(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 103490978 A
(43)申请公布日 2014.01.01

(21)申请号 201310392651.5

(22)申请日 2013.09.02

(71)申请人 用友软件股份有限公司
地址 100094 北京市海淀区北清路68号用友软件园

(72)发明人 李纯 蒋生锋

(74)专利代理机构 北京友联知识产权代理事务所(普通合伙) 11343
代理人 尚志峰 汪海屏

(51)Int.Cl.
H04L 12/58(2006.01)
H04L 29/06(2006.01)
G06F 17/30(2006.01)

权利要求书2页 说明书7页 附图4页

(54)发明名称

终端、服务器和消息监视方法

(57)摘要

本发明提供了一种终端、一种服务器和一种消息监视方法,其中终端包括:判断单元,用于在第一客户端发送消息至第二客户端时,根据存储在第一客户端的敏感词根表判断消息是否包含敏感词;消息上传单元,连接至判断单元,用于在确定消息包含敏感词时,将消息发送至服务器进行保存。通过本发明的方案,使客户端只有在发送信息触及敏感词时,才开始向服务器端发送此次会话以后的N条记录,防止了大量非敏感信息保存到服务器资源,减轻了服务器压力,也保证了敏感信息的完整性。

CN 103490978 A

1. 一种终端，其特征在于，包括：

判断单元，用于在第一客户端发送消息至第二客户端时，根据存储在所述第一客户端的敏感词根表判断所述消息是否包含敏感词；

消息上传单元，连接至所述判断单元，用于在确定所述消息包含敏感词时，将所述消息发送至服务器进行保存。

2. 根据权利要求 1 所述的终端，其特征在于，所述敏感词根表中每个敏感词具有对应的敏感等级；

所述判断单元还用于在确定所述消息包含敏感词时，根据所述消息中包含的敏感词对应的敏感等级，判断所述消息是否可以被发送至所述第二客户端。

3. 根据权利要求 2 所述的终端，其特征在于，所述终端还包括：提示单元，在确定所述消息不可被发送至所述第二客户端时，提示用户不可发送包含敏感词的消息；

所述消息上传单元还用于在确定所述消息可被发送至所述第二客户端时，将所述消息之后的预设条数的消息发送至所述服务器进行保存。

4. 根据权利要求 1 至 3 中任一项所述的终端，其特征在于，还包括：更新单元和检测单元，所述更新单元用于接收来自所述服务器的新增敏感词，并根据所述新增敏感词更新所述敏感词根表，所述检测单元用于检测所述终端中保存的消息是否包含所述新增敏感词；

所述消息上传单元还用于将所述终端中保存的包含有新增敏感词的消息发送至所述服务器进行保存。

5. 一种服务器，其特征在于，包括：

敏感词同步单元，将设置的敏感词以及敏感词等级同步至各终端；

存储器，接收各所述终端上传的消息，并根据所述消息包含的敏感词类型对所述消息进行分类保存。

6. 一种消息监视方法，其特征在于，包括：

在第一客户端发送消息至第二客户端时，根据存储在所述第一客户端的敏感词根表判断所述消息是否包含敏感词；

在确定所述消息包含敏感词时，将所述消息发送至服务器进行保存。

7. 根据权利要求 6 所述的消息监视方法，其特征在于，还包括：

所述敏感词根表中每个敏感词具有对应的敏感等级；

在确定所述消息包含敏感词时，根据所述消息中包含的敏感词对应的敏感等级，判断所述消息是否可以被发送至所述第二客户端。

8. 根据权利要求 7 所述的消息监视方法，其特征在于，在确定所述消息不可被发送至所述第二客户端时，提示用户不可发送包含敏感词的消息；

在确定所述消息可被发送至所述第二客户端时，将所述消息之后的预设条数的消息发送至所述服务器进行保存。

9. 根据权利要求 6 所述的消息监视方法，其特征在于，所述服务器根据所述消息中包含的敏感词类型对来自所述第一客户端的消息进行分类保存。

10. 根据权利要求 6 至 9 中任一项所述的消息监视方法，其特征在于，还包括：

所述服务器将新增敏感词发送至所述第一客户端，以更新所述敏感词根表；

检测所述第一客户端中保存的消息是否包含所述新增敏感词；

将所述第一客户端中保存的包含有新增敏感词的消息发送至所述服务器进行保存。

终端、服务器和消息监视方法

技术领域

[0001] 本发明涉及计算机技术领域，具体而言，涉及一种终端、一种服务器和一种消息监视方法。

背景技术

[0002] 即时通信（Instant messaging，简称 IM）目前已经成为用户通过网络进行通信的重要手段。随着近些年企业即时通信也在迅速发展，正在逐渐成为企业内部的一种常用的沟通手段。但当企业用户使用时，企业的管理层很难控制员工使用该工具的用途，无法检查其收发的消息是否与工作相关、是否泄漏公司机密等，所以便出现了消息监视系统。

