(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102203796 B
(45)授权公告日 2014.06.18

(21)申请号 200980143665.5
(22)申请日 2009.11.03
(30)优先权数据
08305772.9 2008.11.04 EP
12/269,243 2008.11.12 US
(85)PCT国际申请进入国家阶段日
2011.05.04
(86)PCT国际申请的申请数据
PCT/EP2009/064551 2009.11.03
(87)PCT国际申请的公布数据
WO2010/052218 EN 2010.05.14
(73)专利权人 阿玛得斯两合公司
地址 法国比奥
(72)发明人 R·格兰冈 F·里希耶斯基
C·奥亚梅斯 M·蒙特莱 S·罗伊
J·巴雷特
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 李向英
(51)Int.Cl.
G06F 21/62(2013.01)
(56)对比文件
US 2008/0240447 A1,2008.10.02,
CN 1295688 A,2001.05.16,
WO 03/088052 A1,2003.10.23,
审查员 吴琼

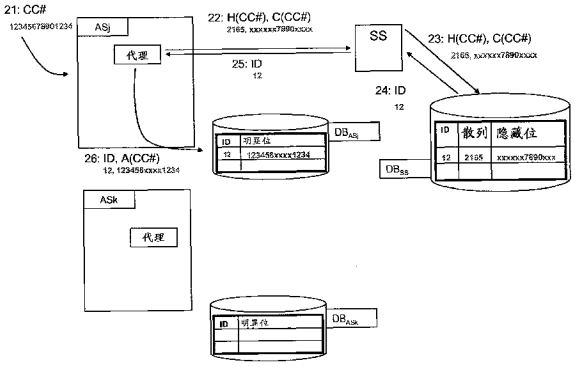
权利要求书4页 说明书11页 附图6页

(54)发明名称

存储和检索信息的方法和系统

(57)摘要

一种存储和检索与敏感信息(CC#)相关联的使用数据((CC#)、应用性数据)的方法,信息在包括多个能够使用信息的应用系统($ASi_{i=1..n}$)的环境中要求保证其安全性,存储信息包括下述步骤:在多个应用系统中给定应用系统(AS_j):接收信息,从信息产生提取的数据(C(CC#))和补足数据(A(CC#)),从信息产生编码的信息(H(CC#)),向服务器系统(SS)发送所提取的数据和所编码的信息,在服务器系统:产生索引ID并向所编码的信息和所提取的数据分配这个索引ID,在与服务器系统相关联的数据库(DB_{SS})中存储所编码的信息、所提取的数据和索引ID,向多个应用系统的给定应用系统转发索引ID,在给定应用系统:向与信息有关的、应用存储的数据(A(CC#)、应用性数据)分配索引ID,在与给定应用系统相关联的数据库(DB_{ASj})中与应用存储的数据一起存储索引ID。



CN 102203796 B

1. 一种存储和检索敏感信息的方法，所述敏感信息在包括多个能够使用所述信息的应用系统的环境中要求保证其安全性，所述方法包括：

●在所述多个应用系统的给定应用系统：

- 接收所述信息，

- 从所述信息产生提取的数据和补足数据，使得独立地取得的所述提取的数据和所述补足数据不足以使用所述信息，以及使得从一起取得的所述提取的数据和补足数据能够产生所述信息，

- 从所述信息产生编码的信息，

- 向服务器系统发送所提取的数据和所编码的信息，

●在服务器系统：

- 产生索引并向所编码的信息和所提取的数据分配这个索引，

- 在与服务器系统相关联的数据库中存储所编码的信息、所提取的数据和索引，

- 向多个应用系统的所述给定应用系统转发索引，

●在所述给定应用系统：

- 向补足数据分配索引，

- 在与所述给定应用系统相关联的数据库中与所述补足数据一起存储索引。

2. 根据权利要求 1 的方法，还包括在多个应用系统之中任何所考虑的应用系统检索所述信息，该检索步骤包括以下步骤：

●在所述所考虑的应用系统：

- 接收索引，

- 向服务器系统发送索引，

●在服务器系统：

- 从服务器系统的数据库检索所述索引所对应的所提取的数据，

- 向所述所考虑的应用系统发送所提取的数据，

●在所述所考虑的应用系统：

- 接收补足数据，

- 从所提取的数据和补足数据重建信息。

3. 根据权利要求 2 的方法，其中，所述所考虑的应用系统是给定应用系统，以及在所述所考虑的应用系统接收补足数据包括基于索引检索补足数据，它被存储在与给定应用系统相关联的数据库中。

4. 根据权利要求 2 的方法，其中，所述所考虑的应用系统是不同于给定应用系统的应用系统，并且它不包括连同补足数据存储所述索引的数据库，以及在所述所考虑的应用系统接收补足数据包括从所述给定应用系统接收补足数据。

