(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 113706149 A
(43)申请公布日 2021.11.26

(21)申请号 202111022309.7

(22)申请日 2021.09.01

(71)申请人 杨思亭
地址 529000 广东省江门市蓬江区港口二路95号101室

(72)发明人 杨思亭 朱刚

(74)专利代理机构 东莞市浩宇专利代理事务所(普通合伙) 44460
代理人 石艳丽

(51)Int.Cl.
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)
G06F 16/2458(2019.01)

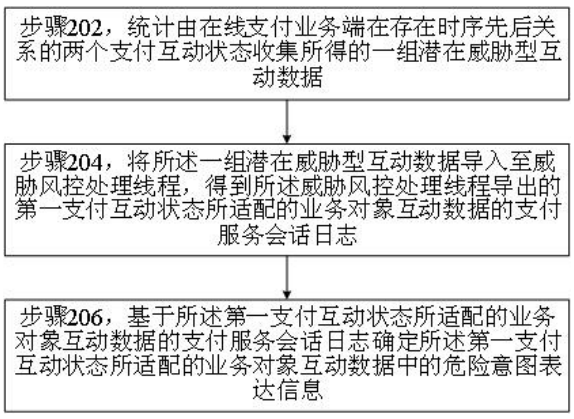
权利要求书4页 说明书16页 附图2页

(54)发明名称

一种应对在线支付数据威胁的大数据风控处理方法及系统

(57)摘要

本申请涉及的应对在线支付数据威胁的大数据风控处理方法及系统，鉴于危险意图表达信息的确定是基于与危险意图存在紧密关联的支付服务会话日志实现的，可以精准全面地定位出不同的支付环境中危险意图目标事件，从支付服务会话日志中识别危险意图目标事件，结合支付环境分析将危险意图目标事件中的危险意图表达信息进行完善。基于AI智能的支付服务会话日志分析策略在保障支付服务会话日志精度和丰富程度的同时，能尽可能提高处理效率。此外，能够基于危险意图表达信息确定业务对象在进行支付互动时的各种异常倾向信息，尽可能避免对异常倾向信息的漏检，进而确保数据威胁风控处理的前置检测阶段的准确性和可靠性。



CN 113706149 A

1.一种应对在线支付数据威胁的大数据风控处理方法,其特征在于,应用于大数据风控服务系统,包括:

统计由在线支付业务端在存在时序先后关系的两个支付互动状态收集所得的一组潜在威胁型互动数据;

将所述一组潜在威胁型互动数据导入至威胁风控处理线程,得到所述威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志;

基于所述第一支付互动状态所适配的业务对象互动数据的支付服务会话日志确定所述第一支付互动状态所适配的业务对象互动数据中的危险意图表达信息。

2.根据权利要求1所述的方法,其特征在于,存在时序先后关系的两个支付互动状态包括第一支付互动状态和第二支付互动状态,所述在线支付业务端包括境内支付业务端和跨境支付业务端,所述境内支付业务端在第一支付互动状态收集所得的潜在威胁型互动数据为第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据,所述跨境支付业务端在第一支付互动状态收集所得的潜在威胁型互动数据为第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据,所述境内支付业务端在第二支付互动状态收集所得的潜在威胁型互动数据为第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据,所述跨境支付业务端在第二支付互动状态收集所得的潜在威胁型互动数据为第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据;

所述第一支付互动状态所适配的业务对象互动数据为所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据或所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据,所述威胁风控处理线程是通过多组第一调试范例通过智能化分析调试得到的,所述多组第一调试范例中的每组第一调试范例包括:所述在线支付业务端在存在时序先后关系的两个支付互动状态收集所得的潜在威胁型互动数据以及支付服务会话日志主题。

3.根据权利要求2所述的方法,其特征在于,基于所述第一支付互动状态所适配的业务对象互动数据的支付服务会话日志确定所述第一支付互动状态所适配的业务对象互动数据中的危险意图表达信息,包括:

通过会话解析策略对所述支付服务会话日志进行解析,得到所述第一支付互动状态所适配的业务对象互动数据中的危险意图事件;

依据第一支付环境挖掘子线程对所述第一支付互动状态所适配的业务对象互动数据中的支付环境表达信息进行挖掘得到第一支付环境特征,其中,所述第一支付环境挖掘子线程是通过多组第二调试范例通过智能化分析调试得到的,所述多组第二调试范例中的每组第二调试范例包括:潜在威胁型互动数据以及第一挖掘主题;

将所述危险意图事件与所述第一支付环境特征进行绑定得到所述危险意图表达信息。

4.根据权利要求2所述的方法,其特征在于,所述威胁风控处理线程中包括互动数据处理子线程、第一描述识别子线程和第二支付环境挖掘子线程,其中,将所述一组潜在威胁型互动数据导入至威胁风控处理线程,得到所述威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志,包括:

将所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互

动数据处理子线程,得到所述互动数据处理子线程导出的第一数据差异分析情况,以及将所述第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互动数据处理子线程,得到所述互动数据处理子线程导出的第二数据差异分析情况,其中,所述互动数据处理子线程是通过多组第三调试范例通过智能化分析调试得到的,所述多组第三调试范例中的每组第三调试范例包括:所述在线支付业务端在同一支付互动状态收集所得的两组潜在威胁型互动数据和互动数据差异化主题;

将所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据导入至所述第一描述识别子线程,得到所述第一描述识别子线程导出的云支付威胁描述,其中,所述第一描述识别子线程是通过多组第四调试范例通过智能化分析调试得到的,所述多组第四调试范例中的每组第四调试范例包括:所述在线支付业务端中的境内支付业务端在存在时序先后关系的两个支付互动状态收集所得的潜在威胁型互动数据和交互特征主题;

使用第二支付环境挖掘子线程对所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据中的支付环境表达信息进行挖掘得到第二支付环境表达信息,其中,所述第二支付环境挖掘子线程是通过多组第五调试范例通过智能化分析调试得到的,所述多组第五调试范例中的每组第五调试范例包括:潜在威胁型互动数据和第二表达信息挖掘主题;

基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述云支付威胁描述和所述第二支付环境表达信息确定所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志。

5.根据权利要求4所述的方法,其特征在于,基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述云支付威胁描述和所述第二支付环境表达信息确定所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志,包括:

基于所述云支付威胁描述对所述第二数据差异分析情况进行危险意图倾向分析,得到将所述第二数据差异分析情况匹配至所述第一支付互动状态的第一互动数据切换情况;

使用所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付环境表达信息对所述第一互动数据切换情况进行优化,得到第一互动数据优化结果;

通过所述第一互动数据优化结果、所述第一数据差异分析情况和所述云支付威胁描述得到所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志。

6.根据权利要求4或5所述的方法,其特征在于,所述威胁风控处理线程导出的所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志与事先设置的所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的在先支付服务会话日志之间的第一服务互动检测结果符合第一目标检测要求,所述第一目标检测要求用于表征所述第一服务互动检测结果的量化检测结果在第一设定约束区间之内。

