报告正文

参照以下提纲撰写，要求内容翔实、清晰，层次分明，标题突出。**请勿删除或改动下述提纲标题及括号中的文字。**

（一）立项依据与研究内容(建议8000字以下)：

1.**项目的立项依据**（研究意义、国内外研究现状及发展动态分析，需结合科学研究发展趋势来论述科学意义；或结合国民经济和社会发展中迫切需要解决的关键科技问题来论述其应用前景。附主要参考文献目录）；

1.1 研究背景与科学意义

在信息系统中，基于用户历史行为数据进行异常检测可以帮助发现复杂系统中的异常事件、潜在风险因素或者突变模式，从而对系统安全性、稳定性和健康状态进行监测和管理。例如，针对跨媒体人物行为的异常检测可以及时发现异常行为，防范危害公共安全事件；基于多源异构系统日志抽取用户行为并进行异常检测，可以支撑网络入侵检测和内部威胁检测等安全应用；在电子商务平台中分析用户行为可以挖掘用户的违法交易行为，保障数字经济安全。然而，**随着网络和信息系统的发展，用户行为描述形式日益丰富和多样化，仅仅分析用户行为序列，无法准确描述行为语义，难以识别真实的异常行为和用户，也无法得到异常推断的原因。**

以内部威胁检测为例，图 1展示了某用户离职前违规盗取原单位项目源代码和用户数据，为实现改目标，该用户产生多个行为，被分散记录在不同的日志中，包括网络日志、操作系统日志、数据库日志和应用日志，以及防火墙和杀毒软件日志，这些日志的结构各不相同，用户行为的抽取方法和描述方式也不相同。仅分析单一来源的日志无法形成对用户行为和意图的整体认知，难以准确检测用户的异常行为和异常用户。为准确检测该用户的异常行为，必须融合上述多源异构日志数据行分析。类似地，面向公共安全事件的人物异常行为检测需要对关键人物在多媒体平台上的数据进行综合分析研判，包括其社交网络言论、交通信息、购物记录等多源异构数据；而在电子商务平台中，需要融合用户交易记录、历史评价、好友关系、关注和收藏等信息，才能综合分析用户意图，准确识别异常行为。因此，用户行为异常检测需要分析多源异构用户行为数据。

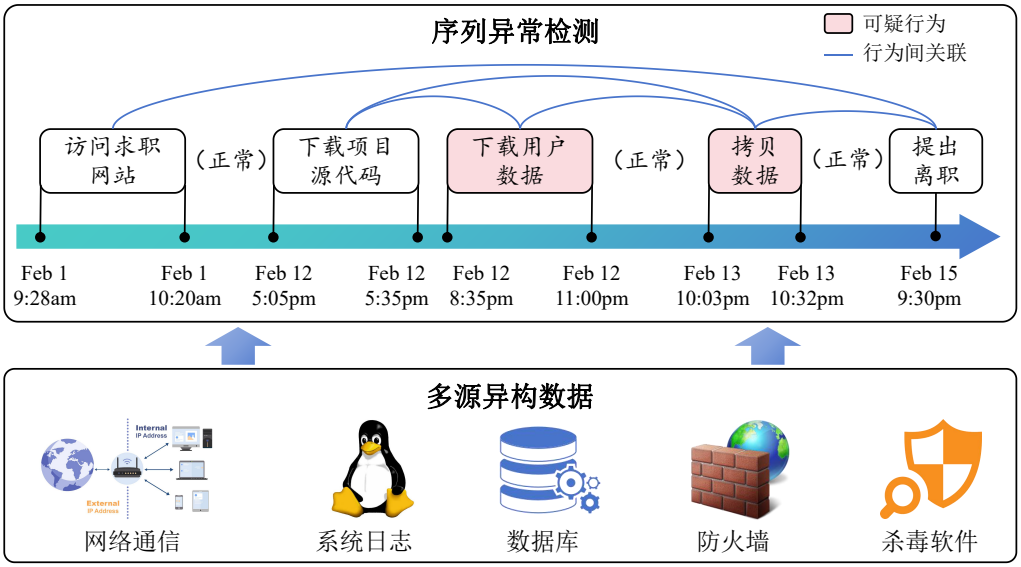

图 1: 多源异构数据融合的序列异常检测示例。

基于多源异构数据的行为异常检测不仅是学术界的研究热点，也得到了工业界的极大关注。国内外高校（清华大学、上海交通大学，新加坡国立大学、普渡大学、卡内基梅隆大学）和研究机构（中国科学院自动化研究所、IBM、亚马逊、华为、阿里巴巴），均致力于异常检测研究。 2023年清华大学、南开大学和中国计算机学会联合举办国际智能运维挑战赛，[1]参赛队伍基于多源异构数据进行异常检测、故障定位和故障分类等。 2022年亚马逊和多所国际知名高校在SIGKDD会议组织题为“异常和新颖性检测、解释和调节”研讨会（ANDEA），[2]，关注复杂信息系统中的异常和新颖性检测的新技术、模型解释和改进方法。可见，基于多源异构数据的异常检测是目前国内外研究热点。

目前用于用户行为异常检测的传统机器学习或者深度学习模型，大都关注行为序列的异常检测，缺乏对多源异构数据的建模能力，无法准确建模用户行为意图，异常检测准确率和泛化性较差。现有研究表明，目前异常检测研究的数据场景比较简单，即使用传统机器学习方法也能取得很好的效果，大部分模型的泛化性能不佳，实际应用效果不够理想[1]。目前，现有针对多源异构数据的行为异常检测仍存在以下问题：