5. 根据权利要求 1 的方法，其中，所述产生补足数据和提取的数据的步骤包括把信息划分为第一部分和第二部分。

6. 根据权利要求 5 的方法，其中，信息是信用卡号，以及补足数据对应于所述信用卡号的明显位，而所提取的数据对应于所述信用卡号的隐藏位。

7. 根据权利要求 1 的方法，其中，产生编码的信息的步骤包括以散列函数计算信息的散列值，所述散列函数对于服务器系统未知。

8. 根据权利要求 1 的方法，其中，在任何应用系统所进行的以下步骤中的至少一个由代理组件操作：

●从信息产生补足数据和所提取的数据，

●从所述信息产生所编码的信息，

●向服务器系统发送所提取的数据和所编码的信息，

●发送与给定应用系统相关联的数据库中的补足数据，

●产生若干消息，包括要从所述任何应用系统发送的数据，所述消息采用似 EDIFACT 格式，

●读取若干消息，包括要在所述任何应用系统接收的数据，所述消息采用似 EDIFACT 格式。

9. 根据权利要求 1 的方法，其中，在任何时间，信息仅仅在处理所述信息的应用系统的处理存储器中可用。

10. 一种存储和检索敏感信息的系统，所述敏感信息在包括多个能够使用所述信息的应用系统的环境中要求保证其安全性，所述系统包括：

●在所述多个应用系统之中的给定应用系统，所述给定应用系统包括：

- 用于接收所述信息的装置，

- 用于从所述信息产生提取的数据和补足数据，使得独立地取得的所述所提取的数据和所述补足数据不足以由任何应用系统使用所述信息，以及使得从一起取得的所述所提取的数据和补足数据产生所述信息的装置，

- 用于从所述信息产生编码的信息的装置，

- 用于向服务器系统发送所提取的数据和所编码的信息的装置，

●服务器系统，所述服务器系统包括：

- 用于产生索引并向所编码的信息和所提取的数据分配这个索引的装置，

- 用于在与服务器系统相关联的数据库中存储所编码的信息、所提取的数据和索引的装置，

- 用于向多个应用系统的所述给定应用系统转发索引的装置，

●给定应用系统还包括：

- 用于向补足数据分配索引的装置，

- 用于在与所述给定应用系统相关联的数据库中与所述补足数据一起存储索引的装置。

11. 一种存储和检索与敏感信息相关联的应用性数据的方法，所述敏感信息在包括多个能够使用所述信息的应用系统的环境中要求保证其安全性，所述方法包括：

●在所述多个应用系统的给定应用系统：

- 接收所述信息，

- 从所述信息产生提取的数据，使得独立地取得的所述所提取的数据不足以使用所述信息，以及使得从一起取得的所述所提取的数据和补足数据能够产生所述信息，所述补足数据还从所述信息产生并在独立取得时不足以使用所述信息，

- 从所述信息产生编码的信息，

- 向服务器系统发送所提取的数据和所编码的信息，

●在服务器系统：

- 产生索引并向所编码的信息和所提取的数据分配这个索引，
- 在与服务器系统相关联的数据库中存储所编码的信息、所提取的数据和索引，
- 向多个应用系统的所述给定应用系统转发索引，

●在所述给定应用系统：

- 向与信息相关联的应用性数据分配索引，
- 在与所述给定应用系统相关联的数据库中与所述应用性数据一起存储索引。

12. 根据权利要求 11 的方法，其中，应用性数据至少由应用系统使用并且不要求高级别的安全性。

13. 根据权利要求 12 的方法，其中应用性数据涉及忠诚度程序。

14. 根据权利要求 11 的方法，还包括在任何所考虑的应用系统检索所述应用性数据，所述检索步骤包括以下步骤：

●在所述所考虑的应用系统：

- 接收所述信息，
- 从所述信息产生所提取的数据，以及从所述信息产生所编码的信息，
- 向服务器系统发送所提取的数据和所编码的信息，

●在服务器系统：

- 从服务器系统的数据库检索对应于所提取的数据和所编码的信息的索引，
- 向所述所考虑的应用系统转发索引，

●在所述所考虑的应用系统：

- 接收索引，
- 检索以索引定位的应用性数据。

15. 根据权利要求 14 的方法，其中，所述所考虑的应用系统是给定应用系统，以及应用性数据是从与给定应用系统相关联的数据库检索的。

16. 根据权利要求 14 的方法，其中，所述所考虑的应用系统是不同于给定应用系统的应用系统，并且在其相关联数据库中不包括以索引定位的应用性数据，以及检索应用性数据包括以下步骤：