7.根据权利要求2所述的方法，其特征在于，所述威胁风控处理线程中包括互动数据处理子线程、第二描述识别子线程和第二支付环境挖掘子线程，其中，将所述一组潜在威胁型互动数据导入至威胁风控处理线程，得到所述威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志，包括：

将所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互动数据处理子线程，得到所述互动数据处理子线程导出的第一数据差异分析情况，以及将所述第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互动数据处理子线程，得到所述互动数据处理子线程导出的第二数据差异分析情况，其中，所述互动数据处理子线程是通过多组第三调试范例通过智能化分析调试得到的，所述多组第三调试范例中的每组第三调试范例包括：所述在线支付业务端在同一支付互动状态收集所得的两组潜在威胁型互动数据和互动数据差异化主题；

将所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述第二描述识别子线程，得到所述第二描述识别子线程导出的跨境支付互动描述，其中，所述第二描述识别子线程是通过多组第六调试范例通过智能化分析调试得到的，所述多组第六调试范例中的每组第六调试范例包括：所述在线支付业务端中的跨境支付业务端在存在时序先后关系的两个支付互动状态收集所得的潜在威胁型互动数据和交互特征主题；

使用所述第二支付环境挖掘子线程对所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据中的支付环境表达信息进行挖掘得到第三支付环境表达信息，其中，所述第二支付环境挖掘子线程是通过多组第五调试范例通过智能化分析调试得到的，所述多组第五调试范例中的每组第五调试范例包括：潜在威胁型互动数据和第二表达信息挖掘主题；

基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述跨境支付互动描述和所述第三支付环境表达信息确定所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志。

8.根据权利要求7所述的方法，其特征在于，基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述跨境支付互动描述和所述第三支付环境表达信息确定所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志，包括：

基于所述跨境支付互动描述对所述第二数据差异分析情况进行危险意图倾向分析，得到将所述第二数据差异分析情况匹配至所述第一支付互动状态的第二互动数据切换情况；

使用所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据和所述第三支付环境表达信息对所述第二互动数据切换情况进行优化，得到第二互动数据优化结果；

通过所述第二互动数据优化结果、所述第一数据差异分析情况和所述跨境支付互动描述得到所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志。

9.根据权利要求7或8所述的方法，其特征在于，所述威胁风控处理线程导出的所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志与事先设置的所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的在先支付服务会话日志之间的第二服务互动检测结果符合第二目标检测要求，所述第二目标检测要求用于表征所述第二服务互动检测结果的量化检测结果在第二设定约束区间之内。

10.一种大数据风控服务系统，其特征在于，包括处理器和存储器；所述处理器和所述存储器通信连接，所述处理器用于从所述存储器中读取计算机程序并执行，以实现上述权利要求1-9任一项所述的方法。

一种应对在线支付数据威胁的大数据风控处理方法及系统

技术领域

[0001] 本申请涉及在线支付和大数据风控技术领域，特别涉及应对在线支付数据威胁的大数据风控处理方法及系统。

背景技术

[0002] 近年来，互联网支付市场呈现快速增长态势，在线支付市场的规模不断加速扩大，竞争加剧促使在线支付行业的集中度提升，由此造成的数据信息安全隐患不容忽视。随着电子商务的迅猛发展，消费者已不再满足于国内网购，开始将目光转向海外市场，跨境支付和境内支付的多样化支付模式给用户信息安全带来了更多的挑战。

[0003] 现目前，为了确保在线支付用户的相关重要隐私数据的安全性，通常会部署一系列的风控措施，而部署风控措施的首要条件之一是进行数据信息威胁检测，然而发明人发现，相关技术在进行数据信息威胁检测时，容易存在漏检现象，这样难以确保威胁检测的准确性和可靠性。

发明内容

[0004] 为改善相关技术中存在的技术问题，本申请提供了应对在线支付数据威胁的大数据风控处理方法及系统。

[0005] 本申请提供了一种应对在线支付数据威胁的大数据风控处理方法，应用于大数据风控服务系统，包括：

统计由在线支付业务端在存在时序先后关系的两个支付互动状态收集所得的一组潜在威胁型互动数据；

将所述一组潜在威胁型互动数据导入至威胁风控处理线程，得到所述威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志；

基于所述第一支付互动状态所适配的业务对象互动数据的支付服务会话日志确定所述第一支付互动状态所适配的业务对象互动数据中的危险意图表达信息。

[0006] 对于一些可独立实施的技术方案而言，存在时序先后关系的两个支付互动状态包括第一支付互动状态和第二支付互动状态，所述在线支付业务端包括境内支付业务端和跨境支付业务端，所述境内支付业务端在第一支付互动状态收集所得的潜在威胁型互动数据为第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据，所述跨境支付业务端在第一支付互动状态收集所得的潜在威胁型互动数据为第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据，所述境内支付业务端在第二支付互动状态收集所得的潜在威胁型互动数据为第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据，所述跨境支付业务端在第二支付互动状态收集所得的潜在威胁型互动数据为第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据；

所述第一支付互动状态所适配的业务对象互动数据为所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据或所述第一支付互动状态所适配的对

应于异地入侵风险的潜在威胁型互动数据，所述威胁风控处理线程是通过多组第一调试范例通过智能化分析调试得到的，所述多组第一调试范例中的每组第一调试范例包括：所述在线支付业务端在存在时序先后关系的两个支付互动状态收集所得的潜在威胁型互动数据以及支付服务会话日志主题。

[0007] 对于一些可独立实施的技术方案而言，基于所述第一支付互动状态所适配的业务对象互动数据的支付服务会话日志确定所述第一支付互动状态所适配的业务对象互动数据中的危险意图表达信息，包括：

通过会话解析策略对所述支付服务会话日志进行解析，得到所述第一支付互动状态所适配的业务对象互动数据中的危险意图事件；

依据第一支付环境挖掘子线程对所述第一支付互动状态所适配的业务对象互动数据中的支付环境表达信息进行挖掘得到第一支付环境特征，其中，所述第一支付环境挖掘子线程是通过多组第二调试范例通过智能化分析调试得到的，所述多组第二调试范例中的每组第二调试范例包括：潜在威胁型互动数据以及第一挖掘主题；

将所述危险意图事件与所述第一支付环境特征进行绑定得到所述危险意图表达信息。

[0008] 对于一些可独立实施的技术方案而言，所述威胁风控处理线程中包括互动数据处理子线程、第一描述识别子线程和第二支付环境挖掘子线程，其中，将所述一组潜在威胁型互动数据导入至威胁风控处理线程，得到所述威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志，包括：

将所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互动数据处理子线程，得到所述互动数据处理子线程导出的第一数据差异分析情况，以及将所述第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互动数据处理子线程，得到所述互动数据处理子线程导出的第二数据差异分析情况，其中，所述互动数据处理子线程是通过多组第三调试范例通过智能化分析调试得到的，所述多组第三调试范例中的每组第三调试范例包括：所述在线支付业务端在同一支付互动状态收集所得的两组潜在威胁型互动数据和互动数据差异化主题；

