定	不可控
Liu 等 ^[3]	BERT-TF-IDF-BiLSTM	分类	不具备	需要	固定	不可控
Heaps 等 ^[4]	BERT	分类	不具备	需要	固定	不可控
Bao 等 ^[5]	BERT-Att-BiLSTM	分类	不具备	需要	固定	不可控
IDSAM	T5	生成	具备	无须	可调	可控

通过对比实验，可以更全面地了解 IDSAM 在全监督训练模式下的性能表现。

全监督实验结果对比如表 4 所示，可以看出，尽管 IDSAM 是针对 few-shot 设计的，但是在全监督训练模式下，其性能依然表现优异。相比序列标定的方法，IDSAM 分别取得了 1.44%、14.93%、0.88%、0.48% 和 1.61% 的领先优势；相比使用 prompt 的 TemplateNER，IDSAM 实现了 0.31% 的领先。与机制相似的 2INER 相比，IDSAM 也展现出了 1.5% 的优势，这是由于 2INER 额外采用了“类型提取”“类型判别”两个其他的辅助任务，过多的辅助任务给模型主线任务带来了噪声干扰。虽然与采用 PEFT 的 LightNER 相比，IDSAM 落后 0.72%，但综合来看，IDSAM 表现不俗，在全监督模式下具有强大的竞争力。

表 4 全监督实验结果对比

Table 4 Comparison of fully-supervised experiments results

模型	技术路径	F1	Span-F1
Yang 等 ^[26]	序列标定	90.77%(1.44%)	—
BOND	序列标定	77.28%(14.93%)	—
TENER	序列标定	91.33%(0.88%)	—
LC-BERT	序列标定	91.73%(0.48%)	—
LC-BART	序列标定	90.60%(1.61%)	—
TemplateNER	prompt	91.90%(0.31)	—
LightNER	PEFT	92.93%(-0.72%)	—
BARTNER	提示	—	93.24%(1.72%)
2INER	指令 + 情境	90.71%(1.5%)	93.93%(1.03%)
IDSAM	指令 + 情境	92.21%	94.96

3.4 few-shot 实验评估

本实验遵循标准的 k -shot NER 设置^[31]：对于每种实体类型，从训练集中随机抽取 k 个训练示例组成新的训练集，并将剩余示例作为验证集进行验证，其中 $k \in \{10, 20, 50\}$ 。同时，针对每种类型的实体，从数据集中随机选取 N 个实体以生成描述 D ， $N \in \{1, 5, 10\}$ 。

实验中将 IDSAM 与基于度量方法和基于 prompt 方法的几类典型实现方法进行了比较。

1) 基于度量的方法：包括 BERT-tagger^[32] 和 StructShot^[14]。BERT-tagger 以 BERT 为基干模型并采用分类模式实现，StructShot 采用 viterbi 算法予以实现。

2) 基于 prompt 的方法：包括 BARTNER 和 EntLM。EntLM 采用无模板 hard prompt 调优方法^[33]。

few-shot 实验结果对比如表 5 所示，当 N 设置为 5， k 值取 10、20、50 时，IDSAM 的 $F1$ 分数相较传统序列标定方法的 BERT-tagger 分别提高 6.42%、2.29%、0.59%，较 StructShot 则分别提高了 3.96%、1.44%、-0.94%。与采用模板提示的 TemplateNER 相比，IDSAM 的 $F1$ 分数分别提高了 8.47%、4.57%、1.08%。与 BARTNER 相比，IDSAM 高出了 16.50%、8.55%、1.09%。相较于 EntLM，IDSAM 分别高出 1.54%、1.43%、0.13%。同时，通过与对照组的平均 $F1$ 分数比较可以看出，基于指令和描述的生成式方法 IDSAM 在 few-shot 下的序列标注任务中取得了最优效果，整体优势显著。

表5 few-shot实验结果对比

Table 5 Comparison of few-shot experiments results

模型	F1 分数			
	k=10	k=20	k=50	平均值
BERT-tagger	59.91%	68.66%	73.20%	67.26%
StructShot	62.37%	69.51%	74.73%	68.87%
TemplateNER	57.86%	66.38%	72.71%	65.65%
BARTNER	45.70%	62.40%	72.70%	60.27%
EntLM	64.79%	69.52%	73.66%	69.32%
IDSAM	66.33%	70.95%	73.79%	70.35%