●在给定应用系统：

- 接收将被检索的应用性数据所对应的索引，
- 在给定应用系统的数据库中检索基于索引的应用性数据，
- 向所考虑的应用系统发送所述应用性数据。

17. 根据权利要求 11 的方法，其中，产生补足数据和所提取的数据的步骤包括把信息划分为第一部分和第二部分。

18. 根据权利要求 17 的方法，其中，信息是信用卡号，以及补足数据对应于所述信用卡号的明显位，而所提取的数据对应于所述信用卡号的隐藏位。

19. 根据权利要求 11 的方法，其中，产生编码的信息的步骤包括以散列函数计算信息的散列值，所述散列函数对于服务器系统未知。

20. 根据权利要求 11 的方法，其中，在任何应用系统所进行的以下步骤中的至少一个由代理组件操作：

●从信息产生所提取的数据，

●从所述信息产生所编码的信息，

●向服务器系统发送所提取的数据和所编码的信息，

●产生若干消息，包括要从所述任何应用系统发送的数据，所述消息采用似 EDIFACT 格式，

●读取若干消息，包括要在所述任何应用系统接收的数据，所述消息采用似 EDIFACT 格式。

21. 根据权利要求 11 的方法，其中，在任何时间，信息仅仅在处理所述信息的应用系统的处理存储器中可用。

22. 一种存储和检索与敏感信息相关联的应用性数据的系统，所述敏感信息在包括多个能够使用所述信息的应用系统的环境中要求保证其安全性，所述系统包括：

●在所述多个应用系统之中的给定应用系统，所述给定应用系统包括：

- 用于接收所述信息的装置，

- 用于从所述信息产生提取的数据，使得独立地取得的所述所提取的数据不足以由任何应用系统使用所述信息，以及使得从一起取得的所述提取的数据和补足数据产生所述信息的装置，所述补足数据还从所述信息产生并且当独立地取得时不足以使用所述信息，

- 用于从所述信息产生编码的信息的装置，

- 用于向服务器系统发送所提取的数据和所编码的信息的装置，

●服务器系统，所述服务器系统包括：

- 用于产生索引并向所编码的信息和所提取的数据分配这个索引的装置，

- 用于在与服务器系统相关联的数据库中存储所编码的信息、所提取的数据和索引的装置，

- 用于向多个应用系统的所述给定应用系统转发索引的装置，

●给定应用系统还包括：

- 用于向与所述信息相关联的应用性数据分配索引的装置，

- 用于在与所述给定应用系统相关联的数据库中与所述应用性数据一起存储索引的装置。

存储和检索信息的方法和系统

技术领域

[0001] 一般来说，本发明涉及存储和检索电子信息的方法和系统。本发明的方法和系统尤其针对要求保证其安全并且必须对多种应用的使用可用的电子信息的存储。本方法也指存储和检索与信息有关的使用数据的方法。

背景技术

[0002] 保证敏感信息的存储和操作安全是个主要问题，尤其是对于许多应用不得不使用这样的敏感信息的组织。

[0003] 电子交易的发展增加了要求敏感信息的交易的数目。另外，为了便利交易以及对用户更有吸引力，许多组织努力消除为了完成交易重新输入全部所需数据的需要。这暗示了存储敏感信息。然而，存储敏感信息可能很难完全安全。确实，存储敏感信息的数据库可能被窃或者遭受黑客攻击。另外，在敏感信息从存储它的数据库向处理它的应用传送期间，它可能被非法检索。

[0004] 为了提高存储的安全性，某些系统允许将敏感信息拆分为两部分并将每个部分存储在各自的数据库中。

[0005] 不过，这些系统已经证实并非完全令人满意，尤其是在多种应用需要处理同一敏感信息的环境中。

[0006] 这多种应用可能由提供许多服务的单一组织运行。若干全球分布系统 (GDS) 比如 AMADEUS 或 SABRE 是这样的组织的典型实例，它们提供的许多服务涉及要求敏感信息的多种应用。

[0007] 几个截然不同的公司也可以合作以向消费者提供整合的服务。例如，电子商务和银行可以合作以向消费者提供容易的在线采购解决方案。几家商户也能够合作以形成组织并向消费者提供范围更宽的服务和产品。

[0008] 本发明的目的是提供高效且有用户吸引力的方法，以在许多应用可能需要处理同一敏感信息的环境中存储和检索信息。

发明内容

[0009] 本发明介绍了存储和检索与敏感信息相关联的使用数据的方法，该敏感信息在包括多个能够使用信息和使用数据的应用系统 $ASi_{i=1..n}$ 的分布式环境中要求保证其安全。敏感信息的典型实例为信用卡号。存储信息包括下述步骤。

[0010] 多个应用系统 $ASi_{i=1..n}$ 中给定应用系统 AS_j 接收信息并从信息产生提取的数据和补足数据。所提取的数据和补足数据按以下方式产生：

[0011] - 独立地取得它们时，任何应用系统 $ASi_{i=1..n}$ 都不可能使用敏感信息，以及

[0012] - 一起取得它们时，便能够产生和使用信息。

[0013] 另外，所述给定应用系统 AS_j 从信息产生编码的信息。然后，它向服务器系统 SS 发送所提取的数据和所编码的信息。

[0014] 所述服务器系统 SS 产生索引 ID 并向所编码的信息和所提取的数据分配这个索引 ID。然后服务器系统 SS 在与服务器系统 SS 相关联的数据库 DB_{SS} 中存储所编码的信息、所提取的数据和索引 ID。所述服务器服务器 SS 进一步向多个应用系统 $ASi_{i=1..n}$ 中给定应用系统 AS_j 转发索引 ID。

[0015] 然后，给定应用系统 AS_j 向与信息有关的、应用存储的数据分配索引 ID。最后，给定应用系统 AS_j 在与给定应用系统 AS_j 相关联的数据库 DB_{ASj} 中与应用存储的数据一起存储索引 ID。

[0016] 根据本发明的第一种使用情况，使用数据是信息，而应用存储的数据是补足数据。

[0017] 因此，给定应用系统 AS_j 仅仅发送所提取的数据和所编码的信息。不存在敏感信息的交换。另外，由于给定应用系统 AS_j 的数据库 DB_{ASj} 仅仅存储补足数据和 ID 而服务器系统的数据库 DB_{SS} 仅仅存储所提取的数据、所编码的信息和索引 ID，那么所提取的和补足数据绝不会存储在同一数据库中。所以，搜寻所述网络、窃取或黑客攻击给定应用系统 AS_j 的数据库或服务器系统 SS 的数据库中任何一个都不能够或者获得补足和提取的数据或者获得完整信息。所以信息无法被重建和非法使用。