将所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据导入至所述第一描述识别子线程，得到所述第一描述识别子线程导出的云支付威胁描述，其中，所述第一描述识别子线程是通过多组第四调试范例通过智能化分析调试得到的，所述多组第四调试范例中的每组第四调试范例包括：所述在线支付业务端中的境内支付业务端在存在时序先后关系的两个支付互动状态收集所得的潜在威胁型互动数据和交互特征主题；

使用第二支付环境挖掘子线程对所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据中的支付环境表达信息进行挖掘得到第二支付环境表达信息，其中，所述第二支付环境挖掘子线程是通过多组第五调试范例通过智能化分析调试得到的，所述多组第五调试范例中的每组第五调试范例包括：潜在威胁型互动数据和第二表达信息挖掘主题；

基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述云支付威胁描述和所述第二支付环境表达信息确定所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志。

[0009] 对于一些可独立实施的技术方案而言，基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述云支付威胁描述和所述第二支付环境表达信息确定所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志，包括：

基于所述云支付威胁描述对所述第二数据差异分析情况进行危险意图倾向分析，得到将所述第二数据差异分析情况匹配至所述第一支付互动状态的第一互动数据切换情况；

使用所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付环境表达信息对所述第一互动数据切换情况进行优化，得到第一互动数据优化结果；

通过所述第一互动数据优化结果、所述第一数据差异分析情况和所述云支付威胁描述得到所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志。

[0010] 对于一些可独立实施的技术方案而言，所述威胁风控处理线程导出的所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志与事先设置的所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的在先支付服务会话日志之间的第一服务互动检测结果符合第一目标检测要求，所述第一目标检测要求用于表征所述第一服务互动检测结果的量化检测结果在第一设定约束区间之内。

[0011] 对于一些可独立实施的技术方案而言，所述威胁风控处理线程中包括互动数据处理子线程、第二描述识别子线程和第二支付环境挖掘子线程，其中，将所述一组潜在威胁型互动数据导入至威胁风控处理线程，得到所述威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志，包括：

将所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互动数据处理子线程，得到所述互动数据处理子线程导出的第一数据差异分析情况，以及将所述第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互动数据处理子线程，得到所述互动数据处理子线程导出的第二数据差异分析情况，其中，所述互动数据处理子线程是通过多组第三调试范例通过智能化分析调试得到的，所述多组第三调试范例中的每组第三调试范例包括：所述在线支付业务端在同一支付互动状态收集所得的两组潜在威胁型互动数据和互动数据差异化主题；

将所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述第二描述识别子线程，得到所述第二描述识别子线程导出的跨境支付互动描述，其中，所述第二描述识别子线程是通过多组第六调试范例通过智能化分析调试得到的，所述多组第

六调试范例中的每组第六调试范例包括:所述在线支付业务端中的跨境支付业务端在存在时序先后关系的两个支付互动状态收集所得的潜在威胁型互动数据和交互特征主题;

使用所述第二支付环境挖掘子线程对所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据中的支付环境表达信息进行挖掘得到第三支付环境表达信息,其中,所述第二支付环境挖掘子线程是通过多组第五调试范例通过智能化分析调试得到的,所述多组第五调试范例中的每组第五调试范例包括:潜在威胁型互动数据和第二表达信息挖掘主题;

基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述跨境支付互动描述和所述第三支付环境表达信息确定所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志。

[0012] 对于一些可独立实施的技术方案而言,基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述跨境支付互动描述和所述第三支付环境表达信息确定所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志,包括:

基于所述跨境支付互动描述对所述第二数据差异分析情况进行危险意图倾向分析,得到将所述第二数据差异分析情况匹配至所述第一支付互动状态的第二互动数据切换情况;

使用所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据和所述第三支付环境表达信息对所述第二互动数据切换情况进行优化,得到第二互动数据优化结果;

通过所述第二互动数据优化结果、所述第一数据差异分析情况和所述跨境支付互动描述得到所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志。

[0013] 对于一些可独立实施的技术方案而言,所述威胁风控处理线程导出的所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志与事先设置的所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的在先支付服务会话日志之间的第二服务互动检测结果符合第二目标检测要求,所述第二目标检测要求用于表征所述第二服务互动检测结果的量化检测结果在第二设定约束区间之内。

[0014] 本申请还提供了一种大数据风控服务系统,包括处理器和存储器;所述处理器和所述存储器通信连接,所述处理器用于从所述存储器中读取计算机程序并执行,以实现上述的方法。

[0015] 本申请的实施例提供的技术方案可以包括以下有益效果。

[0016] 通过本申请,统计由在线支付业务端在存在时序先后关系的两个支付互动状态收集所得的一组潜在威胁型互动数据,将一组潜在威胁型互动数据导入至威胁风控处理线程,得到威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志,基于第一支付互动状态所适配的业务对象互动数据的支付服务会话日志确定第一支付互动状态所适配的业务对象互动数据中的危险意图表达信息。鉴于危险意图表达信息的确定是基于与危险意图存在紧密关联的支付服务会话日志实现的,可以精准全面地

定位出不同的支付环境中危险意图目标事件，从支付服务会话日志中识别危险意图目标事件，结合支付环境分析将危险意图目标事件中的危险意图表达信息进行完善。本申请使用基于AI智能的支付服务会话日志分析策略在保障支付服务会话日志精度和丰富程度的同时，能尽可能提高处理效率。如此设计，能够基于危险意图表达信息确定业务对象在进行支付互动时的各种异常倾向信息，尽可能避免对异常倾向信息的漏检，进而确保数据威胁风控处理的前置检测阶段的准确性和可靠性。

附图说明

[0017] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本申请的实施例，并于说明书一起用于解释本申请的原理。

[0018] 图1是本申请实施例提供的一种大数据风控服务系统的硬件结构示意图。

[0019] 图2是本申请实施例提供的一种应对在线支付数据威胁的大数据风控处理方法的流程图。

[0020] 图3是本申请实施例提供的一种应对在线支付数据威胁的大数据风控处理装置的结构框图。

[0021] 图4是本申请实施例提供的一种应对在线支付数据威胁的大数据风控处理方法的实施环境的通信架构示意图。

具体实施方式

[0022] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0023] 需要说明的是，本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。

[0024] 本申请实施例一所提供的方法实施例可以在大数据风控服务系统、计算机终端或者类似的运算装置中执行。以运行在大数据风控服务系统上为例，图1是本申请实施例的一种应对在线支付数据威胁的大数据风控处理方法的大数据风控服务系统的硬件结构框图。如图1所示，大数据风控服务系统100可以包括一个或多个(图1中仅示出一个)处理器102(处理器102可以包括但不限于微处理器MCU或可编程逻辑器件FPGA等的处理装置)和用于存储数据的存储器104，可选地，上述大数据风控服务系统还可以包括用于通信功能的传输设备106。本领域普通技术人员可以理解，图1所示的结构仅为示意，其并不对上述大数据风控服务系统100的结构造成限定。例如，大数据风控服务系统100还可包括比图1中所示更多或者更少的组件，或者具有与图1所示不同的配置。

