



(12) 发明专利

(10) 授权公告号 CN 109151015 B

(45) 授权公告日 2021.10.08

(21) 申请号 201810917292.3

G06Q 40/04 (2012.01)

(22) 申请日 2018.08.13

(56) 对比文件

(65) 同一申请的已公布的文献号

CN 108090763 A, 2018.05.29

申请公布号 CN 109151015 A

CN 108090763 A, 2018.05.29

(43) 申请公布日 2019.01.04

CN 106487749 A, 2017.03.08

(73) 专利权人 南京敞视信息科技有限公司

CN 106549757 A, 2017.03.29

地址 210000 江苏省南京市雨花经济开发

CN 103927653 A, 2014.07.16

区凤华路18号1幢B317-3室

US 2012259789 A1, 2012.10.11

审查员 彭风华

(72) 发明人 祝磊 丁往兰 夏振荣 陈志

(74) 专利代理机构 南京天翼专利代理有限责任

公司 32112

代理人 于忠洲

(51) Int. Cl.

H04L 29/08 (2006.01)

H04L 29/06 (2006.01)

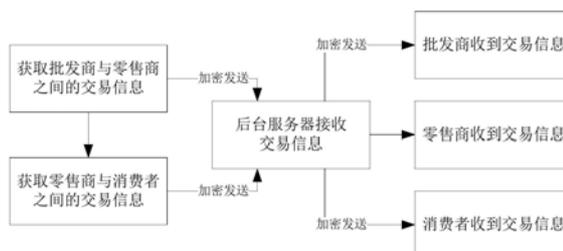
权利要求书2页 说明书5页 附图1页

(54) 发明名称

一种交易信息安全推送方法

(57) 摘要

本发明提供了一种交易信息安全推送方法,步骤包括:利用物联网电子秤获取批发商与零售商之间的交易信息,并将交易信息加密发送至后台服务器,再由后台服务器根据零售商信息和批发商信息将交易信息加密发送至批发商和零售商的手机客户端;利用物联网电子秤获取零售商与消费者之间的交易信息,并将交易信息加密发送至后台服务器,再由后台服务器根据零售商信息和消费者信息将交易信息加密发送至零售商和消费者的手机客户端。该交易信息安全推送方法利用加密发送交易信息能够确保信息中包含的零售商信息、批发商信息以及消费者信息得到安全可靠的保护。



1. 一种交易信息安全推送方法,其特征在于,包括如下步骤:

步骤1,利用物联网电子秤获取批发商与零售商之间的交易信息,包括零售商信息、批发商信息、交易时间、交易食品信息以及交易数量,并将交易信息加密发送至后台服务器,再由后台服务器根据零售商信息和批发商信息将交易信息加密发送至批发商和零售商的手机客户端;

步骤2,利用物联网电子秤获取零售商与消费者之间的交易信息,包括零售商信息、消费者信息、购买食品信息、购买时间以及购买数量,并将交易信息加密发送至后台服务器,再由后台服务器根据零售商信息和消费者信息将交易信息加密发送至零售商和消费者的手机客户端;

加密发送包括如下步骤:

首先由发送端和接收端约定一个密钥 $g$ ,在发送端发送通信请求时,再由发送端生成密钥 $a$ ,再根据密钥 $g$ 生成 $g(a)$ ,并将 $g(a)$ 发送至接收端,接收端在接收到 $g(a)$ 后,首先由接收端生成密钥 $b$ ,再根据密钥 $g$ 生成 $g(b)$ ,根据密钥 $g(a)$ 生成 $g(ab)$ ;  $g(ab)=g(b)*g(a)$ ;

再由接收端将 $g(b)$ 发送至发送端,发送端在接收到 $g(b)$ 后,由发送端根据 $g(a)$ 生成 $g(ab)$ ,再由发送端利用自身生成的 $g(ab)$ 对待通信参数进行加密生成VC校验值,并将VC校验值以及待通信参数一起发送至接收端;

