

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2015 年 7 月 9 日 (09.07.2015)



(10) 国际公布号
WO 2015/100969 A1

- (51) 国际专利分类号:
G06Q 20/38 (2012.01)
- (21) 国际申请号: PCT/CN2014/080494
- (22) 国际申请日: 2014 年 6 月 23 日 (23.06.2014)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410014450.6 2014 年 1 月 6 日 (06.01.2014) CN
- (71) 申请人: 同济大学 (TONGJI UNIVERSITY)
[CN/CN]; 中国上海市杨浦区四平路 1239 号, Shanghai 200092 (CN)。
- (72) 发明人: 蒋昌俊 (JIANG, Changjun); 中国上海市杨浦区四平路 1239 号, Shanghai 200092 (CN)。 陈闾中 (CHEN, Hongzhong); 中国上海市杨浦区四平路 1239 号, Shanghai 200092 (CN)。 闫春钢 (YAN, Chungang); 中国上海市杨浦区四平路 1239 号, Shanghai 200092 (CN)。 丁志军 (DING, Zhijun); 中国上海市杨浦区四平路 1239 号, Shanghai 200092 (CN)。 于汪洋 (YU, Wangyang); 中国上海市杨浦区四平路 1239 号, Shanghai 200092 (CN)。 钟珺竹

(ZHONG, Junzhu); 中国上海市杨浦区四平路 1239 号, Shanghai 200092 (CN)。

(74) 代理人: 上海光华专利事务所 (J.Z.M.C. PATENT AND TRADEMARK LAW OFFICE); 中国上海市杨浦区国定路 335 号 5022 室余明伟, Shanghai 200433 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO,

[见续页]

(54) Title: SOFTWARE BEHAVIOR MONITORING AND VERIFICATION SYSTEM

(54) 发明名称: 软件行为监控验证系统

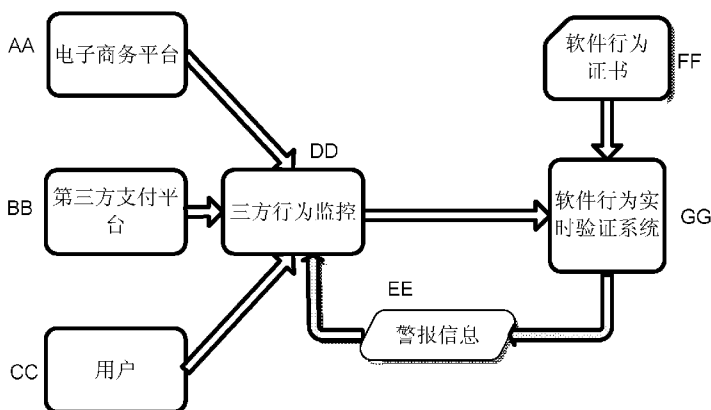


图 1 / Fig. 1

- AA E-commerce platform
BB Third party payment platform
CC User
DD Three-party behavior monitoring
EE Alarm information
FF Software behavior certification
GG Software behavior real-time verification system

(57) Abstract: A software behavior monitoring and verification system, mainly consisting of a software behavior certification, a three-party software behavior monitor and a software behavior real-time verification system; the software behavior certification is a three-party communication data packet in the proper transaction flow of a user, an E-commerce website and a third party payment platform; the three-party software behavior monitor is a data packet monitor installed on the E-commerce website, the third party payment platform and a user client; the software behavior real-time verification system extracts and integrates the key sequence and information after receiving transaction interaction information data packets respectively submitted by the three party monitors, and compares in real time a user behavior interaction sequence with a software behavior model according to a global unique order number. In the case of illegal acts such as wrong sequence and fake identification, an alarm is reported and the transaction is closed. Key parameters such as a three party interaction url ARE utilized to describe a legal normal three party transaction interaction flow, and propose a software behavior certification.