[0025] 存储器104可用于存储计算机程序，例如，应用软件的软件程序以及模块，如本申请实施例中的应对在线支付数据威胁的大数据风控处理方法所适配的计算机程序，处理器102通过运行存储在存储器104内的计算机程序，从而执行各种功能应用以及数据处理，即实现上述的方法。存储器104可包括高速随机存储器，还可包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器104可进

一步包括相对于处理器102远程设置的存储器，这些远程存储器可以通过网络连接至大数据风控服务系统100。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0026] 传输装置106用于经由一个网络接收或者发送数据。上述的网络具体实例可包括大数据风控服务系统100的通信供应商提供的无线网络。在一个实例中，传输装置106包括一个网络适配器(Network Interface Controller，简称为NIC)，其可通过基站与其他网络设备相连从而可与互联网进行通讯。在一个实例中，传输装置106可以为射频(Radio Frequency，简称为RF)模块，其用于通过无线方式与互联网进行通讯。

[0027] 在本申请实施例中提供了一种运行于上述大数据风控服务系统的应对在线支付数据威胁的大数据风控处理方法，图2是基于本申请实施例的应对在线支付数据威胁的大数据风控处理方法的流程图，如图2所示，该流程可以包括如下步骤所描述的内容。

[0028] 步骤202，统计由在线支付业务端在存在时序先后关系的两个支付互动状态收集所得的一组潜在威胁型互动数据，其中，存在时序先后关系的两个支付互动状态包括第一支付互动状态和第二支付互动状态，所述在线支付业务端包括境内支付业务端和跨境支付业务端，所述境内支付业务端在第一支付互动状态收集所得的潜在威胁型互动数据为第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据，所述跨境支付业务端在第一支付互动状态收集所得的潜在威胁型互动数据为第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据，所述境内支付业务端在第二支付互动状态收集所得的潜在威胁型互动数据为第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据，所述跨境支付业务端在第二支付互动状态收集所得的潜在威胁型互动数据为第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据。

[0029] 步骤204，将所述一组潜在威胁型互动数据导入至威胁风控处理线程，得到所述威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志，其中，所述第一支付互动状态所适配的业务对象互动数据为所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据或所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据，所述威胁风控处理线程是通过多组第一调试范例通过智能化分析调试得到的，所述多组第一调试范例中的每组第一调试范例包括：所述在线支付业务端在存在时序先后关系的两个支付互动状态收集所得的潜在威胁型互动数据以及支付服务会话日志主题。

[0030] 步骤206，基于所述第一支付互动状态所适配的业务对象互动数据的支付服务会话日志确定所述第一支付互动状态所适配的业务对象互动数据中的危险意图表达信息。

[0031] 在一些可独立实施的设计思路下，对于在线支付业务端在前后两个存在时序先后关系的的支付互动状态，第一支付互动状态state和第二支付互动状态state+1，有境内和跨境两个支付业务端分别收集所得的一组潜在威胁型互动数据包括第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据domestic_risk_data_state0，第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据cross-border_risk_data_state0，第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据domestic_risk_data_state1，第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据cross-border_risk_data_state1四组潜在威胁型互动数据。在本申请实施

例中可以将对应于本地入侵风险的潜在威胁型互动数据作为模板潜在威胁型互动数据，也可以将对应于异地入侵风险的潜在威胁型互动数据作为模板潜在威胁型互动数据。在将对应于本地入侵风险的潜在威胁型互动数据作为模板潜在威胁型互动数据的前提下，第一支付互动状态所适配的业务对象互动数据为第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据domestic_risk_data_state0。在将对应于异地入侵风险的潜在威胁型互动数据作为模板潜在威胁型互动数据作为模板潜在威胁型互动数据的前提下，第一支付互动状态所适配的业务对象互动数据为第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据cross-border_risk_data_state0。

[0032] 对于一些可独立实施的实施方式，威胁风控处理线程是通过多组调试范例通过智能化分析调试得到的，将一组潜在威胁型互动数据导入至该威胁风控处理线程可以得到第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据domestic_risk_data_state0的支付服务会话日志，也可以得到对应于异地入侵风险的潜在威胁型互动数据cross-border_risk_data_state0的支付服务会话日志。通过该支付服务会话日志可以确定出在第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据domestic_risk_data_state0中危险意图的表达信息，也可以确定出在第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据cross-border_risk_data_state0中危险意图的表达信息。

[0033] 基于上述内容，统计由在线支付业务端在存在时序先后关系的两个支付互动状态收集所得的一组潜在威胁型互动数据，将一组潜在威胁型互动数据导入至威胁风控处理线程，得到威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志，基于第一支付互动状态所适配的业务对象互动数据的支付服务会话日志确定第一支付互动状态所适配的业务对象互动数据中的危险意图表达信息。鉴于危险意图表达信息的确定是基于与危险意图存在紧密关联的支付服务会话日志实现的，可以精准全面地定位出不同的支付环境中危险意图目标事件，从支付服务会话日志中识别危险意图目标事件，结合支付环境分析将危险意图目标事件中的危险意图表达信息进行完善。本申请使用基于AI智能的支付服务会话日志分析策略在保障支付服务会话日志精度和丰富程度的同时，能尽可能提高处理效率。如此设计，能够基于危险意图表达信息确定业务对象在进行支付互动时的各种异常倾向信息，尽可能避免对异常倾向信息的漏检，进而确保数据威胁风控处理的前置检测阶段的准确性和可靠性。

[0034] 在一些可独立实施的设计思路下，基于所述第一支付互动状态所适配的业务对象互动数据的支付服务会话日志确定所述第一支付互动状态所适配的业务对象互动数据中的危险意图表达信息，包括：通过会话解析策略对所述支付服务会话日志进行解析，得到所述第一支付互动状态所适配的业务对象互动数据中的危险意图事件；依据第一支付环境挖掘子线程对所述第一支付互动状态所适配的业务对象互动数据中的支付环境表达信息进行挖掘得到第一支付环境特征，其中，所述第一支付环境挖掘子线程是通过多组第二调试范例通过智能化分析调试得到的，所述多组第二调试范例中的每组第二调试范例包括：潜在威胁型互动数据以及第一挖掘主题；将所述危险意图事件与所述第一支付环境特征进行绑定得到所述危险意图表达信息。

[0035] 对于一些可独立实施的实施方式，可以采用会话解析策略解析第一支付互动状态

所适配的对应于本地入侵风险的潜在威胁型互动数据domestic_risk_data_state0或第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据cross-border_risk_data_state0中的危险意图目标事件，下面为解析危险意图目标事件的相关内容，其中可以包括以下三个步骤：第一方面，使用设定分类网络提取支付服务会话日志；第二方面，使用基于多维特征聚类的会话解析策略对支付服务会话日志进行日志解析；第二方面，解析危险意图事件和请求响应事件，提取出危险意图目标事件(存在信息窃取和篡改等风险的意图对应的事件)。