[0003] 目前即时通信的消息监视装置的主要监视方式为：将所有用户发送的文字、文件、图片信息统一存储在服务器端，然后特殊权限人员利用消息监视客户端进行消息监视。但是这种装置有很多弊端，在企业内部即时通信使用频率很高，很容易造成服务器端数据量增长过快，造成查询效率下降，并占用大量服务器资源的问题，企业级即时通信中所应用的 P2P 通道技术优势也无法得到展现，而且存储的大部分信息都是无需监视的非敏感信息。

发明内容

[0004] 为了解决上述技术问题，提出了一种新的消息监视技术，可防止大量非敏感信息保存到服务器资源，减轻了服务器压力。

[0005] 有鉴于此，根据本发明的一个方面，提出了一种终端，包括：判断单元，用于在第一客户端发送消息至第二客户端时，根据存储在所述第一客户端的敏感词根表判断所述消息是否包含敏感词；消息上传单元，连接至所述判断单元，用于在确定所述消息包含敏感词时，将所述消息发送至服务器进行保存。

[0006] 在该技术方案中，在将客户端的消息发送至其他客户端之前，需要根据保存在客户端中的敏感词根表来判断该消息是否包含敏感词，如果包含敏感词，说明该消息可能涉及到需监视的内容，则将该消息上传的服务器进行保存，监视人员可通过该服务器来监视客户端发送的消息，这样可以避免将所有的消息保存至服务器，导致服务器保存的数据量太大，占用系统资源，并且可避免保存很多无需被监视数据的问题，从而影响查询效率。

[0007] 在上述技术方案中，优选的，所述敏感词根表中每个敏感词具有对应的敏感等级；所述判断单元还用于在确定所述消息包含敏感词时，根据所述消息中包含的敏感词对应的敏感等级，判断所述消息是否可以被发送至所述第二客户端。

[0008] 针对每个敏感词，可设置对应的敏感等级，等级越高，说明涉及的内容涉密程度较高，可以设置在敏感等级为二级以上时，禁止发送该消息。因此，在将客户端的消息发送至其他客户端之前，需判断该消息所包含的敏感词的敏感等级，如果是二级以上，该消息就不能被发送至其他终端，进一步提高即时通信的数据安全性。

[0009] 在上述任一技术方案中，优选的，所述终端还可以包括：提示单元，在确定所述消息不可被发送至所述第二客户端时，提示用户不可发送包含敏感词的消息；所述消息上传

单元还用于在确定所述消息可被发送至所述第二客户端时，将所述消息之后的预设条数的消息发送至所述服务器进行保存。

[0010] 如果消息涉密程度较高，则该消息不可被发送至其他终端，并且可提示用户该消息所包含的敏感词，提高用户体验。如果确定包含敏感词的消息可以被发送，则将这之后的消息也上传给服务器进行保存，以便于对本次会话内容进行监视，该预设条数可以根据实际需要被任意设置。

[0011] 在上述任一技术方案中，优选的，还包括：更新单元和检测单元，所述更新单元用于接收来自所述服务器的新增敏感词，并根据所述新增敏感词更新所述敏感词根表，所述检测单元用于检测所述终端中保存的消息是否包含所述新增敏感词；所述消息上传单元还用于将所述终端中保存的包含有新增敏感词的消息发送至所述服务器进行保存。

[0012] 如果新增加敏感词，则可以将该新增的敏感词加入客户端的敏感词根表中进行更新，并检测终端中当前保存的消息是否包含该新增的敏感词，如果包含，则将这些消息上传至服务器进行保存。