[0018] 另外，索引 ID 由服务器系统 SS 而不是由接收信息的给定应用系统 AS_j 产生。因此，索引 ID 被分配给由编码的信息和提取的数据形成的单一对。所以，不存在与同一信息有关的并发的索引 ID。为了交换与给定信息有关的数据，各种应用系统 $ASi_{i=1..n}$ 能够共享与所述信息相关联的唯一索引 ID。所以，本发明尤为便于在许多应用系统 $ASi_{i=1..n}$ 使用敏感信息的分布式环境中存储所述敏感信息。

[0019] 服务器系统 SS 的数据库 DB_{SS} 存储所提取的数据，连同所编码的信息和索引 ID。因此，应用系统能够或者在向所述应用系统提供了索引 ID 时接收所提取的数据，或者在应用系统访问所提取的数据和所编码的信息时接收索引 ID。所以，这样的方法允许向多个应用系统 $ASi_{i=1..n}$ 提供这些应用系统 $ASi_{i=1..n}$ 应对预定的使用时需要的各种数据。所以，本发明允许安全的存储，用于多个应用系统 $ASi_{i=1..n}$ 应对的多种操作。

[0020] 即使一个或许多应用模块 $ASi_{i=1..n}$ 被窃、受迫或受到黑客攻击，信息也无法检索。得到所述编码过程确实不能获得信息，因为所提取的数据和所编码的信息都不存储在与各种应用系统 $ASi_{i=1..n}$ 相关联的数据库 DB_{ASi} 中。因此，本发明增强了信息存储的安全性。

[0021] 根据本发明，在多个应用系统 $ASi_{i=1..n}$ 中任何所考虑的应用系统 AS_k 检索敏感信息都包括以下步骤。所述所考虑的应用系统 AS_k 接收索引 ID，以及向服务器系统 SS 发送索引 ID。服务器系统 SS 从服务器系统 SS 的数据库检索所述 ID 对应的所提取的数据。它进一步向所述所考虑的应用系统 AS_k 发送所提取的数据。然后，所考虑的应用系统 AS_k 接收补足数据并且从所提取的数据和补足数据重建信息。因此，所考虑的应用系统 AS_k 的应用能够使用信息。

[0022] 所述完整的敏感信息既不交换也不存储。信息仅仅在所考虑的应用系统 AS_k 应对需要所述敏感信息的处理时在所考虑的应用系统 AS_k 可用。典型情况下，信息存储在所述处理存储器中而不在别处。一旦使用完成，信息便被去除。另外，所提取的和补足数据不存储在同一数据库中。所以，搜寻所述网络或者窃取所述数据库中任何一个都不能够获得敏感信息。

[0023] 由于本发明允许通过仅仅输入索引便使敏感信息可用，所以本发明消除了敏感信

息的附加重新输入或操作。所以，本发明降低了用户操作或输入敏感信息时其损失或被窃的风险。

[0024] 根据这第一种使用情况的第一个事件，所述所考虑的应用系统 AS_k 是给定应用系统 AS_j。因此，在所述所考虑的应用系统 AS_k 接收补足数据的步骤包括在所述给定应用系统 AS_j 接收索引 ID 以及由于索引 ID，检索在与给定应用系统 AS_j 相关联的数据库 DB_{ASj} 中存储的补足数据。

[0025] 因此，在已经向需要信息的所考虑的应用系统 AS_k 提供了这种信息的情况下，在收到索引 ID 后，能够从所考虑的应用系统 AS_k 的数据库 DB_{ASk} 直接检索补足数据。另外，向服务器系统 SS 发送所述索引触发了从服务器系统 SS 转发所提取的数据。然后应用系统 AS_k 获得所提取的和补足数据并且能够获得所述需要的信息。

[0026] 根据这第一种使用情况的第二个事件，所考虑的应用系统 AS_k 不同于给定应用系统 AS_j。另外，所考虑的应用 AS_k 不包括连同索引 ID 一起定位补足数据的数据库。因此，在所述所考虑的应用系统 AS_k 接收补足数据的上述步骤包括从给定应用系统 AS_j 接收补足数据。

[0027] 更确切地说，当所考虑的应用 AS_k 收到索引 ID 并要求这个索引 ID 对应的信息时，它检查这个索引 ID 是否存储在其相关联的数据库 DB_{ASk} 中。在这个数据库不包括这个索引 ID 或者不包括所述索引对应的补足数据的情况下，所述所考虑的应用系统 AS_k 发送请求。这个请求包括所要求信息的索引 ID。所述请求到达给定应用系统 AS_j。给定应用系统 AS_j 关联到用索引 ID 来定位补足数据的数据库。

[0028] 响应所述请求，给定应用系统 AS_j 从其数据库 DB_{ASj} 检索补足数据并将它转发到所考虑的应用系统 AS_k。另外，所考虑的应用系统 AS_k 向服务器系统 SS 发送所述索引以便接收所提取的数据。因此，所考虑的 AS_k 应用系统能够结合补足数据和所提取的数据以获得并使用所述要求的信息。