[0036] 危险意图目标事件解析得到的结果可能包含多个危险意图目标，通过基于业务对象互动数据的支付环境解析方法将危险意图目标事件的每个目标支付环境进行完善。本申请实施例中第一支付环境挖掘子线程可以是基于智能化分析的AI智能网络(比如基于深度学习的神经网络)，使用基于智能化分析的AI智能对对应于本地入侵风险的潜在威胁型互动数据domestic_risk_data_state0或对应于异地入侵风险的潜在威胁型互动数据cross-border_risk_data_state0进行支付环境解析，得到每个支付环境的支付环境特征。然后通过支付环境特征进行支付环境解析并进行危险意图事件解析，能够得到危险意图目标事件。通过支付服务会话日志危险意图目标事件所适配的事件解析和支付环境解析来进行危险意图表达信息的确定，既可以利用支付服务会话日志与目标危险意图的紧密关联的特性，也可以利用支付环境解析的时效性的的优点，这样可以快速、准确地得到危险意图表达信息。

[0037] 在一些可独立实施的技术方案中，所述威胁风控处理线程中包括互动数据处理子线程、第一描述识别子线程(特征提取网络)和第二支付环境挖掘子线程(支付环境解析网络)，其中，将所述一组潜在威胁型互动数据导入至威胁风控处理线程，得到所述威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志，包括：将所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互动数据处理子线程，得到所述互动数据处理子线程导出的第一数据差异分析情况，以及将所述第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互动数据处理子线程，得到所述互动数据处理子线程导出的第二数据差异分析情况，其中，所述互动数据处理子线程是通过多组第三调试范例通过智能化分析调试得到的，所述多组第三调试范例中的每组第三调试范例包括：所述在线支付业务端在同一支付互动状态收集所得的两组潜在威胁型互动数据和互动数据差异化主题；将所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据导入至所述第一描述识别子线程，得到所述第一描述识别子线程导出的云支付威胁描述，其中，所述第一描述识别子线程是通过多组第四调试范例通过智能化分析调试得到的，所述多组第四调试范例中的每组第四调试范例包括：所述在线支付业务端中的境内支付业务端在存在时序先后关系的两个支付互动状态收集所得的潜在威胁型互动数据和交互特征主题；使用第二支付环境挖掘子线程对所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据中的支付环境表达信息进行挖掘得到第二支付环境表达信息，其中，所述第二支付环境挖掘子线程是通过多组第五调试范例通

过智能化分析调试得到的，所述多组第五调试范例中的每组第五调试范例包括：潜在威胁型互动数据和第二表达信息挖掘主题；基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述云支付威胁描述和所述第二支付环境表达信息确定所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志。

[0038] 在一些可独立实施的设计思路下，在相关实施例中将对应于本地入侵风险的潜在威胁型互动数据domestic_risk_data_state0作为模板潜在威胁型互动数据，例如，对于威胁风控处理线程而言，该威胁风控处理线程中可以包括互动数据处理子线程、第一描述识别子线程和第二支付环境挖掘子线程，将domestic_risk_data_state0，cross-border_risk_data_state0导入互动数据处理子线程计算出第一数据差异分析情况condition_state0。在一些可能的示例中，上述的互动数据处理子线程可以但不限于是卷积神经网络，将domestic_risk_data_state1，cross-border_risk_data_state1导入互动数据处理子线程计算出第二数据差异分析情况condition_state1，进一步地，可以将domestic_risk_data_state0和domestic_risk_data_state1导入至描述识别子线程计算出云支付威胁描述threat_description，其中，描述识别子线程可以是长短期记忆神经网络。

[0039] 在一些可独立实施的设计思路下，基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述云支付威胁描述和所述第二支付环境表达信息确定所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志，包括：基于所述云支付威胁描述对所述第二数据差异分析情况进行危险意图倾向分析，得到将所述第二数据差异分析情况匹配至所述第一支付互动状态的第一互动数据切换情况；使用所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付环境表达信息对所述第一互动数据切换情况进行优化，得到第一互动数据优化结果；通过所述第一互动数据优化结果、所述第一数据差异分析情况和所述云支付威胁描述得到所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志。

[0040] 在一些可独立实施的设计思路下，利用云支付威胁描述的结果将condition_state1按危险意图倾向分析，使得每个描述的量化描述数据变为支付互动状态state0的量化描述数据，进而得到后续的支付服务会话日志。本申请实施例中针对支付服务会话日志的确定使用了基于智能化分析的方法，可以快速、准确地确定支付服务会话日志。

[0041] 在一些可独立实施的设计思路下，所述威胁风控处理线程导出的所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志与事先设置的所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的在先支付服务会话日志之间的第一服务互动检测结果符合第一目标检测要求，所述第一目标检测要求用于表征所述第一服务互动检测结果的量化检测结果在第一设定约束区间之内。

[0042] 在一些可独立实施的设计思路下，支付服务会话日志网络可以预先配置两个服务互动检测结果对在线支付互动过程进行指导。第一个服务互动检测结果为check1，由第一数据差异分析情况condition_state0和经过云支付威胁描述threat_description将第二数据差异分析情况condition_state1映射后的互动数据切换情况condition_X确定得到。第二个服务互动检测结果check2，由支付服务会话日志和范例主题确定得到。

[0043] 在一些可独立实施的设计思路下，所述威胁风控处理线程中包括互动数据处理子

线程、第二描述识别子线程和第二支付环境挖掘子线程，其中，将所述一组潜在威胁型互动数据导入至威胁风控处理线程，得到所述威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志，包括：将所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互动数据处理子线程，得到所述互动数据处理子线程导出的第一数据差异分析情况，以及将所述第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互动数据处理子线程，得到所述互动数据处理子线程导出的第二数据差异分析情况，其中，所述互动数据处理子线程是通过多组第三调试范例通过智能化分析调试得到的，所述多组第三调试范例中的每组第三调试范例包括：所述在线支付业务端在同一支付互动状态收集所得的两组潜在威胁型互动数据和互动数据差异化主题；将所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述第二描述识别子线程，得到所述第二描述识别子线程导出的跨境支付互动描述，其中，所述第二描述识别子线程是通过多组第六调试范例通过智能化分析调试得到的，所述多组第六调试范例中的每组第六调试范例包括：所述在线支付业务端中的跨境支付业务端在存在时序先后关系的两个支付互动状态收集所得的潜在威胁型互动数据和交互特征主题；使用所述第二支付环境挖掘子线程对所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据中的支付环境表达信息进行挖掘得到第三支付环境表达信息，其中，所述第二支付环境挖掘子线程是通过多组第五调试范例通过智能化分析调试得到的，所述多组第五调试范例中的每组第五调试范例包括：潜在威胁型互动数据和第二表达信息挖掘主题；基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述跨境支付互动描述和所述第三支付环境表达信息确定所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志。