3.5 属性生成效果

在WGA部分的实验环节中,核心任务是验证其具备安全业务属性泛化和聚类的能力及在不同安全需求下动态提取安全业务属性的能力。将IDE中提取出的 y_j^i 共同传入WGA进行实验,并将提取到的候选属性信息传入Neo4j生成安全业务属性库进行可视化验证,得到候选属性DAG。候选属性DAG部分节点可视化如图4所示,其中蓝色节点为候选属性节点,黄色节点为对应的衍生属性节点

点,所有黄色节点共同组成安全业务属性集。

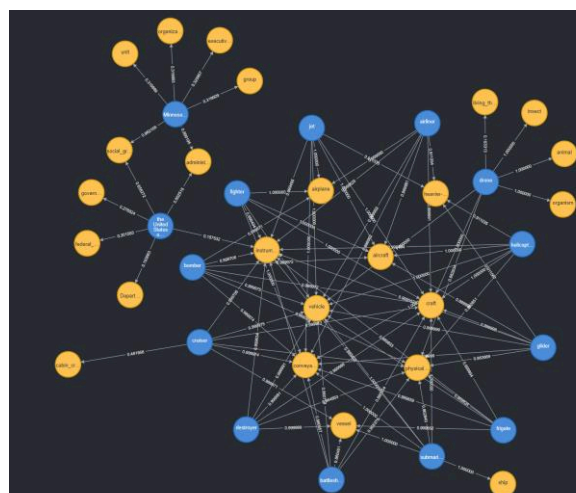


图4 候选属性DAG部分节点可视化

Figure 4 Visualization of nodes in the DAG of candidate attributes

不同安全管控级别下业务属性集可视化如图5所示。在最高安全需求情况下,业务属性库应只包含最细粒度的安全业务属性,如图5(a)中所示的黄色节点,经过WGA处理的候选业务属性能



(a) 最高安全管控级别时的属性图



(b) 高安全管控级别时的属性图



(c) 中安全管控级别时的属性图



(d) 低安全管控级别时的属性图

图5 不同安全管控级别下业务属性集可视化

Figure 5 Visualization of service attribute set under different security control levels

够满足最细粒度的安全业务属性需求；高、中、低安全管控级别的属性图分别如图5(b)、图5(c)、图5(d)所示，部分候选属性经过WGA语义泛化及去冗余处理后，分别出现多个候选属性共享同一属性的情况，且属性库规模进一步缩减，与实验预期一致。

实践证明，WGA能够在不同安全需求情况下生成粒度精细、层级可控的动态属性库，为访问控制技术提供足够的属性支撑服务。

4 结果分析

为评估各模块对IDSAM最终性能的影响，本文进行了消融实验。

4.1 I 与 D 对IDSAM性能的影响

为验证 I 和 D 对IDSAM性能的影响，本实验测试了去除 I 与 D ，但输出形式不变的模型T5-large的性能。IDSAM与T5-large的实验结果对比如表6所示，相比之下，当 $N=5$ 时，IDSAM在3种样本情况下分别高出10.53%、7.35%和5.19%，说明采用“指令+描述”方法后，模型能够更准确地理解任务的含义，从而获得更优异的性能。

表6 IDSAM与T5-large的实验结果对比
Table 6 Experimental results comparison between IDSAM and T5-large

模型	F1 分数			
	$k=10$	$k=20$	$k=50$	平均值
T5-large	55.80%	63.60%	68.6%	62.67%
IDSAM	66.33%	70.95%	73.79%	70.35%

4.2 D 对IDSAM性能的影响

本节深入探讨 D 对实体识别部分任务的影响。

首先，验证IDSAM在添加 D 与不添加 D 时的性能表现。IDSAM与InstructionNER的实验结果对比如表7所示，相较于纯粹的基于指令学习的InstructionNER，拥有 D 的IDSAM的 $F1$ 在 $N=5$ 、 $k=10$ 、20时分别提高了5.03%、3.75%；仅在 $k=50$ 时，InstructionNER的性能领先IDSAM 2.51%；从平均 $F1$ 分数来看，IDSAM以2.08%的优势领先于InstructionNER。这一结果表明，IDSAM能够从描述中有效学习到相关知识，进而提升NER任务的整体性能。

表7 IDSAM与InstructionNER的实验结果对比
Table 7 Experimental results comparison between IDSAM and InstructionNER

模型	F1 分数			
	$k=10$	$k=20$	$k=50$	平均值
InstructionNER	61.30%	67.20%	76.30%	68.27%
IDSAM	66.33%	70.95%	73.79%	70.35%