[0013] 根据本发明的另一方面，还提供了一种服务器，包括：敏感词同步单元，将设置的敏感词以及敏感词等级同步至各终端；存储器，接收各所述终端上传的消息，并根据所述消息包含的敏感词类型对所述消息进行分类保存。

[0014] 根据本发明的服务器能够对各终端的敏感词根表进行同步更新，并且对客户端之间的交互信息进行交互，并且保存的消息都是涉密信息，减小了服务器的数据保存量，从而降低了系统压力，提高了消息查询效率。

[0015] 根据本发明的再一方面，还提供了一种消息监视方法，包括：在第一客户端发送消息至第二客户端时，根据存储在所述第一客户端的敏感词根表判断所述消息是否包含敏感词；在确定所述消息包含敏感词时，将所述消息发送至服务器进行保存。

[0016] 在该技术方案中，在将客户端的消息发送至其他客户端之前，需要根据保存在客户端中的敏感词根表来判断该消息是否包含敏感词，如果包含敏感词，说明该消息可能涉及到需监视的内容，则将该消息上传的服务器进行保存，监视人员可通过该服务器来监视客户端发送的消息，这样可以避免将所有的消息保存至服务器，导致服务器保存的数据量太大，占用系统资源，并且可避免保存很多无需被监视数据的问题，从而影响查询效率。

[0017] 在上述技术方案中，优选的，还可以包括：所述敏感词根表中每个敏感词具有对应的敏感等级；在确定所述消息包含敏感词时，根据所述消息中包含的敏感词对应的敏感等级，判断所述消息是否可以被发送至所述第二客户端。

[0018] 针对每个敏感词，可设置对应的敏感等级，等级越高，说明涉及的内容涉密程度较高，可以设置在敏感等级为二级以上时，禁止发送该消息。因此，在将客户端的消息发送至其他客户端之前，需判断该消息所包含的敏感词的敏感等级，如果是二级以上，该消息就不能被发送至其他终端，进一步提高即时通信的数据安全性。

[0019] 在上述任一技术方案中，优选的，在确定所述消息不可被发送至所述第二客户端时，提示用户不可发送包含敏感词的消息；在确定所述消息可被发送至所述第二客户端时，将所述消息之后的预设条数的消息发送至所述服务器进行保存。

[0020] 如果消息涉密程度较高，则该消息不可被发送至其他终端，并且可提示用户该消息所包含的敏感词，提高用户体验。如果确定包含敏感词的消息可以被发送，则将这之后的

消息也上传给服务器进行保存，以便于对本次会话内容进行监视，该预设条数可以根据实际需要被任意设置。

[0021] 在上述任一技术方案中，优选的，所述服务器根据所述消息中包含的敏感词类型对来自所述第一客户端的消息进行分类保存。

[0022] 在上述任一技术方案中，优选的，还可以包括：所述服务器将新增敏感词发送至所述第一客户端，以更新所述敏感词根表；检测所述第一客户端中保存的消息是否包含所述新增敏感词；将所述第一客户端中保存的包含有新增敏感词的消息发送至所述服务器进行保存。

[0023] 如果新增加敏感词，则可以将该新增的敏感词加入客户端的敏感词根表中进行更新，并检测终端中当前保存的消息是否包含该新增的敏感词，如果包含，则将这些消息上传至服务器进行保存。

附图说明

[0024] 图 1 示出了根据本发明的实施例的终端的框图；

[0025] 图 2 示出了根据本发明的实施例的服务器的框图；

[0026] 图 3 示出了根据本发明的一个实施例的消息监视方法的流程图；

[0027] 图 4 示出了根据本发明的另一实施例的新增敏感词的消息监视处理过程的示意图；

[0028] 图 5 示出了根据本发明的另一实施例的消息监视方法的流程图。

具体实施方式

[0029] 为了能够更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

[0030] 在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的其他方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

[0031] 图 1 示出了根据本发明的实施例的终端的框图。

[0032] 如图 1 所示，根据本发明的实施例的终端 100，包括：判断单元 102，用于在第一客户端发送消息至第二客户端时，根据存储在所述第一客户端的敏感词根表判断所述消息是否包含敏感词；消息上传单元 104，连接至所述判断单元，用于在确定所述消息包含敏感词时，将所述消息发送至服务器进行保存。