(57) 摘要:

[见续页]

RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, **本国际公布:**
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, — 包括国际检索报告(条约第 21 条(3))。
TG)。

一种软件行为监控验证系统，由软件行为证书、三方软件行为监控器、软件行为实时验证系统三个部分组成；软件行为证书是根据用户，电子商务网站，第三方支付平台在正确交易流程下的三方通信数据包；三方软件行为监控器，是安装于电子商务网站、第三方支付平台、用户客户端上的数据包监控器；软件行为实时验证系统在接收三方监控器分别提交的交易交互信息数据包后，提取并整合其中的关键序列与信息，并根据全球唯一订单号，将用户行为交互序列与软件行为模型进行实时对比，一旦发生乱序，假冒身份等非法行为则进行警报并关闭交易。利用三方交互 url 等关键参数，刻画合法正常三方交易交互流程，提出了软件行为证书。

软件行为监控验证系统

技术领域

[0001] 本发明涉及电子商务网络交易安全监控技术领域。

背景技术

[0002] 随着 Internet 的发展，电子商务（E—Commerce）已经逐渐成为人们进行商务活动的新模式，也越来越成为国际贸易中重要的经营模式。它以计算机技术、通信技术与网络技术为基础，利用电子数据交换、电子邮件、电子支付等方式实现了整个商务活动的电子化、数字化和网络化。电子交易平台的出现，使整个销售、交易和确认的程序已被网上交易所取代。由从前第一代的银行交易系统 Electronic Brokerage System (EBS)，发展至银行自行研发的单一交易平台，到今天由第三方提供的多主体交易平台，以及由市场推动的应用程序接口（API），都显示出电子交易迅猛发展的势头，但它的发展还面临着许多机遇和调整。

[0003] 近年来，电子商务模式主要由 B2C、B2B 和 C2C 构成，但这些模式也都普遍采用第三方支付的模式，用户、电子商务网站、第三方支付平台是目前电子交易过程中的三个主要主体。上述三方通过签名，认证，加密等技术相互信任，互相调用接口进行通信，从而协作完成整个网上交易过程。然而由于当今软件开发技术的不够完善，在用户客户端软件，电子商务网站，甚至是第三方支付平台都可能存在着一定的通信接口漏洞和逻辑错误等。

[0004] 本发明面向的情况是合法注册的恶意用户往往可以利用这些漏洞从事非法行为，为自己谋取非法利益。并且由于这种漏洞的隐藏性，多样性和难以防范性、用户行为的多变性、以及网络平台的分布式与松耦合性，这三者因素综合，导致传统的安全方法无法保证现今电子网络交易安全。

发明内容

[0005] 本发明的目的在于克服现有技术的不足，公开了一种软件行为监控验证系统，提出用户、电子商务平台、第三方支付平台三方相互协作的安全保证模式，交易流程全程监控，实时警报。

[0006] 本发明给出的技术方案为：

一种软件行为监控验证系统，其特征在于，由软件行为证书、三方软件行为监控器、软件行为实时验证系统三个部分组成。

[0007] 所述软件行为证书是根据用户，电子商务网站，第三方支付平台在正确交易流程下的三方通信数据包，从而由专业人员人为刻画三方正常合法交互行为，形成软件行为证书。所述软件行为证书是电子商务网站、第三方支付平台、用户客户端三者，包括两两之间各自形成的交互模式，形成对应的软件行为模型。

[0008] 所述三方软件行为监控器，是安装于电子商务网站、第三方支付平台、用户客户

端上的数据包监控器，用来实时监控在一次完整交易中参与交易的三方之间相互传递的数据包，并且进行数据包中的必要参数信息（URL 地址，参数等）的提取和整合，便于将关键信息发送给软件行为实时验证系统。所述监控器以 jpcap 为技术基础，主要捕获 http 协议数据包，并提取数据包中的 URL 地址及参数信息，以及交易三方中电商编号和第三方支付平台编号。随后与软件行为实时验证系统建立 socket 连接，将关键信息以 tcp 数据包的形式发送给软件行为实时验证系统。