在接收端接收到VC校验值以及待通信参数后,利用自身生成的 $g(ab)$ 对待通信参数进行加密生成VC校验值,并由接收端比较自身生成的VC校验值与接收发送端发送的VC校验值是否一致,若一致,则表明通信数据未被篡改,若不一致,则表明通信数据已被篡改,并将是否已被篡改的结果发送至发送端;

步骤1中,获取批发商与零售商之间的交易信息的具体步骤为:

步骤1.1,利用批发商电子秤上对应的批发商ID获取批发商信息,利用批发商电子秤上设置的摄像头采集零售商的面部照片,并生成对应于面部图片识别的零售商信息;

步骤1.2,根据零售商的支付方式确定相应的信息推送线程,并利用零售商已关注的微信公共号推送本次交易的交易时间、交易食品信息以及交易数量;

步骤1.3,将本次交易的批发商信息、零售商信息、交易时间、交易食品信息以及交易数量打包发送至后台服务器存储;

支付方式包括现金支付、微信支付以及支付宝支付;信息推送线程包括现金支付批发信息推送线程、微信支付批发信息推送线程以及支付宝支付批发信息推送线程;由面部图片识别获得的零售商信息为零售商的编号代码,由批发商ID获取批发商信息为批发商的编号代码;

现金支付批发信息推送线程为:将零售商的零售商信息在数据库中进行查询,若找到相同的零售商信息且该零售商信息之前使用过微信支付,则将交易信息与该零售商信息对应的微信OpenID相关联,并利用零售商已关注的微信公共号向该微信OpenID推送本次交易信息;

微信支付批发信息推送线程为:在零售商微信支付后,获取零售商的微信OpenID,再将零售商的零售商信息与微信OpenID相关联,并将零售商信息和微信OpenID对应存储在后台服务器中,再利用零售商已关注的微信公共号向该微信OpenID推送本次交易信息;

支付宝支付批发信息推送线程为:在零售商支付宝支付后,获取零售商的支付宝

OpenID,并生成电子账单二维码供零售商微信扫码,在零售商使用微信扫码后,则获取零售商的微信OpenID,再将该零售商的支付宝OpenID与微信OpenID相关联,并将支付宝OpenID和微信OpenID对应存入后台服务器中,再利用零售商已关注的微信公共号向该微信OpenID推送本次交易信息;

步骤2中,获取零售商与消费者之间的交易信息的具体步骤为:

步骤2.1,利用零售商电子秤上对应的零售商ID获取零售商信息,利用零售商电子秤上设置的摄像头采集消费者的面部照片,并生成对应于面部图片识别的消费者信息;

步骤2.2,根据消费者的支付方式确定相应的信息推送线程,并利用消费者已关注的微信公共号推送本次交易的交易时间、交易食品信息以及交易数量;

步骤2.3,将本次销售的零售商信息、消费者信息、交易时间、交易食品信息以及交易数量打包发送至后台服务器存储。

2.根据权利要求1所述的交易信息安全推送方法,其特征在于,g(a)、g(b)以及g(ab)分别为密钥g的a、b以及ab幂次方。

3.根据权利要求1所述的交易信息安全推送方法,其特征在于,支付方式包括现金支付、微信支付以及支付宝支付;信息推送线程包括现金支付零售信息推送线程、微信支付零售信息推送线程以及支付宝支付零售信息推送线程;由面部图片识别获得的消费者信息为消费者的编号代码,由零售商ID获取零售商信息为零售商的编号代码。

4.根据权利要求3所述的交易信息安全推送方法,其特征在于,

现金支付零售信息推送线程为:将消费者的消费者信息在数据库中进行查询,若找到相同的消费者信息且该消费者信息之前使用过微信支付,则将交易信息与该消费者信息对应的微信OpenID相关联,并利用消费者已关注的微信公共号向该微信OpenID推送本次交易信息;

微信支付零售信息推送线程为:在消费者微信支付后,获取消费者的微信OpenID,再将消费者的消费者信息与微信OpenID相关联,并将消费者信息和微信OpenID对应存储在后台服务器中,再利用消费者已关注的微信公共号向该微信OpenID推送本次交易信息;