[0033] 在该技术方案中，在将客户端的消息发送至其他客户端之前，需要根据保存在客户端中的敏感词根表来判断该消息是否包含敏感词，如果包含敏感词，说明该消息可能涉及到需监视的内容，则将该消息上传的服务器进行保存，监视人员可通过该服务器来监视客户端发送的消息，这样可以避免将所有的消息保存至服务器，导致服务器保存的数据量太大，占用系统资源，并且可避免保存很多无需被监视数据的问题，从而影响查询效率。

[0034] 在上述技术方案中，优选的，所述敏感词根表中每个敏感词具有对应的敏感等级；所述判断单元 102 还用于在确定所述消息包含敏感词时，根据所述消息中包含的敏感词对

应的敏感等级，判断所述消息是否可以被发送至所述第二客户端。

[0035] 针对每个敏感词，可设置对应的敏感等级，等级越高，说明涉及的内容涉密程度较高，可以设置在敏感等级为二级以上时，禁止发送该消息。因此，在将客户端的消息发送至其他客户端之前，需判断该消息所包含的敏感词的敏感等级，如果是二级以上，该消息就不能被发送至其他终端，进一步提高即时通信的数据安全性。

[0036] 在上述任一技术方案中，优选的，所述终端还可以包括：提示单元 106，在确定所述消息不可被发送至所述第二客户端时，提示用户不可发送包含敏感词的消息；所述消息上传单元 104 还用于在确定所述消息可被发送至所述第二客户端时，将所述消息之后的预设条数的消息发送至所述服务器进行保存。

[0037] 如果消息涉密程度较高，则该消息不可被发送至其他终端，并且可提示用户该消息所包含的敏感词，提高用户体验。如果确定包含敏感词的消息可以被发送，则将这之后的消息也上传给服务器进行保存，以便于对本次会话内容进行监视，该预设条数可以根据实际需要被任意设置。

[0038] 在上述任一技术方案中，优选的，还可以包括：更新单元 108 和检测单元 110，所述更新单元 108 用于接收来自所述服务器的新增敏感词，并根据所述新增敏感词更新所述敏感词根表，所述检测单元 110 用于检测所述终端中保存的消息是否包含所述新增敏感词；所述消息上传单元 104 还用于将所述终端中保存的包含有新增敏感词的消息发送至所述服务器进行保存。

[0039] 如果新增加敏感词，则可以将该新增的敏感词加入客户端的敏感词根表中进行更新，并检测终端中当前保存的消息是否包含该新增的敏感词，如果包含，则将这些消息上传至服务器进行保存。

[0040] 图 2 示出了根据本发明的实施例的服务器的框图。

[0041] 如图 2 所示，根据本发明的实施例的服务器 200 包括：敏感词同步单元 202，将设置的敏感词以及敏感词等级同步至各终端；存储器 204，接收各所述终端上传的消息，并根据所述消息包含的敏感词类型对所述消息进行分类保存。

[0042] 根据本发明的服务器能够对各终端的敏感词根表进行同步更新，并且对客户端之间的交互信息进行交互，并且保存的消息都是涉密信息，减小了服务器的数据保存量，从而降低了系统压力，提高了消息查询效率。

[0043] 下面结合图 3 和图 4 来详细说明根据本发明的消息监视方法。

[0044] 如图 3 所示，发送客户端发送消息的处理流程描述：

[0045] 步骤 302，发送客户端发送信息。

[0046] 步骤 304，发送客户端根据客户端敏感词根表判断信息中是否包含敏感词汇。

[0047] 步骤 306，若未包含敏感词汇，则将此信息通过 P2P 通道发送给接收客户端。

[0048] 步骤 308，若包含敏感词汇，根据敏感词等级判断此消息是否能够继续发送给接收客户端。

[0049] 步骤 310，若判断此消息可继续发送，则将此消息通过 P2P 通道发送给接收客户端，并将此条消息及之后的 N 条消息记录传送至服务器端。

[0050] 步骤 312，若判断不可继续发送此消息，则将此消息上传服务器端。

[0051] 步骤 314，提示发送客户端不可发送此类包含敏感词的信息。

[0052] 步骤 316，包含敏感词汇的会话记录上传服务器端后，服务器端分析上传消息类型，将其分类存储于数据库中。

[0053] 消息管理人员可使用消息监视管理客户端，通过消息监视管理模块进行敏感信息查询及管理。

[0054] 下面以具体示例来说明上述处理过程。

[0055] A 客户端发送了一条消息给 B 客户端，消息内容为“单号为 Doc00007 的产品内部价格是多少？”。

[0056] 即时通信客户端根据客户端敏感词根表判断信息中是否包含敏感词汇，若不包含，则通过 P2P 通道将此消息发送给 B 客户端；若本地敏感词根表中包含“单号”敏感词，则此消息则包含了敏感词汇，根据此敏感词汇的等级判断此消息是否可继续发送。