[0009] 所述软件行为实时验证系统在接收三方监控器分别提交的交易交互信息数据包后，提取并整合其中的关键序列与信息，并根据全球唯一订单号，将用户行为交互序列与软件行为模型进行实时对比，一旦发生乱序，假冒身份等非法行为则进行警报并关闭交易。

[0010] 所述软件行为证书中刻画的软件行为有着一定的行为逻辑，体现在：

1) 软件行为证书中每一个 transition_node 为一个行为结点，三方中任一方所捕捉到的数据包分为两大类：接收的消息，发送的消息，分别对应 transition_node 中的 input, output, 两者有着必要的逻辑顺序，接收消息必须先于发送消息；将捕获的到行为序列与相对应的 transition_node 相对比，一旦违反上述逻辑顺序则进行警报；

2) 与此同时，软件行为实时验证系统还将接收或者发送消息的当前主体与证书行为结点 (transition_node) 中属性 attri 所记录的主体名称进行对比，如不相符则意味着非法用户身份冒充攻击，立即警报；

3) place_node 则刻画了行为结点与行为结点之间的逻辑顺序，行为结点 (transition_node) 也必须按照一定的交易顺序排列，一旦发生跳跃，乱序则意味着合法正常交易流程被打破，出现了违规操作，立即警报。

[0011] 本发明的创新点及其有益效果：利用三方交互 url 等关键参数，刻画合法正常三方交易交互流程，提出了软件行为证书。软件行为证书是根据用户，电子商务网站，第三方支付平台在正确交易流程下的三方通信数据包，从而由专业人员人为刻画三方正常合法交互行为，形成软件行为证书。本发明提出用户，电子商务平台，第三方支付平台三方相互协作的安全保证模式，交易流程全程监控，实时警报。

附图说明

[0012] 图 1 是软件行为监控验证整体架构图。

[0013] 图 2 三方软件行为监控器流程图。

[0014] 图 3 软件行为实时验证系统流程图。

[0015] 图 4 软件行为证书格式 (place_node)。

[0016] 图 5 软件行为证书格式 (transition_node)。

具体实施方式

[0017] 整个软件行为监控验证系统的架构如图 1 所示。

[0018] 整个软件行为监控验证系统将真正合法用户的行为固化下来形成软件行为证书。

然后主要根据全球唯一订单号，将交易过程中的三方交互行为序列与软件行为证书进行实时对比，单步验证，一旦任何一方发生消息乱序或者假冒身份等非法行为则进行警报或采取一定的措施。

[0019] 三方软件行为监控器：在电子商务网站、第三方支付平台以及用户客户端安装数据包监控器，用来实时监控在一次完整交易中参与交易的三方之间相互传递的数据包，并且进行数据包中的必要参数信息的提取和整合，便于将关键信息发送给软件行为实时验证系统。所述监控器以 jpcap 为技术基础，主要捕获 http 协议数据包，并提取数据包中的 URL 地址及参数信息，以及交易三方中电商编号和第三方支付平台编号。随后与软件行为实时验证系统建立 socket 连接，将关键信息以 tcp 数据包的形式发送给软件行为实时验证系统。三方软件行为监控流程图如图 2 所示：

软件行为实时验证系统：在与三方软件行为监控器建立 socket 连接之后，接收三方软件行为监控器发送过来的 tcp 数据包，提取并整合其中的关键序列与信息。然后根据全球唯一订单号，将用户行为交互序列与软件行为模型进行实时验证，一旦发生乱序，假冒身份等非法行为则进行警报并关闭交易。软件行为实时验证系统流程图如图 3 所示：

电子商务网站与第三方支付平台，以及用户客户端三者，包括两两之间各自的交互模式所形成的软件行为证书。软件行为证书由专业人员手动构建，并以 XML 文件格式存储在服务器中。

[0020] 软件行为证书格式如图 4, 图 5 所示：

input 为三方（用户，电子商务网站，第三方支付平台）中任一方接收到的关键参数（url 等）。output 为当前方发送的关键参数。这些交互信息代表了软件行为序列。