IDSAM与对照组的few-shot实验结果对比如图6所示。在50 Shot的实验中，IDSAM出现 $F1$ 分数落后现象。这是因为InstructionNER对一个名为“类型提取”的辅助任务进行了额外训练，以提高对实体类别的判断能力，而IDSAM未进行相关辅助训练，在实验过程中生成了错误的实体类别，从而在多样本实验中失分。如前文所述，仅以NER提取到的实体类别作为属性，既存在粒度粗糙问题，也会出现较大的误差。本文的核心目标是对实体的安全业务属性进行提取，并非完全的NER，因此并未针对这一现象进行调整。

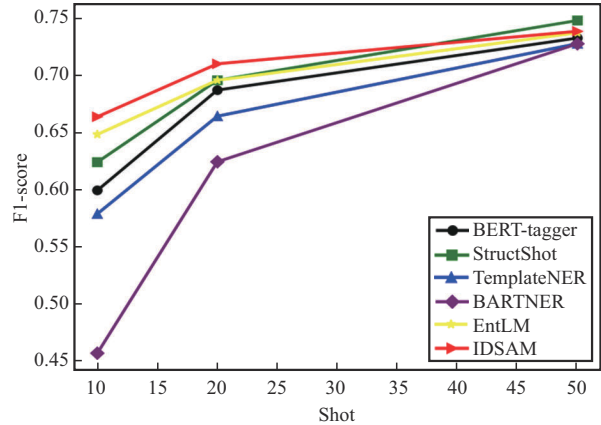


图6 IDSAM与对照组的few-shot实验结果对比
Figure 6 Comparison of few-shot experiments results between IDSAM and control group

从图6还可以看出，随着样本数量的递增，IDSAM的 $F1$ 分数增长速率明显小于大部分基线模型。这是因为随着监督信号的增多，IDSAM能够逐渐学习到任务中的特定语义关系，而此时 D 中的标签词可能包含冗余信息，这些信息会干扰这一学习过程，减缓 $F1$ 分数的进一步增长。再者，IDSAM关注的重点是对实体的准确提取，而非实体类型，这也是 $F1$ 分数

增速减缓的原因之一。最后，当样本量较大时，对实体类别的错判可能会产生次优结果，也是导致 $F1$ 分数增长放缓的原因之一。

然后，验证 D 的数量对 IDSAM 性能的影响。 D 的数量对 IDSAM 性能的影响如表 8 所示，ISDAM 的 $F1$ 分数与 D 的数量呈现正相关关系。值得注意的是，随着 D 数量的增长， $F1$ 分数的增长速率在逐步减小，这与 Zhang 等^[21]的研究发现一致。在初始阶段， D 能够为 IDSAM 提供更多的背景信息和任务指导，从而显著提升 IDSAM 的预测能力。但随着 D 数量的不断增加，这些额外信息可能带来的边际效用会逐渐减少。此外，过多的 D 会降低 IDSAM 的有效输入长度。在本文的实验中， D 的数量设置为 5 可以获得最大增量收益，而在实际中如何确定 D 的数值仍有待进一步探讨和研究。

表 8 D 的数量对 IDSAM 性能的影响
Table 8 Influence of the number of D on IDSAM performance

Shot	D	$F1$ 分数
10	1	63.23%
	5	66.33%
	10	67.88%
20	1	69.22%
	5	70.95%
	10	71.13%
50	1	71.85%
	5	73.79%
	10	74.38%

最后，验证不同形式的 D 对 IDSAM 中主线任务提取效果的影响。实验比较了第 2.2 节中所述形式与形如 “<entity_type> examples are: <entity 1>, <entity 2>, ..., <entity n >” 两类 D 在 50 Shot 实验中对 $F1$ 分数的影响。不同形式的 D 对 IDSAM 性能的影响如表 9 所示，原始 D 与新 D 的 $F1$ 分数分别为 73.79% 和 20.51%，说明 D 的形式也是影响 IDSAM 最终性能的关键因素之一，也体现了上下文质量对 LLM 生成质量具有重大的影响。

表 9 不同形式的 D 对 IDSAM 性能的影响
Table 9 Influence of different forms D on IDSAM performance