[0057] 若不可继续发送，则提示 A 客户端，不可发送包含“单号”的消息，并将此消息记录上传至服务器端；若可以继续发送，则将此消息通过 P2P 通道发送给 B 客户端，并将此消息及之后的 N（用户可设置）条会话记录上传至服务器端。

[0058] 即时通信服务器端接收到包含敏感词汇的消息后，根据消息类型，将消息分类存储到服务器数据库中。

[0059] 消息管理人员 C，可使用消息监视管理客户端，通过消息监视管理模块进行敏感信息查询及管理。

[0060] 继续参考图 3，客户端删除消息的处理流程描述如下：

[0061] 即时通信客户端删除本地消息记录。

[0062] 首先删除不可见且发送时间与当前时间的时间间隔大于客户端消息保留期的消息记录。

[0063] 步骤 318，判断所删除消息发送时间与当前时间的时间间隔是否大于客户端消息保留期(用户可设，如设置为 1 年)，此判断保证当有新敏感词汇添加到本地时，可以对在保留期内的消息记录进行比对，上传涉及新敏感词汇的消息记录。

[0064] 步骤 322，若大于消息保留期，则直接删除此本地消息记录。

[0065] 步骤 320，若不大于消息保留期，则将消息置为本地不可见，但不删除数据。

[0066] 下面以具体示例来说明上述处理过程。

[0067] A 客户端删除一些本地消息记录。

[0068] 客户端首先删除客户端不可见且发送时间与当前时间的时间间隔大于客户端消息保留期的消息记录，然后判断要删除的消息记录发送时间与当前时间的时间间隔是否大于客户端消息保留期 1 年。

[0069] 若消息记录发送时间与当前时间的时间间隔大于 1 年，则直接从本地数据库中删除此消息记录；否则只将此消息记录置为客户端不可见，但不从本地数据库中删除此消息记录。

[0070] 如图 4 所示，为客户端新增敏感词的处理流程，该流程描述如下：

[0071] 步骤 402，消息监视管理人员，通过消息监视管理客户端在即时服务器中添加敏感词。

[0072] 步骤 404，新增敏感词通过即时通信服务器，发送到即时通信客户端，即时通信客户端将新增敏感词添加到客户端敏感词根表中。

[0073] 步骤 406，创建新线程，检查客户端消息记录中是否包含此新增敏感词，如果不包含，则进入步骤 410，做任何处理；若有包含新增敏感词的消息记录，则金融步骤 408，将此消息及之后的 N（用户可设）条会话记录上传服务器端。

[0074] 下面以具体示例来说明上述处理过程。

[0075] 消息监视管理员 A，通过消息监视管理客户端新添敏感词“改革”。

[0076] 此新增敏感词，通过服务器端发送到 B 客户端。

[0077] B 客户端将“改革”添加到客户端敏感词根表中，并创建新线程，检查 B 客户端的消息记录中是否包含敏感词“改革”，若查找到包含此敏感词的消息记录，则将此消息记录及之后与其有关的 N 条会话记录上传至服务器端。

[0078] 图 5 示出了根据本发明的另一实施例的消息监视方法的流程图。

[0079] 如图 5 所示，根据本发明的实施例的消息监视方法可以包括以下步骤：步骤 502，在第一客户端发送消息至第二客户端时，根据存储在所述第一客户端的敏感词根表判断所述消息是否包含敏感词；步骤 504，在确定所述消息包含敏感词时，将所述消息发送至服务器进行保存。

[0080] 在该技术方案中，在将客户端的消息发送至其他客户端之前，需要根据保存在客户端中的敏感词根表来判断该消息是否包含敏感词，如果包含敏感词，说明该消息可能涉及到需监视的内容，则将该消息上传的服务器进行保存，监视人员可通过该服务器来监视客户端发送的消息，这样可以避免将所有的消息保存至服务器，导致服务器保存的数据量太大，占用系统资源，并且可避免保存很多无需被监视数据的问题，从而影响查询效率。