[0029] 所考虑的应用系统 AS_k 可以进一步将补足数据存储在其数据库中并用索引 ID 来定位它。因此，下一次所考虑的应用系统 AS_k 将能够获得信息而不要求给定应用系统 AS_j 向它转发补足数据。

[0030] 所以，几个分布式应用系统能够交换数据，以便使所考虑的应用能够获得所要求的信息，尽管直到此时从未向这个所考虑的应用提供信息。

[0031] 所以，本发明提供了安全的方法，一旦在分布式环境的任何一个应用系统中已经输入了信息，所述方法消除了消费者重新输入信息的需要。

[0032] 另外，各种应用系统之间的数据交换对用户完全透明。

[0033] 根据本发明的第二种使用情况，使用数据与应用存储的数据一致并且是应用性数据。这些应用性数据意在由应用系统 $ASi_{i=1..n}$ 的至少某个应用使用。另外，所述应用性数据不要求高级别的安全性。所以，应用性数据能够被照此存储在给定应用 AS_j 的数据库中。例如，应用性数据可以关联到用户概况数据（用户忠诚度程序、用户偏爱、航班离港和 / 或到港、与所述航班相关联的服务请求、宾馆或轿车租赁信息、消费者概况数据等）。

[0034] 在任何所考虑的应用系统 AS_k 检索所述应用性数据都包括以下步骤。所述所考虑的应用系统 AS_k 接收敏感信息。它从所述信息产生所提取的数据和所编码的信息。所考虑的应用系统 AS_k 向服务器系统 (SS) 发送所提取的数据和所编码的信息。

[0035] 然后，服务器系统 (SS) 从服务器系统的数据库 DB_{SS} 检索由提取的数据和编码的信息二者形成的配对所对应的索引 ID。它向所述所考虑的应用系统 AS_k 转发索引 ID。

[0036] 所考虑的应用系统 AS_k 接收索引 ID 并检索用索引 ID 来定位的应用性数据。因此，所考虑的应用系统 AS_k 的应用能够使用应用性数据。

[0037] 如同对于所述第一种使用情况，在这第二种使用情况下，所述信用卡被窃的风险显著降低了，因为所考虑的应用系统 AS_k 和服务器系统都不保存完整信息。另外，在任何应用系统 $ASi_{i=1..n}$ 与服务器系统 SS 之间的单次传输中也从未传送完整信息。

[0038] 根据这第二种使用情况的第一个事件，所考虑的应用系统 AS_k 是给定应用系统 AS_j。因此，从与给定应用系统 AS_j 相关联的数据库 DB_{ASj} 检索所述应用性数据。

[0039] 因此，一旦在任何应用系统输入了信息，便能够快速检索应用性数据。这允许所述应用的容易和用户友好的使用。

[0040] 另外，信息的所述检索是高度安全的。给定应用系统 AS_j 的数据库确实甚至不必包括补足数据、提取的数据或信息中任何一种。服务器系统 SS 的数据库不包括补足数据或信息。仅仅向服务器系统发送所编码的信息和所提取的数据。

[0041] 因此，补足和提取的数据从不存储在同一数据库中，并且信息仅仅在产生所提取的数据和所编码的信息时才在应用的处理存储器中可用。所以，搜寻所述网络、窃取或黑客攻击任何数据库证实为无价值。

[0042] 根据这第二种使用情况的第二个事件，所考虑的应用系统 AS_k 是与给定应用系统 AS_j 不同的应用系统。所述应用 AS_k 在其相关联的数据库 DB_{ASk} 中不包括用索引 ID 定位的所述应用性数据。因此，检索应用性数据包括以下指示的步骤。从服务器系统收到索引 ID 后，所考虑的应用系统 AS_k 向给定应用系统 AS_j 发送所述索引 ID。然后给定应用系统 AS_j 接收索引 ID 并根据索引 ID 从其数据库 DB_{ASj} 检索所述应用性数据。最后，给定应用系统 AS_j 向所述所考虑的应用系统 AS_k 发送所述应用性数据。

[0043] 这第二种使用情况的第二个事件强调了以下事实：即使在所考虑的应用系统 AS_k 不存储所要求的应用性数据的情况下，也能够向这个所考虑的应用 AS_k 提供这份应用性数据，同时对敏感信息保持高级别的安全性。确实，这种敏感信息从未存储也未在任何应用系统之间的单次传输或者任何应用系统与服务器系统之间的单次传输中传送。

[0044] 在优选实施例中产生补足数据和提取的数据的步骤包括把信息划分为第一部分和第二部分。

[0045] 本发明对于信息为信用卡号的方法尤为便利。那么，补足数据能够对应于所述信用卡号的明显位而所提取的数据能够对应于所述信用卡号的隐藏位。

[0046] 产生信息的编码版本的步骤可以包括通过散列函数计算信息的散列值。在优选实施例中，服务器系统 (SS) 不知所述散列函数。所以，本发明允许显著限制某人可能通过访问信息的所述编码版本而获得敏感信息的风险。