支付宝支付零售信息推送线程为:在消费者支付宝支付后,获取消费者的支付宝OpenID,并生成电子账单二维码供消费者微信扫码,在消费者使用微信扫码后,则获取消费者的微信OpenID,再将该消费者的支付宝OpenID与微信OpenID相关联,并将支付宝OpenID和微信OpenID对应存入后台服务器中,再利用消费者已关注的微信公共号向该微信OpenID推送本次交易信息。

## 一种交易信息安全推送方法

### 技术领域

[0001] 本发明涉及一种信息推送方法,尤其是一种交易信息安全推送方法。

### 背景技术

[0002] 由于现有的物联网电子秤在与后台服务器以及后台服务器与手机客户端进行信息推送时只是采用了现有的互联网协议,并没有设计特别的加密,当通信的信息中包含了零售商信息、批发商信息以及消费者信息时,便会容易造成信息的泄漏。因此有必要设计出一种交易信息安全推送方法,能够实现交易信息的安全推送。

### 发明内容

[0003] 本发明的目的在于:提供一种交易信息安全推送方法,能够实现交易信息的安全推送。

[0004] 为了实现上述发明目的,本发明提供了一种交易信息安全推送方法,包括如下步骤:

[0005] 步骤1,利用物联网电子秤获取批发商与零售商之间的交易信息,包括零售商信息、批发商信息、交易时间、交易食品信息以及交易数量,并将交易信息加密发送至后台服务器,再由后台服务器根据零售商信息和批发商信息将交易信息加密发送至批发商和零售商的手机客户端;

[0006] 步骤2,利用物联网电子秤获取零售商与消费者之间的交易信息,包括零售商信息、消费者信息、购买食品信息、购买时间以及购买数量,并将交易信息加密发送至后台服务器,再由后台服务器根据零售商信息和消费者信息将交易信息加密发送至零售商和消费者的手机客户端。

[0007] 进一步地,加密发送包括如下步骤:

[0008] 首先由发送端和接收端约定一个密钥 $g$ ,在发送端发送通信请求时,再由发送端生成密钥 $a$ ,再根据密钥 $g$ 生成 $g(a)$ ,并将 $g(a)$ 发送至接收端,接收端在接收到 $g(a)$ 后,首先由接收端生成密钥 $b$ ,再根据密钥 $g$ 生成 $g(b)$ ,根据密钥 $g(a)$ 生成 $g(ab)$ ;

[0009] 再由接收端将 $g(b)$ 发送至发送端,发送端在接收到 $g(b)$ 后,由发送端根据 $g(a)$ 生成 $g(ab)$ ,再由发送端利用自身生成的 $g(ab)$ 对待通信参数进行加密生成VC校验值,并将VC校验值以及待通信参数一起发送至接收端;

[0010] 在接收端接收到VC校验值以及待通信参数后,利用自身生成的 $g(ab)$ 对待通信参数进行加密生成VC校验值,并由接收端比较自身生成的VC校验值与接收发送端发送的VC校验值是否一致,若一致,则表明通信数据未被篡改,若不一致,则表明通信数据已被篡改,并将是否已被篡改的结果发送至发送端。

[0011] 进一步地, $g(a)$ 、 $g(b)$ 以及 $g(ab)$ 分别为密钥 $g$ 的 $a$ 、 $b$ 以及 $ab$ 幂次方。

[0012] 进一步地, $g(ab) = g(b) * g(a)$ 。

[0013] 进一步地,步骤1中,获取批发商与零售商之间的交易信息的具体步骤为:

[0014] 步骤1.1,利用批发商电子秤上对应的批发商ID获取批发商信息,利用批发商电子秤上设置的摄像头采集零售商的面部照片,并生成对应于面部图片识别的零售商信息;

[0015] 步骤1.2,根据零售商的支付方式确定相应的信息推送线程,并利用零售商已关注的微信公共号推送本次交易的交易时间、交易食品信息以及交易数量;

[0016] 步骤1.3,将本次交易的批发商信息、零售商信息、交易时间、交易食品信息以及交易数量打包发送至后台服务器存储。

[0017] 进一步地,支付方式包括现金支付、微信支付以及支付宝支付;信息推送线程包括现金支付批发信息推送线程、微信支付批发信息推送线程以及支付宝支付批发信息推送线程;由面部图片识别获得的零售商信息为零售商的编号代码,由批发商ID获取批发商信息为批发商的编号代码。