(1) 行为数据的异构性。随着信息系统的发展，对用户行为的描述日益多样化，就异常网络攻击检测而言，涉及网络拓扑信息、网络配置信息、审计日志、

[1]http://aiops-challenge.com

[2]https://sites.google.com/view/andea2022/

网络流量监测数据和入侵监测系统告警信息等，各类数据形式各异，数据解析和关键信息抽取方式各不相同。行为数据的异构性导致模型难以对这些数据进行有效建模，因而行为语义表征不完备，难以取得较好的异常检测效果。

(2) 异常行为的隐蔽性。在大规模用户行为数据中心，因为异常行为通常比较隐蔽，其占比极小，例如，在内部威胁检测广泛采用的数据集CERT 5.2[2]中，正负样本比例约为7750 : 1。可见，异常行为的隐蔽性导致正负样本极不平衡。现有主流方法采用无监督学习，无法利用异常标签的监督信息。另一方面，在现实数据场景中，部分隐蔽行为尚未发现，缺少异常行为的标签，容易混淆模型。因此，异常行为的隐蔽性是异常检测的重要挑战之一。

(3) 异常行为的分散性。用户通常需要采取多个行为才能达到某个恶意目的，甚至某个恶意事件是由多名用户协同实施的。异常行为的分散性是指在时间维度上异常行为的连续性较差，在空间上异常行为是在不同地点或者从不同设备发起的。只有综合分析分散的异常行为，才能理解异常行为协作模式，为保障相关系统安全提供指导。然而，异常事件总体数量较少，仅分析用户数据难以归纳多个行为之间的协作模式。

动态异质图为多源异构数据建模和用户行为异常检测提供了新思路。动态异质图（Evolving Heterogeneous Graph）具有多类型的节点和边，同时，节点和边的类型，以及图结构随着时间动态演化。目前，动态异质图是国内外的热点方向，在社交网络、推荐系统、生物信息学等领域逐步开展应用。 2022年NeurIPS会议联合斯坦福大学举办第二届大规模图数据挑战赛Open Graph Benchmark Large-Scale Challenge挑战赛，[3]赛题涵盖图分类、链路预测和图回归等。2023年SIGKDD会议组织International Workshop on Mining and Learning with Graphs，[4]主要关注点之一就是用图建模异构数据。

本项目拟基于多源异构数据构建动态异质图，从时间、结构和语义三方面建模用户行为数据。动态异质图的节点表示用户、设备、数据资源、服务器等多类型实体，边表示用户行为（例如下载数据）、实体间关系等，节点、边的类型和结构随时间的动态演化。

---

[3]https://ogb.stanford.edu/neurips2022/

[4]https://www.mlgworkshop.org/2023/

1.2 国内外相关工作

1.2.1 多源异构数据融合的行为表征

(1) 基于动态异质图的行为建模

(2) 节点表征

(3) 链路表征

1.2.2 行为异常检测

(1) 用户行为异常检测

(2) 动态异质图异常检测

1.2.3 异常预警关联分析

(1) 异常协作检测

(2) 外源知识辅助的事件关联分析

1.2.4 立论总结

参考文献

[1] WU R, KEOGH E J. Current time series anomaly detection benchmarks are flawed and are creating the illusion of progress[J/OL]. IEEE Transactions on Knowledge and Data Engineering, 2020, 35: 2421-2429. https://api.semanticscholar.org/CorpusID:221995939.

[2] GLASSER J, LINDAUER B. Bridging the gap: A pragmatic approach to generating insider threat data[J/OL]. 2013 IEEE Security and Privacy Workshops, 2013: 98-104. https://api.semanticscholar.org/CorpusID:7645357.

2. **项目的研究内容、研究目标，以及拟解决的关键科学问题**（此部分为重点阐述内容）；

3. **拟采取的研究方案及可行性分析**（包括研究方法、技术路线、实验手段、关键技术等说明）；

4. **本项目的特色与创新之处；**

5. **年度研究计划及预期研究结果**（包括拟组织的重要学术交流活动、国际合作与交流计划等）。

（二）研究基础与工作条件

1. **研究基础**（与本项目相关的研究工作积累和已取得的研究工作成绩）；

2. **工作条件**（包括已具备的实验条件，尚缺少的实验条件和拟解决的途径，包括利用国家实验室、国家重点实验室和部门重点实验室等研究基地的计划与落实情况）；

3. **正在承担的与本项目相关的科研项目情况**（申请人和主要参与者正在承担的与本项目相关的科研项目情况，包括国家自然科学基金的项目和国家其他科技计划项目，要注明项目的资助机构、项目类别、批准号、项目名称、获资助金额、起止年月、与本项目的关系及负责的内容等）；

无。

4. **完成国家自然科学基金项目情况**（对申请人负责的前一个已资助期满的科学基金项目（项目名称及批准号）完成情况、后续研究进展及与本申请项目的关系加以详细说明。另附该项目的研究工作总结摘要（限500字）和相关成果详细目录）。

（三）其他需要说明的情况

1. 申请人同年申请不同类型的国家自然科学基金项目情况（列明同年申请的其他项目的项目类型、项目名称信息，并说明与本项目之间的区别与联系）。

无。

2. 具有高级专业技术职务（职称）的申请人或者主要参与者是否

存在同年申请或者参与申请国家自然科学基金项目的单位不一致的情况；如存在上述情况，列明所涉及人员的姓名，申请或参与申请的其他项目的项目类型、项目名称、单位名称、上述人员在该项目中是申请人还是参与者，并说明单位不一致原因。

无。

3. 具有高级专业技术职务（职称）的申请人或者主要参与者是否存在与正在承担的国家自然科学基金项目的单位不一致的情况；如存在上述情况，列明所涉及人员的姓名，正在承担项目的批准号、项目类型、项目名称、单位名称、起止年月，并说明单位不一致原因。

无。

4. 其他。

无。