[0081] 在上述技术方案中，优选的，还可以包括：所述敏感词根表中每个敏感词具有对应的敏感等级；在确定所述消息包含敏感词时，根据所述消息中包含的敏感词对应的敏感等级，判断所述消息是否可以被发送至所述第二客户端。

[0082] 针对每个敏感词，可设置对应的敏感等级，等级越高，说明涉及的内容涉密程度较高，可以设置在敏感等级为二级以上时，禁止发送该消息。因此，在将客户端的消息发送至其他客户端之前，需判断该消息所包含的敏感词的敏感等级，如果是二级以上，该消息就不能被发送至其他终端，进一步提高即时通信的数据安全性。

[0083] 在上述任一技术方案中，优选的，在确定所述消息不可被发送至所述第二客户端时，提示用户不可发送包含敏感词的消息；在确定所述消息可被发送至所述第二客户端时，将所述消息之后的预设条数的消息发送至所述服务器进行保存。

[0084] 如果消息涉密程度较高，则该消息不可被发送至其他终端，并且可提示用户该消息所包含的敏感词，提高用户体验。如果确定包含敏感词的消息可以被发送，则将这之后的消息也上传给服务器进行保存，以便于对本次会话内容进行监视，该预设条数可以根据实际需要被任意设置。

[0085] 在上述任一技术方案中，优选的，所述服务器根据所述消息中包含的敏感词类型对来自所述第一客户端的消息进行分类保存。

[0086] 在上述任一技术方案中，优选的，还可以包括：所述服务器将新增敏感词发送至所述第一客户端，以更新所述敏感词根表；检测所述第一客户端中保存的消息是否包含所述新增敏感词；将所述第一客户端中保存的包含有新增敏感词的消息发送至所述服务器进行保存。

[0087] 如果新增加敏感词，则可以将该新增的敏感词加入客户端的敏感词根表中进行更新，并检测终端中当前保存的消息是否包含该新增的敏感词，如果包含，则将这些消息上传至服务器进行保存。

[0088] 通过上述消息监视方法，使客户端只有在发送信息触及敏感词时，才开始向服务器端发送此次会话以后的 N 条记录，防止了大量非敏感信息保存到服务器资源，减轻了服务器压力，也保证了敏感信息的完整性，使得管理层对信息监视更加高效。

[0089] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

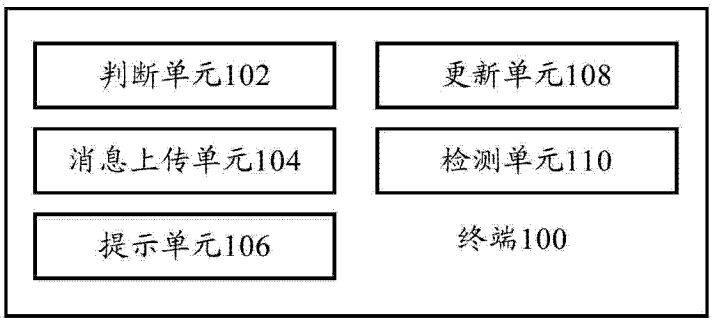
判断单元102
更新单元108
消息上传单元104
检测单元110
提示单元106
终端100