[0047] 本发明也提供了一种系统，用于存储和检索与在分布式环境中要求保证其安全性的信息相关联的使用数据，所述环境包括能够使用所述信息和所述使用数据的多个应用系统 $ASi_{i=1..n}$。本发明的系统包括服务器系统 SS，以及多个应用系统 $ASi_{i=1..n}$ 之中的给定应用系统 AS_j。给定应用系统 AS_j 被安排为：

[0048] - 接收信息，

[0049] - 从所述信息产生提取的数据和补足数据，使得独立取得的所述所提取的数据和所述补足数据不足以由任何应用系统 $ASi_{i=1..n}$ 使用所述信息 CC#，以及使得从一起取得的所述所提取的和补足数据能够产生和使用所述信息，

[0050] - 从所述信息产生编码的信息，

[0051] - 向服务器系统 SS 发送所提取的数据和所编码的信息。

[0052] 服务器系统 SS 被安排为：

[0053] - 产生索引 ID 并向所编码的信息和所提取的数据分配这个索引 ID，

[0054] - 在与服务器系统 SS 相关联的数据库 DB_{SS} 中存储所编码的信息、所提取的数据和索引 ID，

[0055] - 向多个应用系统 $ASi_{i=1..n}$ 的所述给定应用系统 AS_j 转发索引 ID，给定应用系统 AS_j 也被安排为：

[0056] - 向与信息有关的应用存储的数据分配索引 ID，

[0057] - 在与所述给定应用系统 AS_j 相关联的数据库 DB_{ASj} 中与所述应用存储的数据一起存储索引 ID。

[0058] 更一般地说，根据本发明的系统包括被安排为实行以上介绍的方法的服务器系统和应用系统 ASi。

[0059] 操作敏感信息的应用系统包括处理存储器并且被安排为信息仅仅在所述处理存储器中可用。

[0060] 一旦应用系统已经使用了信息，它便删除所述信息。所以，敏感信息在使用后不再可访问。这限制了被窃的风险。

[0061] 在优选实施例中，所述系统至少包括应用系统 (ASi) 的处理装置中的高速缓存机构。所述高速缓存机构被安排为在所述信息的处理期间存储信息。每项处理有一个高速缓存实例。

[0062] 在本发明的优选实施例中，系统包括代理组件，它是安全存储系统的一部分并且它包含在应用系统中。所述代理组件的作用是操作试图在宿主所述代理组件的应用系统处发生的以下步骤中的至少一个。

[0063] - 从信息产生补足数据和所提取的数据，

[0064] - 从所述信息产生所编码的信息，

[0065] - 向服务器系统 SS 发送所提取的数据和所编码的信息，

[0066] - 发送与宿主所述代理组件的应用系统相关联的数据库中的补足数据，

[0067] - 产生若干消息，包括要从宿主代理组件的应用系统发送的数据，所述消息采用似 EDIFACT 格式，

[0068] - 读取若干消息，包括要在宿主代理组件的应用系统接收的数据，所述消息采用似 EDIFACT 格式。

[0069] 典型情况下，所述代理组件可以是中间件库。它提供各种 API（应用程序编程接口），连接应用系统的应用和服务器系统。所述代理组件也可以包括高速缓存机构。

[0070] 通过应对信息处理和数据交换，所述代理组件显著地便利了本发明的系统中任何应用的集成。

[0071] 在本发明系统的另一个实施例中，应用系统不包括代理组件并且由它自己应对全

部所要求的动作。因此，这样的应用系统能够例如格式化 / 从服务器系统读取消息、计算信息的所编码的版本等。

[0072] 在本发明的具体实施例中，该方法包括在任何所考虑的应用系统 AS_k 的以下步骤。所考虑的应用系统 AS_k 产生包括几个索引 ID 的请求消息。然后，它向服务器系统发送所述请求消息。另外，服务器系统搜索其数据库并且检索与所述请求消息中包括的索引 ID 相关联的每个提取的数据。然后服务器系统发送包含所检索的提取的数据的响应消息。

[0073] 然后，所考虑的应用系统 AS_k 从服务器系统 SS 接收所述响应消息。最后，所考虑的应用系统 AS_k 能够重建全部信息，对于该信息，已经从服务器系统收到所提取的数据。

[0074] 因此，利用一个单次交易，应用系统能够向服务器系统发送索引的列表，以便接收索引的列表对应的全部所提取的数据。

[0075] 这样的批量处理也能够用于检索应用性数据。确实，所考虑的应用系统能够向服务器系统 SS 发送包含提取的数据和敏感信息的编码版本的列表的请求消息。服务器系统从其数据库检索被分配给所述请求消息中包括的提取的数据和编码的版本对的每个索引。然后它向所述所考虑的应用系统发送包含已经检索出的索引的响应消息。因此，所考虑的应用系统能够检索以所述响应消息的索引所定位的应用性数据。

[0076] 所以，这样的批量处理允许实质上简化和加速许多用户的信息检索。所以，本发明提供的方法增强了向应用的用户提供的服务。这样的批量处理在新应用转移到本发明的存储系统时尤为有用。在进行转移时，大量的数据确实不得不快速而容易地存储。