[0044] 对于一些可独立实施的实施方式，在本申请实施例中将延时交互云支付关键信息cross-border_risk_data_state0作为模板潜在威胁型互动数据，该威胁风控处理线程中包括互动数据处理子线程、第二描述识别子线程和第二支付环境挖掘子线程，将domestic_risk_data_state0，cross-border_risk_data_state0导入互动数据处理子线程计算出第一数据差异分析情况condition_state0，其中，互动数据处理子线程可以是卷积神经网络，将domestic_risk_data_state1，cross-border_risk_data_state1导入互动数据处理子线程计算出第二数据差异分析情况condition_state1，进一步地，还可以将cross-border_risk_data_state0和cross-border_risk_data_state1导入至描述识别子线程计算出跨境支付互动描述description，其中，描述识别子线程可以是长短期记忆神经网络。

[0045] 对于一些可独立实施的实施方式，基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述跨境支付互动描述和所述第三支付环境表达信息确定所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志，包括：基于所述跨境支付互动描述对所述第二数据差异分析情况进行危险意图倾向分析，得到将所述第二数据差异分析情况匹配至所述第一支付互动状态的第二互动数据切换情况；使用所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据和所述

第三支付环境表达信息对所述第二互动数据切换情况进行优化，得到第二互动数据优化结果；通过所述第二互动数据优化结果、所述第一数据差异分析情况和所述跨境支付互动描述得到所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志。

[0046] 在一些可独立实施的设计思路下，利用跨境支付互动描述的结果将condition_state1按危险意图倾向分析，使得每个支付行为事件的量化描述数据变为支付互动状态state0的量化描述数据，得到互动数据切换情况condition_X。

[0047] 在一些可独立实施的设计思路下，所述威胁风控处理线程导出的所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志与事先设置的所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的在先支付服务会话日志之间的第二服务互动检测结果符合第二目标检测要求，所述第二目标检测要求用于表征所述第二服务互动检测结果的量化检测结果在第二设定约束区间之内。

[0048] 对于一些可独立实施的实施方式，可以为支付服务会话日志网络预先设置两个服务互动检测结果以对在线支付互动过程进行指导。第一个服务互动检测结果为check1，由第一数据差异分析情况condition_state0和经过云支付威胁描述threat_description将第二数据差异分析情况condition_state1映射后的互动数据切换情况condition_X确定得到。第二个服务互动检测结果check2，由支付服务会话日志和范例主题确定得到。

[0049] 在上述内容的基础上，在确定出业务对象互动数据中的危险意图表达信息之后，还可以包括针对危险意图表达信息进行针对性风控策略配置的技术方案，基于此，在上述步骤202-步骤206的基础上，还可以包括以下可独立实施的内容：基于所述危险意图表达信息确定异常倾向行为描述，通过所述异常倾向行为描述确定与所述危险意图表达信息所适配的支付服务任务的信息风控机制(比如可以理解为针对信息安全的风控措施/风控策略)。

[0050] 对于一些可独立实施的实施方式，上述步骤“基于所述危险意图表达信息确定异常倾向行为描述，通过所述异常倾向行为描述确定与所述危险意图表达信息所适配的支付服务任务的信息风控机制”，可以通过以下步骤302-步骤308所描述的内容实现。

[0051] 步骤302，基于所述危险意图表达信息所适配的意图表达视觉记录确定目标支付业务用户的异常倾向行为描述。

[0052] 在本申请实施例中，意图表达视觉记录可以是基于危险意图表达信息整理得到的知识图谱，目标支付业务用户可以是进行云支付的用户，异常倾向行为描述用于表征目标支付业务用户进行云支付时的异常倾向行为描述比如频繁登录行为描述或者隐私信息套取行为描述等。

[0053] 步骤304，对所述目标支付业务用户的第一风险操作描述进行识别，得到所述第一风险操作描述的风险操作描述信息。

[0054] 在本申请实施例中，第一风险操作描述表征目标支付业务用户在进行云支付时的异常操作特征，风险操作描述信息表征对目标支付业务用户的第一风险操作描述进行识别所得到的异常操作特征信息，风险操作描述信息可以是纯文本数据也可以是视觉型图数据，在此不作限定。其中，对所述目标支付业务用户的第一风险操作描述进行识别，得到所述第一风险操作描述的风险操作描述信息，进一步还可以包括：对所述目标支付业务用户

的第一风险操作描述进行识别，得到所述第一风险操作描述的支付任务偏好以及所述第一风险操作描述的支付任务偏好的第一任务需求特征。

[0055] 步骤306，判断所述目标支付业务用户的用户主题类别是否为目标用户主题类别；如果所述目标支付业务用户的用户主题类别为所述目标用户主题类别，判断所述异常倾向行为描述中是否包括所述目标支付业务用户的视觉型风险倾向描述；如果所述异常倾向行为描述中包括所述目标支付业务用户的视觉型风险倾向描述，对所述目标支付业务用户的第二风险操作描述进行识别，得到所述第二风险操作描述的风险操作描述信息。在本申请实施例中，用户主题类别表征目标支付业务用户的身份主题信息，目标用户主题类别可以表征为进行云支付时所适配的支付操作主题，视觉型风险倾向描述可以是用户执行支付服务任务时的相关异常操作习惯所适配的特征信息，第二风险操作描述可以是与第一风险操作描述不相同的风险操作描述。其中，所述如果所述异常倾向行为描述中包括所述目标支付业务用户的视觉型风险倾向描述，对所述目标支付业务用户的第二风险操作描述进行识别，得到所述第二风险操作描述的风险操作描述信息，进一步还可以包括：对所述目标支付业务用户的第二风险操作描述进行识别，得到所述第二风险操作描述的支付任务偏好以及所述第二风险操作描述的支付任务偏好的第二任务需求特征。

[0056] 步骤308，基于所述第一风险操作描述的风险操作描述信息与所述第二风险操作描述的风险操作描述信息确定所述目标支付业务用户的支付任务偏好；通过所述支付任务偏好生成所适配的信息风控机制。

[0057] 可以理解，基于上述步骤302-步骤308，首先确定出目标支付业务用户的异常倾向行为描述，其次对目标支付业务用户的第一风险操作描述进行识别，得到第一风险操作描述的风险操作描述信息，这样能够准确地定位出目标支付业务用户在进行云支付时的各种异常倾向信息，此外，为了对目标支付业务用户定制针对性的支付服务任务，进一步对异常倾向行为描述中的视觉型风险倾向描述进行判断，并基于判断结果对目标支付业务用户的第二风险操作描述进行识别，以得到与第一风险操作描述不相同的第二风险操作描述信息，最后基于风险操作描述信息确定目标支付业务用户的支付任务偏好，这样能够基于支付任务偏好实时生成所适配的信息风控机制，从而确保支付任务顺利完成的前提下避免数据信息的丢失，进而提高信息风控机制的运行效率。