图 1


敏感词同步单元202
存储器204
服务器200

图 2

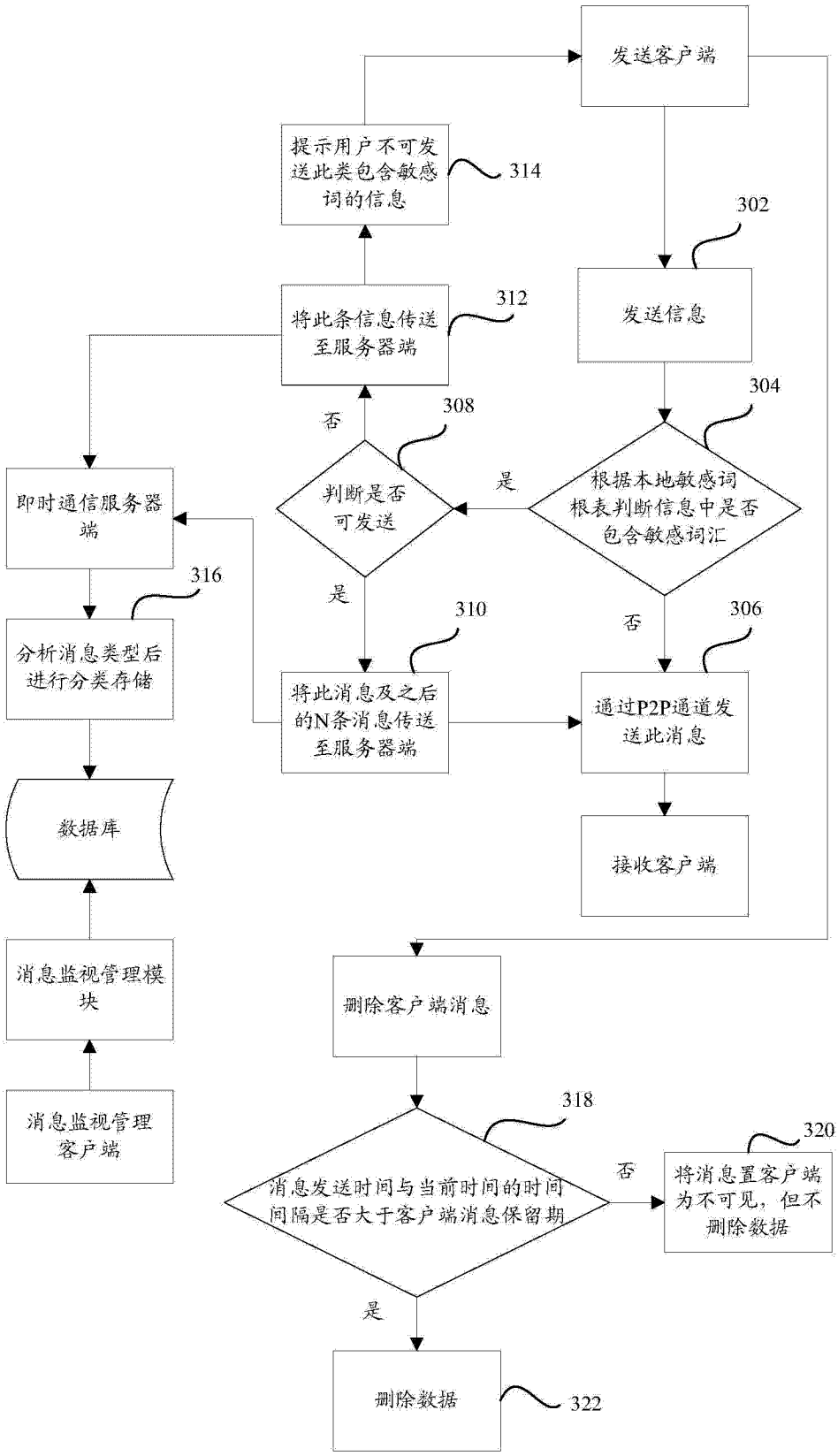
发送客户端
302
发送信息
304
根据本地敏感词根表判断信息中是否包含敏感词汇
是
否
306
通过P2P通道发送此消息
接收客户端
删除客户端消息
318
消息发送时间与当前时间的时间间隔是否大于客户端消息保留期
否
320
将消息置客户端为不可见，但不删除数据
是
删除数据
322
308
判断是否可发送
否
是
310
将此消息及之后的N条消息传送至服务器端
312
将此条信息传送至服务器端
314
提示用户不可发送此类包含敏感词的信息
即时通信服务器端
316
分析消息类型后进行分类存储
数据库
消息监视管理模块
消息监视管理客户端