[0077] 根据上述实施例，为了检索所述索引把提取的数据和编码的信息都发送到服务器系统。发送提取的数据和编码的信息这两者允许显著降低检索错误索引的风险。

[0078] 根据替代实施例，仅仅向服务器系统发送所编码的信息，以便在应用系统接收所述索引。尽管以这个实施例得到错误索引的风险高于提取的数据和编码的信息都在所述请求中时，但是所述风险保持非常低。处理大量数据时，这样的替代实施例尤为有用。它确实避免了操作和向服务器系统发送繁重的提取的数据。

[0079] 信息能够由数字、字母、符号或这三者的组合组成。正如本发明所指出，信息不限于数字。提取的数据和补足数据也能够包括数字、字母、符号或这三者的组合。应用性数据可以包括任何性质的数据和种类的文件比如数字、字母、符号、图片、视频等。

[0080] 所述系统也可以包括附加安全装置。这些安全装置被安排为强化所述多种应用系统之间以及应用系统与服务器系统之间交换的安全性。这些安全装置能够检查每条消息的发送者是否被实际授权。它们可以丢弃由非授权的发送者发送的消息。例如，访问服务器系统可以被限制为有限数目的授权的应用系统。

[0081] 实际上，安全装置执行系统的各种组件之间交换的消息的加密和解密。安全装置也可以包括在尝试反常操作时触发警告的装置。它们也能够包括监视和记录数据的交换、交易和处理的装置。

附图说明

[0082] 根据附图所展示的以下描述，本发明的其他特征、目的和优点将变得更加清楚地显而易见：

[0083] 图 1 是根据本发明包括系统若干主要组件的实例的高层次框图；

[0084] 图 2 是展示了存储敏感信息的使用情况的高层次框图；

[0085] 图 3 是展示了敏感信息检索的第一种使用情况的高层次框图；

[0086] 图 4 是展示了敏感信息检索的第二种使用情况的高层次框图；

[0087] 图 5 是展示了应用性数据检索的第一种使用情况的高层次框图；

[0088] 图 6 是展示了应用性数据检索的第二种使用情况的高层次框图。

具体实施方式

[0089] 本发明的以下详细说明参考了若干附图。虽然本说明包括了若干示范实施例，但是其他实施例也是可能的，并且可以对所介绍的实施例进行改变而不脱离本发明的实质和范围。

[0090] 图 1 展示了根据本发明用于存储和检索信息的系统。

[0091] 本系统包括 n 个应用系统，被称为 AS_1、AS_2、...、AS_i、...、AS_n。每个应用系统都与数据库 DB_{AS1}、DB_{AS2}、...、DB_{ASi}、...、DB_{ASn} 相关联。这些应用系统都包括试图使用敏感信息的若干应用。由几个合作的公司组成的组织或者由像 GDS 的组织运行它们。为了提升向用户提供的若干服务的效率，该组织努力消除每次进行交易时用户重新输入同一数据的需要。

[0092] 这也降低了当用户操作或输入所述敏感信息时敏感信息丢失或被盗的风险。

[0093] 本系统还包括安全的存储系统，由服务器系统 SS 和与这个服务器系统 SS 相关联的数据库 DB_{SS} 组成。

[0094] 本系统还包括通信网络，比如将每个应用系统 AS_i 与服务器系统 SS 互连的因特网。通信网络也允许若干应用系统 AS_i 一起在分布式环境中交换信息。有利地，本系统的多个组件远程布置。

[0095] 信息存储系统的若干组件所执行的处理提供了对敏感或有价值信息进行安全的存储和检索。

[0096] 以下将通过展示性的使用情况详细说明对敏感信息的安全存储和检索。在这些使用情况下，敏感信息是信用卡号 CC#。通常信用卡号由 16 位数字组成。

[0097] 图 2 展示了本发明如何允许存储敏感信息。

[0098] 在步骤 21，多个应用系统 $ASi_{i=1..n}$ 中的应用系统 AS_j 接收信用卡号 CC#。典型情况下，在用户已经通过常规的接口比如键盘输入了这个信用卡号之后就会收到它。这个信用卡号必须容易地可用于后来的阶段的使用而不需要用户重新输入。所以，不得不存储这个信用卡号。处理信用卡号存储的应用系统 AS_j 在下文中被指派为第一应用系统 AS_j。

[0099] 第一应用系统 AS_j 将信用卡号 CC# 分为第一部分和第二部分。在这个展示性实例中，第一部分对应于信用卡号的前六位数字和后四位数字。这个第一部分在应用 AS_j 处将保持可用。第二部分对应于剩余的六位数字。这个第二部分在应用 AS_j 处将不保持可用。在下文中，第一和第二部分分别被指派为明显位 A(CC#) 和隐藏位 C(CC#)。