[0021] 软件行为证书中刻画的软件行为有着一定的行为逻辑。这种逻辑体现了三方交互顺序，前提条件等。软件行为证书中每一个 transition_node 为一个行为结点。三方中任一方所捕捉到的数据包分为两大类：接收的消息，发送的消息。分别对应 transition_node 中的 input, output。而两者也有着必要的逻辑顺序，接收消息必须先于发送消息。我们将捕获的到行为序列与相对应的 transition_node 相对比，一旦违反上述逻辑顺序则进行警报。与此同时，软件行为实时验证系统还将接收或者发送消息的当前主体与证书行为结点（transition_node）中属性 attri 所记录的主体名称进行对比，如不相符则意味着非法用户身份冒充攻击，立即警报。place_node 则刻画了行为结点与行为结点之间的逻辑顺序。也就是说行为结点（transition_node）也必须按照一定的交易顺序排列，一旦发生跳跃，乱序则意味着合法正常交易流程被打破，出现了违规操作，立即警报。

权利要求书

1. 一种软件行为监控验证系统，其特征在于，由软件行为证书、三方软件行为监控器、软件行为实时验证系统三个部分组成；

所述软件行为证书是根据用户，电子商务网站，第三方支付平台在正确交易流程下的三方通信数据包，从而由专业人员人为刻画三方正常合法交互行为，形成软件行为证书。

所述软件行为证书是电子商务网站、第三方支付平台、用户客户端三者，包括两两之间各自形成的交互模式，形成对应的软件行为模型；

所述三方软件行为监控器，是安装于电子商务网站、第三方支付平台、用户客户端上的数据包监控器，用来实时监控在一次完整交易中参与交易的三方之间相互传递的数据包，并且进行数据包中的必要参数信息（URL 地址，参数等）的提取和整合，便于将关键信息发送给软件行为实时验证系统；所述监控器以 jpcap 为技术基础，主要捕获 http 协议数据包，并提取数据包中的 URL 地址及参数信息，以及交易三方中电商编号和第三方支付平台编号；随后与软件行为实时验证系统建立 socket 连接，将关键信息以 tcp 数据包的形式发送给软件行为实时验证系统。

所述软件行为实时验证系统在接收三方监控器分别提交的交易交互信息数据包后，提取并整合其中的关键序列与信息，并根据全球唯一订单号，将用户行为交互序列与软件行为模型进行实时对比，一旦发生乱序，假冒身份等非法行为则进行警报并关闭交易。

2. 根据权利要求 1 所述的软件行为监控验证系统，其特征在于，所述软件行为证书中刻画的软件行为有着一定的行为逻辑，体现在：

1) 软件行为证书中每一个 transition_node 为一个行为结点，三方中任一方所捕捉到的数据包分为两大类：接收的消息，发送的消息，分别对应 transition_node 中的 input, output，两者有着必要的逻辑顺序，接收消息必须先于发送消息；将捕获的到行为序列与相对应的 transition_node 相对比，一旦违反上述逻辑顺序则进行警报；

2) 与此同时，软件行为实时验证系统还将接收或者发送消息的当前主体与证书行为结点（transition_node）中属性 attri 所记录的主体名称进行对比，如不相符则意味着非法用户身份冒充攻击，立即警报；

3) place_node 则刻画了行为结点与行为结点之间的逻辑顺序，行为结点（transition_node）也必须按照一定的交易顺序排列，一旦发生跳跃，乱序则意味着合法正常交易流程被打破，出现了违规操作，立即警报。