形式	Shot	$F1$ 分数
原始 D	50	73.79%
新 D	50	20.51%

4.3 辅助任务对实体识别性能的影响评估

如表 4 中右侧部分所示，当仅考虑对实体的提取时，ISDAM 的 Span- $F1$ 分数相较 2INER 和 BARTNER 分别高出 1.03% 和 1.72%，展现出了更精准的实体提取能力。辅助任务对 IDSAM 性能的影响如表 10 所示，经过辅助任务训练的 IDSAM 相较仅单纯进行主线任务训练的 IDSAM 的 $F1$ 分数提高了 1.25%，证明利用辅助任务进行多任务学习可提升 IDSAM 的实体识别能力，从而可以更好地支持后续的属性提取。

表 10 辅助任务对 IDSAM 性能的影响
Table 10 Influence of auxiliary tasks on IDSAM performance

辅助任务训练	Shot	$F1$ 分数
无	20	69.70%
有	20	70.95%

5 结束语

本文提出了一种基于指令与描述的文本数据安全业务属性生成机制 IDSAM。具体来说，所提机制首先将非结构文本数据安全业务属性提取中的候选业务属性（即实体）提取任务转换为可控生成问题，利用指令和任务相关描述性语句对原始输入进行封装，从而实现了对候选业务属性的提取。同时，本文采用了一个辅助任务，使架构更加聚焦于实体的提取。然后，所提机制利用 WordNet 实现候选业务属性的语义泛化及去冗余，采用基于余弦相似度的聚类方法避免语义丢失问题，并且采用加权 DAG 的思想构建出了可根据安全需求动态生成的、安全管控级别可调的、规模可控的安全业务属性库。实验结果表明，所提机制较基线模型在标准数据集上能够获得更优的平均候选属性识别性能，并且所提机制能够按照设计目标动态生成安全业务属性库。

参考文献:

- [1] 房梁, 殷丽华, 郭云川, 等. 基于属性的访问控制关键技术研究综述[J]. 计算机学报. 2017(40):1680-1698.
FANG L, YIN L H, GUO Y C, et al. A survey of key technologies in attribute-based access control scheme[J]. Chinese Journal of Computers, 2017, (40):1680-1698.
- [2] ALOHALY M, TAKABI H, BLANCO E. A deep learning approach for extracting attributes of abac policies[C]//Proceedings of the 23rd ACM on Symposium on Access Control Models and Technologies. Indianapolis, Indiana. 2018: 137-148.
- [3] LIU A, DU X, WANG N. Unstructured text resource access control attribute mining technology based on convolutional neural network [J]. IEEE Access, 2019, 7: 43031-43041.
- [4] HEAPS J, KRISHNAN R, HUANG Y, et al. Access control policy generation from user stories using machine learning[C]//35th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy XXXV: (DBSec 2021). 2021: 171-188.
- [5] 包乾辉, 文娟, 石淑珍, 等. 融合句法依存与BERT-Att-BiLSTM的属性分类[J]. 北京邮电大学学报. 2023(46):123-128.
BAO Q H, WEN J, SHI S Z, et al. Aspect category classification integrated in syntactic dependency and BERT-Att-BiLSTM[J]. Journal of Beijing University of Posts and Telecommunications, 2023, (46): 123-128.
- [6] WANG L, LI R, YAN Y, et al. Instructionner: a multi-task instruction-based generative framework for few-shot ner[J]. arXiv:2203.03903, 2022.
- [7] LI D, NAN Y, WANG W, et al. Unified language model pre-training for natural language understanding and generation[C]//Proceedings of the 33rd International Conference on Neural Information Processing Systems. 2019: 13063-13075.
- [8] RADFORD A, NARASIMHAN K, SALIMANS T, et al. Improving language understanding by generative pre-training[R]. OpenAI Blog, 2018.
- [9] BROWN T B, MANN B, RYDER N, et al. Language models are few-shot learners[C]//Proceedings of the 34th International Conference on Neural Information Processing Systems. 2020: 1877-1901.
- [10] WEI J, BOSMA M, ZHAO V, et al. Finetuned language models are zero-shot learners[C]//Proceedings of the 10th International Conference on Learning Representations. 2022.
- [11] LIU A, DU X, WANG N. Efficient access control permission decision engine based on machine learning[J]. Security and Communication Networks. 2021, 1: 11.
- [12] STRAKOVÁ J, STRAKA M, HAJIC J. Neural architectures for nested NER through linearization[C]//Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics. 2019: 5326-5331.
- [13] YAN H, DENG B, LI X, et al. TENER: adapting transformer encoder for named entity recognition[J]. arXiv:1911.04474, 2019.
- [14] LIANG C, YU Y, JIANG H, et al. BOND: BERT-assisted open-domain named entity recognition with distant supervision[C]//The Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. 2020.
- [15] LI X Y, FENG J R, MENG Y X, et al. A unified MRC framework for named entity recognition[C]//Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics. 2020: 5849-5859.
- [16] YAN H, GUI T, DAI J Q, et al. A unified generative framework for various ner subtasks[C]//Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing. 2021: 5808-5822.
- [17] CHEN S, NEVES L, SOLORIO T. Style transfer as data augmentation: a case study on named entity recognition[C]//Proceedings of the 2022 Conference on Empirical Methods in Natural Language Processing. 2022: 1827-1841.
- [18] RAFFEL C, SHAZEER N, ROBERTS A, et al. Exploring the limits of transfer learning with a unified text-to-text transformer[J]. The Journal of Machine Learning Research. 2020, 21: 5485-5551.
- [19] LEE D H, KADAKIA A, TAN K, et al. Good examples make a faster LEARNER: simple demonstration-based learning for low-resource ner[C]//Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics. 2022: 2687-2700.
- [20] CHEN J W, LU Y J, LIN H Y, et al. Learning in-context learning for named entity recognition[C]//Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics. 2023: 13661-13675.
- [21] ZHANG J, LIU X, LAI X, et al. 2INER: instructive and in-context learning on few-shot named entity recognition[C]//Findings of the Association for Computational Linguistics: EMNLP 2023. 2023: 3940-3951.
- [22] MILLER G A. WordNet: a lexical database for english [J]. Commun ACM, 1995, 38: 39-41.
- [23] CUI L Y, WU Y, LIU J, et al. Template-based named entity recognition using bart[C]//Proceeding of Findings of the Association for Computational Linguistics: ACL-IJCNLP 2021. 2021: 1835-1845.
- [24] HOU Y P, ZHANG J J, LIN Z H, et al. Large language models are zero-shot rankers for recommender systems[C]//Proceedings of the 46th European Conference on Information Retrieval (ECIR 2024). 2024: 364-381.
- [25] FRIEDMAN L, AHUJA S, ALLEN D, et al. Leveraging large language models in conversational recommender systems[J]. arXiv: 2305.07961, 2023.
- [26] YANG J, LIANG S L, ZHANG Y. Design challenges and misconceptions in neural sequence labeling[C]//Proceedings of the 27th International Conference on Computational Linguistics. 2018: 3879-3889.
- [27] LIANG C, YU Y, JIANG H, et al. Bond: Bert-assisted open-domain named entity recognition with distant supervision[C]//Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. 2020: 1054-1064.
- [28] STRUBELL E, VERGA P, BELANGER D, et al. Fast and accurate entity recognition with iterated dilated convolutions[C]//The 2017

Conference on Empirical Methods in Natural Language Processing. 2017: 2670-2680.

- [29] CUI L Y, ZHANG Y. Hierarchically-refined label attention network for sequence labeling[C]//The 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP). 2019: 4115-4128.
- [30] CHEN X, LI L, DENG S M, et al. LightNER: a lightweight tuning paradigm for low-resource ner via pluggable prompting[C]//Proceedings of the 29th International Conference on Computational Linguistics. 2022: 2374-2387.
- [31] HUANG J, LI C, SUBUDHI K, et al. Few-shot named entity recognition: an empirical baseline study[C]//Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing. 2021: 10408-10423.
- [32] DEVLIN J, CHANG M W, LEE K, et al. BERT: pre-training of deep bidirectional transformers for language understanding[C]//Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies. 2019: 4171-4186.
- [33] MA R T, ZHOU X, GUI T, et al. Template-free prompt tuning for few-shot ner[C]//Proceedings of the 2022 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies. 2022: 5721-5732.

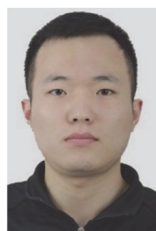
[作者简介]



李晨皓（1992-），男，贵州贵阳人，信息工程大学硕士生，主要研究方向为访问控制技术和自然语言处理。



王娜（1980-），女，山西临汾人，博士，信息工程大学教授，主要研究方向为信息系统安全、大数据和区块链安全。



刘敖迪（1992-），男，黑龙江伊春人，博士，信息工程大学讲师，主要研究方向为大数据安全。