[0058] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到基于上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，或者网络设备等)执行本申请各个实施例所述的方法。

[0059] 在本申请实施例中还提供了一种应对在线支付数据威胁的大数据风控处理方法装置，该装置用于实现上述实施例及优选实施方式，已经进行过说明的不再赘述。如以下所使用的，术语“模块”可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来实现，但是硬件，或者软件和硬件的组合的实现也是可能并被构想的。

[0060] 图3是基于本申请实施例的应对在线支付数据威胁的大数据风控处理装置的结构框图，如图3所示，该装置包括：数据统计模块310，用于统计由在线支付业务端在存在时序

先后关系的两个支付互动状态收集所得的一组潜在威胁型互动数据，其中，存在时序先后关系的两个支付互动状态包括第一支付互动状态和第二支付互动状态，所述在线支付业务端包括境内支付业务端和跨境支付业务端，所述境内支付业务端在第一支付互动状态收集所得的潜在威胁型互动数据为第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据，所述跨境支付业务端在第一支付互动状态收集所得的潜在威胁型互动数据为第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据，所述境内支付业务端在第二支付互动状态收集所得的潜在威胁型互动数据为第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据，所述跨境支付业务端在第二支付互动状态收集所得的潜在威胁型互动数据为第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据；日志获取模块320，用于将所述一组潜在威胁型互动数据导入至威胁风控处理线程，得到所述威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志，其中，所述第一支付互动状态所适配的业务对象互动数据为所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据或所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据，所述威胁风控处理线程是通过多组第一调试范例通过智能化分析调试得到的，所述多组第一调试范例中的每组第一调试范例包括：所述在线支付业务端在存在时序先后关系的两个支付互动状态收集所得的潜在威胁型互动数据以及支付服务会话日志主题；意图确定模块330，用于基于所述第一支付互动状态所适配的业务对象互动数据的支付服务会话日志确定所述第一支付互动状态所适配的业务对象互动数据中的危险意图表达信息。

[0061] 可选地，上述装置通过如下方式实现所述基于所述第一支付互动状态所适配的业务对象互动数据的支付服务会话日志确定所述第一支付互动状态所适配的业务对象互动数据中的危险意图表达信息：通过会话解析策略对所述支付服务会话日志进行解析，得到所述第一支付互动状态所适配的业务对象互动数据中的危险意图事件；依据第一支付环境挖掘子线程对所述第一支付互动状态所适配的业务对象互动数据中的支付环境表达信息进行挖掘得到第一支付环境特征，其中，所述第一支付环境挖掘子线程是通过多组第二调试范例通过智能化分析调试得到的，所述多组第二调试范例中的每组第二调试范例包括：潜在威胁型互动数据以及第一挖掘主题；将所述危险意图事件与所述第一支付环境特征进行绑定得到所述危险意图表达信息。

[0062] 可选地，上述装置通过如下方式实现所述威胁风控处理线程中包括互动数据处理子线程、第一描述识别子线程和第二支付环境挖掘子线程，其中，将所述一组潜在威胁型互动数据导入至威胁风控处理线程，得到所述威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志：将所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互动数据处理子线程，得到所述互动数据处理子线程导出的第一数据差异分析情况，以及将所述第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互动数据处理子线程，得到所述互动数据处理子线程导出的第二数据差异分析情况，其中，所述互动数据处理子线程是通过多组第三调试范例通过智能化分析调试得到的，所述多组第三调试范例中的每组第三调试范例包括：所述在线支付

业务端在同一支付互动状态收集所得的两组潜在威胁型互动数据和互动数据差异化主题；将所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据导入至所述第一描述识别子线程，得到所述第一描述识别子线程导出的云支付威胁描述，其中，所述第一描述识别子线程是通过多组第四调试范例通过智能化分析调试得到的，所述多组第四调试范例中的每组第四调试范例包括：所述在线支付业务端中的境内支付业务端在存在时序先后关系的两个支付互动状态收集所得的潜在威胁型互动数据和交互特征主题；使用第二支付环境挖掘子线程对所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据中的支付环境表达信息进行挖掘得到第二支付环境表达信息，其中，所述第二支付环境挖掘子线程是通过多组第五调试范例通过智能化分析调试得到的，所述多组第五调试范例中的每组第五调试范例包括：潜在威胁型互动数据和第二表达信息挖掘主题；基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述云支付威胁描述和所述第二支付环境表达信息确定所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志。

[0063] 可选地，上述装置用于通过如下方式实现所述基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述云支付威胁描述和所述第二支付环境表达信息确定所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志：基于所述云支付威胁描述对所述第二数据差异分析情况进行危险意图倾向分析，得到将所述第二数据差异分析情况匹配至所述第一支付互动状态的第一互动数据切换情况；使用所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付环境表达信息对所述第一互动数据切换情况进行优化，得到第一互动数据优化结果；通过所述第一互动数据优化结果、所述第一数据差异分析情况和所述云支付威胁描述得到所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志。

[0064] 可选地，所述威胁风控处理线程导出的所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的支付服务会话日志与事先设置的所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据的在先支付服务会话日志之间的第一服务互动检测结果符合第一目标检测要求，所述第一目标检测要求用于表征所述第一服务互动检测结果的量化检测结果在第一设定约束区间之内。

[0065] 可选地，所述威胁风控处理线程中包括互动数据处理子线程、第二描述识别子线程和第二支付环境挖掘子线程，上述装置用于通过如下方式实现所述将所述一组潜在威胁型互动数据导入至威胁风控处理线程，得到所述威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志：将所述第一支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互动数据处理子线程，得到所述互动数据处理子线程导出的第一数据差异分析情况，以及将所述第二支付互动状态所适配的对应于本地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述互动数据处理子线程，得到所述互动数据处理子线程导出的第二数据差异分析情况，其中，所述互动数据处理子线程是通过多组第三调试范例通

过智能化分析调试得到的，所述多组第三调试范例中的每组第三调试范例包括：所述在线支付业务端在同一支付互动状态收集所得的两组潜在威胁型互动数据和互动数据差异化主题；将所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据和所述第二支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据导入至所述第二描述识别子线程，得到所述第二描述识别子线程导出的跨境支付互动描述，其中，所述第二描述识别子线程是通过多组第六调试范例通过智能化分析调试得到的，所述多组第六调试范例中的每组第六调试范例包括：所述在线支付业务端中的跨境支付业务端在存在时序先后关系的两个支付互动状态收集所得的潜在威胁型互动数据和交互特征主题；使用所述第二支付环境挖掘子线程对所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据中的支付环境表达信息进行挖掘得到第三支付环境表达信息，其中，所述第二支付环境挖掘子线程是通过多组第五调试范例通过智能化分析调试得到的，所述多组第五调试范例中的每组第五调试范例包括：潜在威胁型互动数据和第二表达信息挖掘主题；基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述跨境支付互动描述和所述第三支付环境表达信息确定所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志。