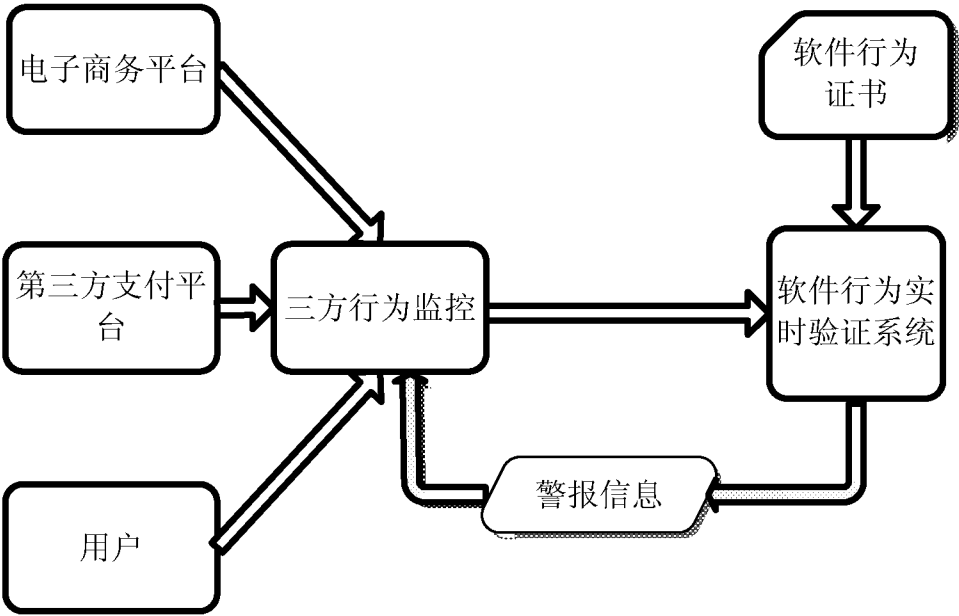


图 1

2/4

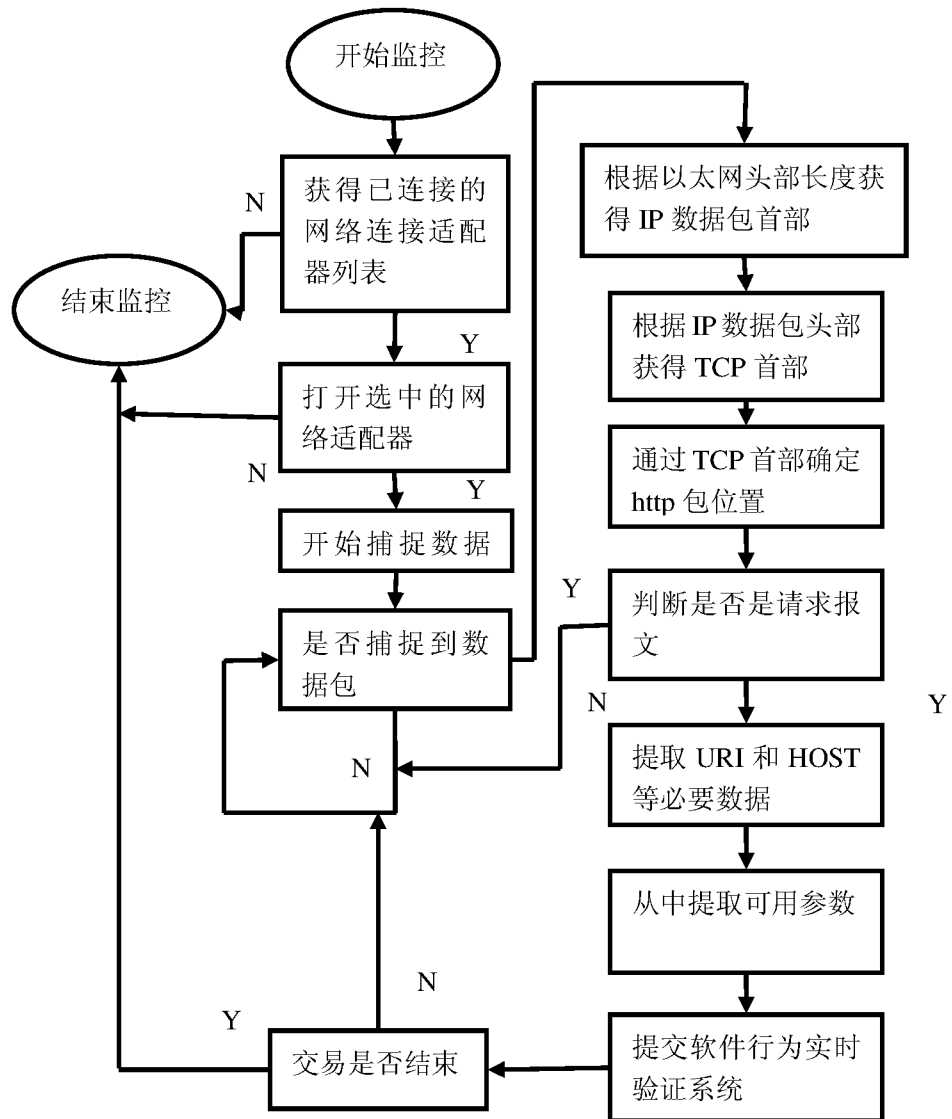


图 2

3/4

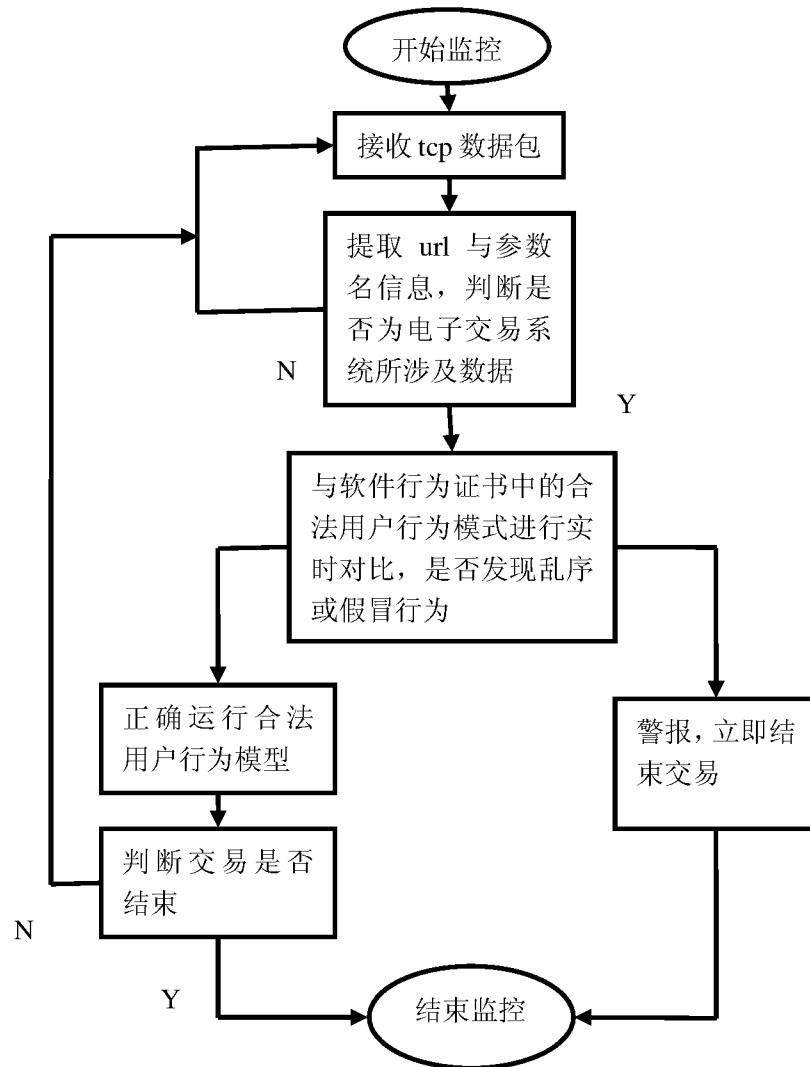


图 3

4/4

```

<place_node>
  <id>1</id>
  <num>1</num>
  <transition_list>
    <No>4</No>
  </transition_list>
</place_node>

