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

行为序列记录一系列按照时间顺序发生的用户行为，从大规模行为序列中识别异常行为具有重要的应用价值，得到了学术界和工业界的广泛关注。针对人物行为序列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；抽取网络和系统日志中的用户行为序列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序列可以挖掘用户异常交易行为，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，面向用户行为序列的异常检测需要分析多源异构用户行为数据。

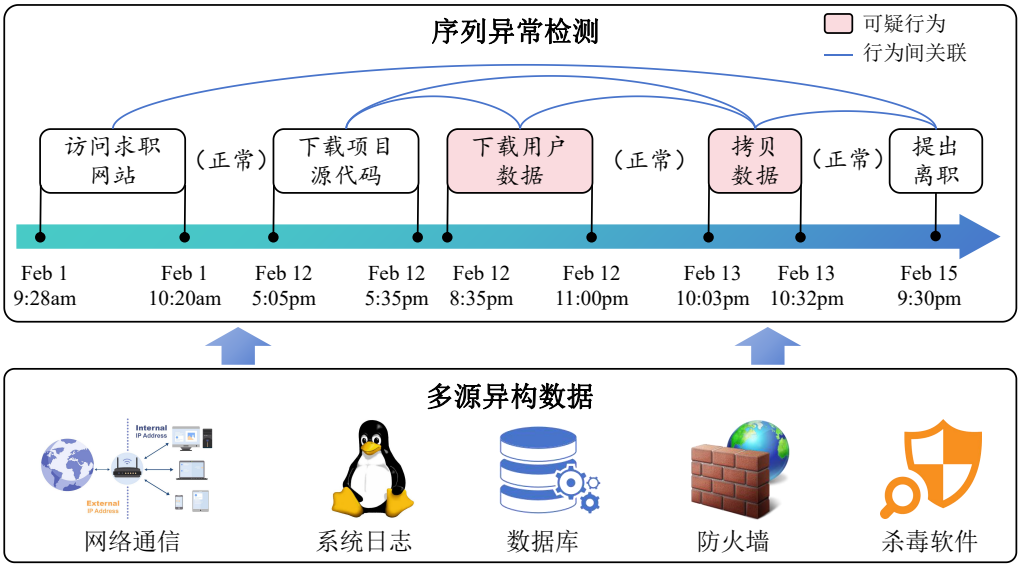

图 1: 多源异构数据融合的序列异常检测示例。

1.2 国内外相关工作

参考文献

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。