图 3

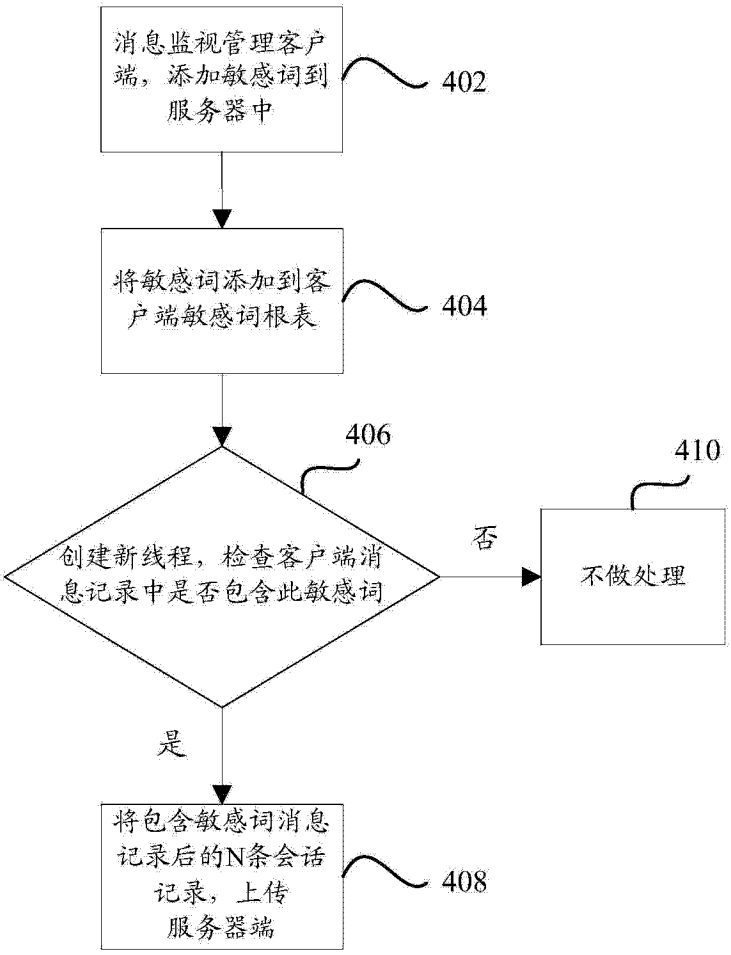
消息监视管理客户端，添加敏感词到服务器中
402
将敏感词添加到客户端敏感词根表
404
406
创建新线程，检查客户端消息记录中是否包含此敏感词
否
410
不做处理
是
将包含敏感词消息记录后的N条会话记录，上传服务器端
408

图 4

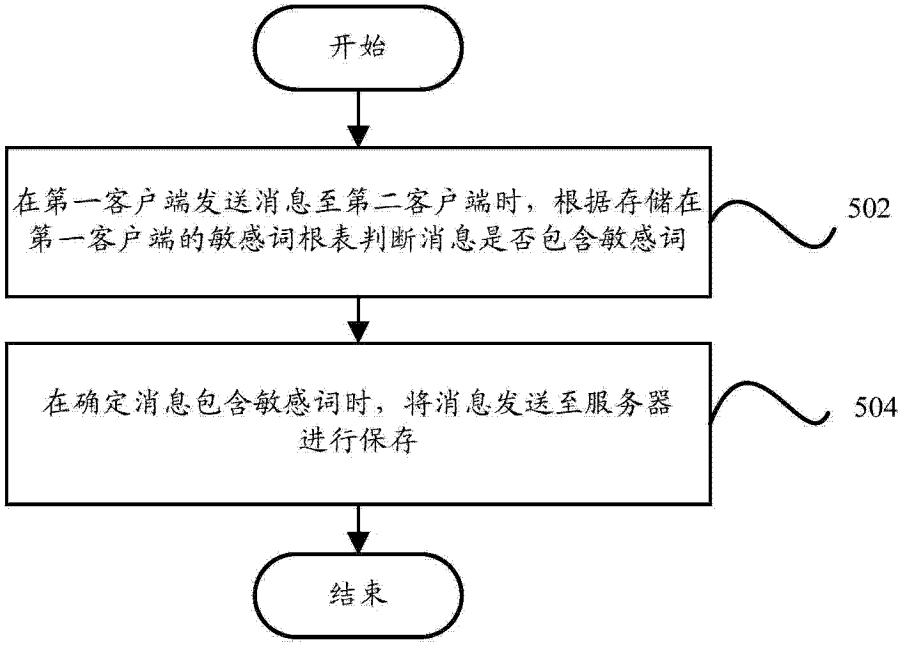
开始
在第一客户端发送消息至第二客户端时，根据存储在第一客户端的敏感词根表判断消息是否包含敏感词
502
在确定消息包含敏感词时，将消息发送至服务器进行保存
504
结束

图 5