[0018] 进一步地,现金支付批发信息推送线程为:将零售商的零售商信息在数据库中进行查询,若找到相同的零售商信息且该零售商信息之前使用过微信支付,则将交易信息与该零售商信息对应的微信OpenID相关联,并利用零售商已关注的微信公共号向该微信OpenID推送本次交易信息;

[0019] 微信支付批发信息推送线程为:在零售商微信支付后,获取零售商的微信OpenID,再将零售商的零售商信息与微信OpenID相关联,并将零售商信息和微信OpenID对应存储在后台服务器中,再利用零售商已关注的微信公共号向该微信OpenID推送本次交易信息;

[0020] 支付宝支付批发信息推送线程为:在零售商支付宝支付后,获取零售商的支付宝OpenID,并生成电子账单二维码供零售商微信扫码,在零售商使用微信扫码后,则获取零售商的微信OpenID,再将该零售商的支付宝OpenID与微信OpenID相关联,并将支付宝OpenID和微信OpenID对应存入后台服务器中,再利用零售商已关注的微信公共号向该微信OpenID推送本次交易信息。

[0021] 进一步地,步骤2中,获取零售商与消费者之间的交易信息的具体步骤为:

[0022] 步骤2.1,利用零售商电子秤上对应的零售商ID获取零售商信息,利用零售商电子秤上设置的摄像头采集消费者的面部照片,并生成对应于面部图片识别的消费者信息;

[0023] 步骤2.2,根据消费者的支付方式确定相应的信息推送线程,并利用消费者已关注的微信公共号推送本次交易的交易时间、交易食品信息以及交易数量;

[0024] 步骤2.3,将本次销售的零售商信息、消费者信息、交易时间、交易食品信息以及交易数量打包发送至后台服务器存储。

[0025] 进一步地,支付方式包括现金支付、微信支付以及支付宝支付;信息推送线程包括现金支付零售信息推送线程、微信支付零售信息推送线程以及支付宝支付零售信息推送线程;由面部图片识别获得的消费者信息为消费者的编号代码,由零售商ID获取零售商信息为零售商的编号代码。

[0026] 进一步地,现金支付零售信息推送线程为:将消费者的消费者信息在数据库中进行查询,若找到相同的消费者信息且该消费者信息之前使用过微信支付,则将交易信息与该消费者信息对应的微信OpenID相关联,并利用消费者已关注的微信公共号向该微信OpenID推送本次交易信息;

[0027] 微信支付零售信息推送线程为:在消费者微信支付后,获取消费者的微信OpenID,再将消费者的消费者信息与微信OpenID相关联,并将消费者信息和微信OpenID对应存储在

后台服务器中,再利用消费者已关注的微信公共号向该微信OpenID推送本次交易信息;

[0028] 支付宝支付零售信息推送线程为:在消费者支付宝支付后,获取消费者的支付宝OpenID,并生成电子账单二维码供消费者微信扫码,在消费者使用微信扫码后,则获取消费者的微信OpenID,再将该消费者的支付宝OpenID与微信OpenID相关联,并将支付宝OpenID和微信OpenID对应存入后台服务器中,再利用消费者已关注的微信公共号向该微信OpenID推送本次交易信息。

[0029] 本发明的有益效果在于:利用加密发送交易信息能够确保信息中包含的零售商信息、批发商信息以及消费者信息得到安全可靠的保护;利用后台服务器向发生交易的零售商、批发商或消费者推送交易信息,能够实现交易双方对当前交易的记录和查看。

## 附图说明

[0030] 图1为本发明的方法流程图。

## 具体实施方式

[0031] 如图1所示,本发明公开的交易信息安全推送方法,包括如下步骤:

[0032] 步骤1,利用物联网电子秤获取批发商与零售商之间的交易信息,包括零售商信息、批发商信息、交易时间、交易食品信息以及交易数量,并将交易信息加密发送至后台服务器,再由后台服务器根据零售商信息和批发商信息将交易信息加密发送至批发商和零售商的手机客户端;