[0066] 可选地，上述装置还用于通过如下方式实现所述基于所述第一数据差异分析情况、所述第二数据差异分析情况、所述跨境支付互动描述和所述第三支付环境表达信息确定所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志：基于所述跨境支付互动描述对所述第二数据差异分析情况进行危险意图倾向分析，得到将所述第二数据差异分析情况匹配至所述第一支付互动状态的第二互动数据切换情况；使用所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据和所述第三支付环境表达信息对所述第二互动数据切换情况进行优化，得到第二互动数据优化结果；通过所述第二互动数据优化结果、所述第一数据差异分析情况和所述跨境支付互动描述得到所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志。

[0067] 可选地，所述威胁风控处理线程导出的所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的支付服务会话日志与事先设置的所述第一支付互动状态所适配的对应于异地入侵风险的潜在威胁型互动数据的在先支付服务会话日志之间的第二服务互动检测结果符合第二目标检测要求，所述第二目标检测要求用于表征所述第二服务互动检测结果的量化检测结果在第二设定约束区间之内。

[0068] 需要说明的是，上述各个模块是可以通过软件或硬件来实现的，对于后者，可以通过以下方式实现，但不限于此：上述模块均位于同一处理器中；或者，上述各个模块以任意组合的形式分别位于不同的处理器中。

[0069] 本申请的实施例还提供了一种存储介质，该存储介质中存储有计算机程序，其中，该计算机程序被设置为运行时执行上述任一项方法实施例中的步骤。

[0070] 可选地，在本申请实施例中，上述存储介质可以包括但不限于：U盘、只读存储器(Read-Only Memory，简称为ROM)、随机存取存储器(Random Access Memory，简称为RAM)、移动硬盘、磁碟或者光盘等各种可以存储计算机程序的介质。

[0071] 在上述基础上，请结合图4，基于上述同样的发明构思，本申请还提供了一种应对

在线支付数据威胁的大数据风控处理方法的实施环境400，所述系统包括相互通信的大数据风控服务系统100及在线支付业务端200，其中，大数据风控服务系统100统计由在线支付业务端200在存在时序先后关系的两个支付互动状态收集所得的一组潜在威胁型互动数据；将所述一组潜在威胁型互动数据导入至威胁风控处理线程，得到所述威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志；基于所述第一支付互动状态所适配的业务对象互动数据的支付服务会话日志确定所述第一支付互动状态所适配的业务对象互动数据中的危险意图表达信息。

[0072] 应当理解的是，本申请并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围执行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

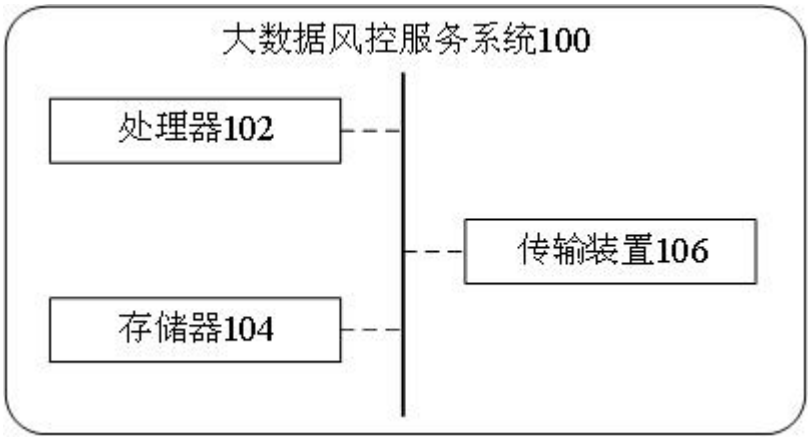

大数据风控服务系统100
处理器102
传输装置106
存储器104

图 1

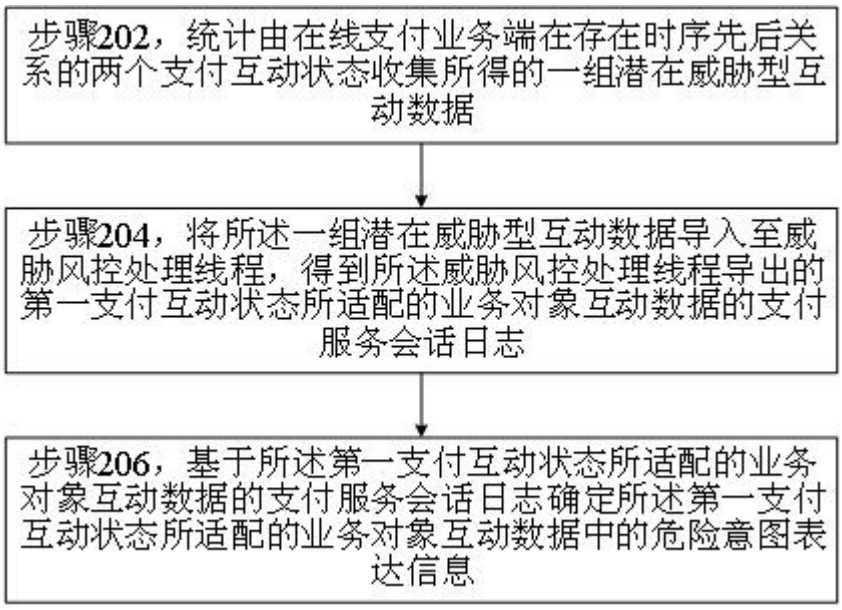

步骤202，统计由在线支付业务端在存在时序先后关系的两个支付互动状态收集所得的一组潜在威胁型互动数据
步骤204，将所述一组潜在威胁型互动数据导入至威胁风控处理线程，得到所述威胁风控处理线程导出的第一支付互动状态所适配的业务对象互动数据的支付服务会话日志
步骤206，基于所述第一支付互动状态所适配的业务对象互动数据的支付服务会话日志确定所述第一支付互动状态所适配的业务对象互动数据中的危险意图表达信息

图 2


数据统计模块310
日志获取模块320
意图确定模块330

图 3

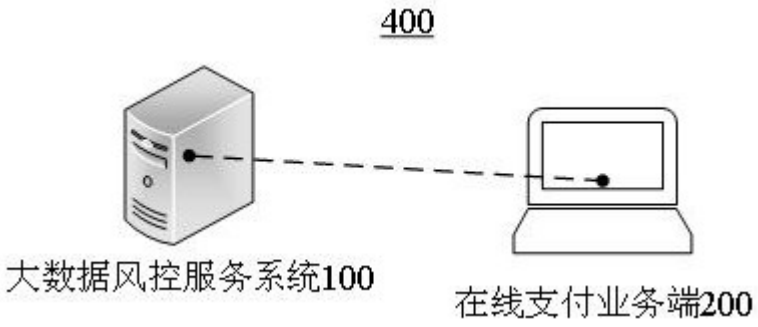


图 4