```

图 4

```

<transition_node>
  <id>5</id>
  <name>HandleIPN</name>
  <attri>merchant</attri>
  <outplace>
    <No>11</No>
    <No>12</No>
  </outplace>
  <inplace>
    <No>6</No>
    <No>8</No>
  </inplace>
  <input>
    <string>orderId</string>
    <string>gross</string>
    <string>status</string>
    <string>hidden</string>
    <string>merchantID</string>
    <string>caasID</string>
    <string>uniqueID</string>
  </input>
  <output>
    <string>http://10.60.149.180/Caas/servlet/Get_down?</string>
    <string>junzhu</string>
    <string>orderId</string>
    <string>merchantID</string>
    <string>caasID</string>
    <string>uniqueID</string>
  </output>
</transition_node>

```

图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/080494

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38 (2012.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, CNTXT, CNPAT, EPODOC, WPI, CNKI: business, security, model, alarm, third w party, pay+, authen+, verifi+, monitor, behaviour, platform, clos+, illegal, transaction, parameter

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103714456 A (TONGJI UNIVERSITY), 09 April 2014 (09.04.2014), claims 1-2	1-2
A	CN 102194177 A (NANJING COFREE SOFTWARE TECHNOLOGY CO., LTD.), 21 September 2011 (21.09.2011), claims 1-2, description, paragraphs [0004]-[0019] and [0021]-[0034], and figure 1	1-2
A	CN 101706937 A (CHINA CONSTRUCTION BANK CORPORATION), 12 May 2010 (12.05.2010), the whole document	1-2
A	CN 103279883 A (CTRIIP COMPUTER TECHNOLOGY (SHANGHAI) CO., LTD.), 04 September 2013 (04.09.2013), the whole document	1-2
A	US 2004034583 A1 (LANIER, C.L. et al.), 19 February 2004 (19.02.2004), the whole document	1-2

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 16 September 2014 (16.09.2014)	Date of mailing of the international search report 13 October 2014 (13.10.2014)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer LIANG, Jing Telephone No.: (86-10) 62414423

International application No.
PCT/CN2014/080494

Form PCT/ISA/210 (patent family annex) (July 2009)

A. 主题的分类		
G06Q 20/38(2012.01)i		
按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类		
B. 检索领域		
检索的最低限度文献(标明分类系统和分类号)		
G06Q		
包含在检索领域中的除最低限度文献以外的检索文献		
在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))		
CNABS, CNTXT, CNPAT, EPODOC, WPI, CNKI: 第三方, 支付, 验证, 商务, 安全, 监控, 模型, 报警, 行为, 平台, 关闭, 非法, 交易, 参数, third w party, pay+, authen+, verifi+, monitor, behavior, platform, clos+, illegal, transaction, parameter		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 103714456 A (同济大学) 2014年 4月 09日 (2014 - 04 - 09) 权利要求1-2	1-2
A	CN 102194177 A (南京柯富锐软件科技有限公司) 2011年 9月 21日 (2011 - 09 - 21) 权利要求1-2, 说明书第[0004]-[0019]段, 第[0021]-[0034]段, 图1	1-2
A	CN 101706937 A (中国建设银行股份有限公司) 2010年 5月 12日 (2010 - 05 - 12) 全文	1-2
A	CN 103279883 A (携程计算机技术上海有限公司) 2013年 9月 04日 (2013 - 09 - 04) 全文	1-2
A	US 2004034583 A1 (LANIER, CHERYL LYNN ET AL.) 2004年 2月 19日 (2004 - 02 - 19) 全文	1-2
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期		国际检索报告邮寄日期
2014年 9月 16日		2014年 10月 13日
ISA/CN的名称和邮寄地址		授权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国		梁静
传真号 (86-10)62019451		电话号码 (86-10)62414423

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2014/080494

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	103714456	A	2014年 4月 09日	无	
CN	102194177	A	2011年 9月 21日	无	
CN	101706937	A	2010年 5月 12日	无	
CN	103279883	A	2013年 9月 04日	无	
US	2004034583	A1	2004年 2月 19日	CA 2435993 A1	2004年 2月 15日