[0033] 步骤2,利用物联网电子秤获取零售商与消费者之间的交易信息,包括零售商信息、消费者信息、购买食品信息、购买时间以及购买数量,并将交易信息加密发送至后台服务器,再由后台服务器根据零售商信息和消费者信息将交易信息加密发送至零售商和消费者的手机客户端。

[0034] 进一步地,加密发送包括如下步骤:

[0035] 首先由发送端和接收端约定一个密钥 $g$ ,在发送端发送通信请求时,再由发送端生成密钥 $a$ ,再根据密钥 $g$ 生成 $g(a)$ ,并将 $g(a)$ 发送至接收端,接收端在接收到 $g(a)$ 后,首先由接收端生成密钥 $b$ ,再根据密钥 $g$ 生成 $g(b)$ ,根据密钥 $g(a)$ 生成 $g(ab)$ ;

[0036] 再由接收端将 $g(b)$ 发送至发送端,发送端在接收到 $g(b)$ 后,由发送端根据 $g(a)$ 生成 $g(ab)$ ,再由发送端利用自身生成的 $g(ab)$ 对待通信参数进行加密生成VC校验值,并将VC校验值以及待通信参数一起发送至接收端;

[0037] 在接收端接收到VC校验值以及待通信参数后,利用自身生成的 $g(ab)$ 对待通信参数进行加密生成VC校验值,并由接收端比较自身生成的VC校验值与接收发送端发送的VC校验值是否一致,若一致,则表明通信数据未被篡改,若不一致,则表明通信数据已被篡改,并将是否已被篡改的结果发送至发送端。

[0038] 进一步地, $g(a)$ 、 $g(b)$ 以及 $g(ab)$ 分别为密钥 $g$ 的 $a$ 、 $b$ 以及 $ab$ 幂次方。

[0039] 进一步地, $g(ab) = g(b) * g(a)$ 。

[0040] 进一步地,步骤1中,获取批发商与零售商之间的交易信息的具体步骤为:

[0041] 步骤1.1,利用批发商电子秤上对应的批发商ID获取批发商信息,利用批发商电子秤上设置的摄像头采集零售商的面部照片,并生成对应于面部图片识别的零售商信息;

[0042] 步骤1.2,根据零售商的支付方式确定相应的信息推送线程,并利用零售商已关注的微信公共号推送本次交易的交易时间、交易食品信息以及交易数量;

[0043] 步骤1.3,将本次交易的批发商信息、零售商信息、交易时间、交易食品信息以及交易数量打包发送至后台服务器存储。

[0044] 进一步地,支付方式包括现金支付、微信支付以及支付宝支付;信息推送线程包括现金支付批发信息推送线程、微信支付批发信息推送线程以及支付宝支付批发信息推送线程;由面部图片识别获得的零售商信息为零售商的编号代码,由批发商ID获取批发商信息为批发商的编号代码。

[0045] 进一步地,现金支付批发信息推送线程为:将零售商的零售商信息在数据库中进行查询,若找到相同的零售商信息且该零售商信息之前使用过微信支付,则将交易信息与该零售商信息对应的微信OpenID相关联,并利用零售商已关注的微信公共号向该微信OpenID推送本次交易信息;

[0046] 微信支付批发信息推送线程为:在零售商微信支付后,获取零售商的微信OpenID,再将零售商的零售商信息与微信OpenID相关联,并将零售商信息和微信OpenID对应存储在后台服务器中,再利用零售商已关注的微信公共号向该微信OpenID推送本次交易信息;

[0047] 支付宝支付批发信息推送线程为:在零售商支付宝支付后,获取零售商的支付宝OpenID,并生成电子账单二维码供零售商微信扫码,在零售商使用微信扫码后,则获取零售商的微信OpenID,再将该零售商的支付宝OpenID与微信OpenID相关联,并将支付宝OpenID和微信OpenID对应存入后台服务器中,再利用零售商已关注的微信公共号向该微信OpenID推送本次交易信息。

[0048] 进一步地,步骤2中,获取零售商与消费者之间的交易信息的具体步骤为:

[0049] 步骤2.1,利用零售商电子秤上对应的零售商ID获取零售商信息,利用零售商电子秤上设置的摄像头采集消费者的面部照片,并生成对应于面部图片识别的消费者信息;

[0050] 步骤2.2,根据消费者的支付方式确定相应的信息推送线程,并利用消费者已关注的微信公共号推送本次交易的交易时间、交易食品信息以及交易数量;

[0051] 步骤2.3,将本次销售的零售商信息、消费者信息、交易时间、交易食品信息以及交易数量打包发送至后台服务器存储。

[0052] 进一步地,支付方式包括现金支付、微信支付以及支付宝支付;信息推送线程包括现金支付零售信息推送线程、微信支付零售信息推送线程以及支付宝支付零售信息推送线程;由面部图片识别获得的消费者信息为消费者的编号代码,由零售商ID获取零售商信息为零售商的编号代码。

[0053] 进一步地,现金支付零售信息推送线程为:将消费者的消费者信息在数据库中进行查询,若找到相同的消费者信息且该消费者信息之前使用过微信支付,则将交易信息与该消费者信息对应的微信OpenID相关联,并利用消费者已关注的微信公共号向该微信OpenID推送本次交易信息;

[0054] 微信支付零售信息推送线程为:在消费者微信支付后,获取消费者的微信OpenID,再将消费者的消费者信息与微信OpenID相关联,并将消费者信息和微信OpenID对应存储在后台服务器中,再利用消费者已关注的微信公共号向该微信OpenID推送本次交易信息;

[0055] 支付宝支付零售信息推送线程为:在消费者支付宝支付后,获取消费者的支付宝

OpenID,并生成电子账单二维码供消费者微信扫码,在消费者使用微信扫码后,则获取消费者的微信OpenID,再将该消费者的支付宝OpenID与微信OpenID相关联,并将支付宝OpenID和微信OpenID对应存入后台服务器中,再利用消费者已关注的微信公共号向该微信OpenID推送本次交易信息。

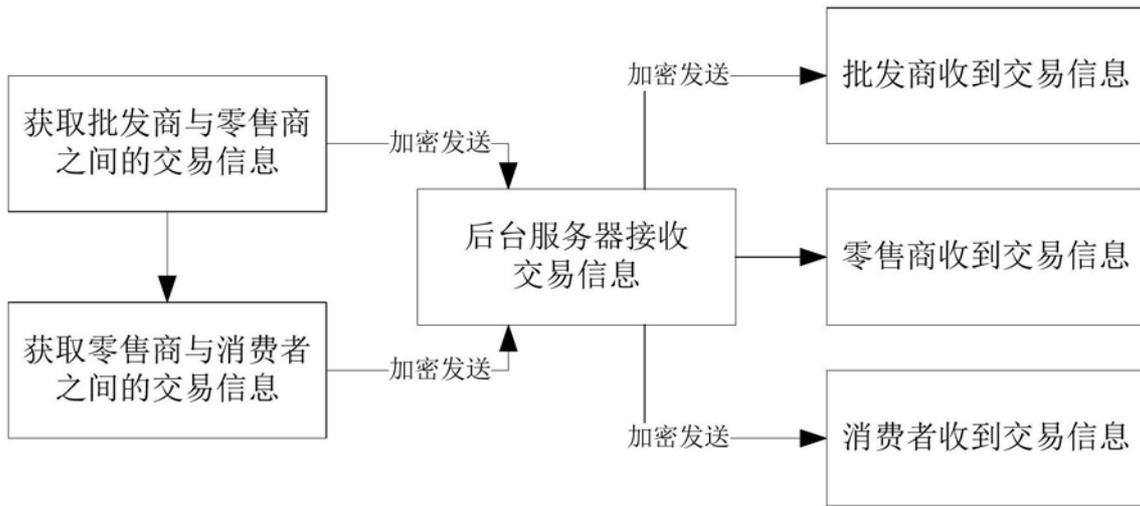


图1