[0100] 明显位 A(CC#) 和隐藏位 C(CC#) 以这样的方式产生：

[0101] - 独立地取得它们时，任何应用系统 $ASi_{i=1..n}$ 都不可能使用所述信用卡号 CC#，以及

[0102] - 一起取得它们时，便能够重建和使用所述信用卡号 CC#。

[0103] 第一应用系统 AS_j 还产生所述信用卡号 CC# 的编码的版本 H(CC#)。更确切地说，

第一应用系统 AS_j 计算信用卡号 CC# 的散列值。

[0104] 在步骤 22，第一应用系统 AS_j 向服务器系统 SS 发送隐藏位 C(CC#) 和编码的信用卡号 H(CC#)。

[0105] 服务器系统 SS 接收隐藏位 C(CC#) 和编码的信用卡号 H(CC#)。它产生索引 ID 并将这个索引 ID 分配给编码的信用卡号 H(CC#) 和隐藏位 C(CC#)。然后服务器系统 SS 将编码的信用卡号 H(CC#)、隐藏位 C(CC#) 和索引 ID 存储在与服务器系统 SS 相关联的数据库 DB_{SS} 中（步骤 23)。服务器系统 SS 一旦在其数据库 DB_{SS} 中已经检查到哪个索引 ID 可用，便产生索引 ID（步骤 24)。如果两元组 (H(CC#)、C(CC#)) 已经被服务器系统 SS 存储，那么就检索分配给这两元组 (H(CC#)、C(CC#)) 的索引 ID，并且将其返回到应用系统。因此，由服务器系统 SS 运行的检查不限于检查索引 ID 的可用性。

[0106] 在步骤 25，服务器系统 SS 进一步向多个应用系统 ($ASi_{i=1..n}$) 中的第一应用系统 AS_j 转发索引 ID。

[0107] 然后，第一应用系统 AS_j 将索引 ID 分配给明显位 A(CC#)。最后，第一应用系统 AS_j 将索引 ID 连同明显位 A(CC#) 一起存储在其数据库 DB_{ASj} 中（步骤 26)。

[0108] 因此，第一应用系统 AS_j 仅仅发送了隐藏位 C(CC#) 和编码的 H(CC#) 信用卡号。不存在完整信用卡号 CC# 的交换。此外，由于第一应用系统 AS_j 的数据库 DB_{ASj} 仅仅存储着明显位 A(CC#) 和 ID，并且由于服务器系统的数据库 DB_{SS} 仅仅存储了隐藏位 C(CC#)、编码的 H(CC#) 信用卡号和索引 ID，那么隐藏的 C(CC#) 和明显位 A(CC#) 绝不会存储在同一数据库中。所以，搜寻网络、窃取或黑客攻击第一应用系统 AS_j 的数据库或服务器系统的数据库 DB_{SS} 中的任何一个都不能够获得明显位 A(CC#) 和隐藏位 C(CC#) 二者，或者获得完整信用卡号 CC#。所以信用卡号 CC# 无法被重建和非法使用。

[0109] 此外，在服务器应用 AS_i 进行散列处理。因此，该功能对服务器系统 SS 保持未知。所以，本发明允许显著限制某人经由访问信用卡号 CC# 的编码的版本而获得信用卡号 CC# 的风险。

[0110] 不仅如此，因为由应用系统 AS_j 发送的数据没有存储在所述应用系统 AS_j 的数据库 DB_{ASj} 中，那么，所发送的数据就无法与所存储的数据一致。所以，为了得到信息（如信用卡号 CC#)，黑客攻击应用系统 AS_j 的数据库 DB_{ASj} 和搜寻由这个应用系统 AS_j 的所传送的消息都是没用的。

[0111] 由每个应用系统 AS_i 所产生的若干隐藏位 C(CC#) 全部一起存储在服务器系统的数据库 DB_{SS} 中。然而，这些隐藏的数字对重建完整信用卡号 CC# 是必不可少的。所以，为保证该敏感信息的安全性而分配的若干资源能够被集中在服务器系统 SS 及其专用数据库 DB_{SS} 上。本发明消除了在各种应用系统 $ASi_{i=1..n}$ 之间散布这些资源的需要。所以，为了预防任何种类的窃取，在服务器系统 SS 处及其相关联的数据库 DB_{SS} 处能够显著地增强安全性。在与应用系统相关联的各种应用系统 $ASi_{i=1..n}$ 和各种数据库 DB_{ASi} 都远程布置的分布式环境中，以及 / 或者在各种应用系统 $ASi_{i=1..n}$ 和各种数据库 DB_{ASi} 都远离服务器系统 SS 及其数据库 DB_{SS} 的分布式环境中，这个方面尤为有利。

[0112] 此外，索引 ID 由服务器系统 SS 产生而不是由任何应用系统 AS_j 产生。因此，索引 ID 被分配给了单一信用卡号 CC#。所以，对于同一信用卡号 CC# 不存在并发的索引 ID。为了交换与给定信用卡号 CC# 有关的数据，各种应用系统 $ASi_{i=1..n}$ 能够共享与所述信用卡号

CC# 相关联的唯一索引 ID。所以，本发明尤其便于在许多应用系统 $ASi_{i=1..n}$ 使用所述信用卡号 CC# 的分布式环境中存储所述信用卡号 CC#。

[0113] 例如，组织的各种应用系统可以共享数据，一旦在第一应用系统 AS_j 处已经输入了完整信用卡号 CC#，就消除了用户在任何应用系统 AS_k 处重新输入其信用卡号的需要。以下将参考图 4 详细说明这种使用情况。

[0114] 所以，本发明有助于增强向应用用户提供的若干服务的效率。

[0115] 以下参考图 3 和图 4 详细介绍了展示信用卡号 CC# 检索的使用情况。

[0116] 图 3 展示了第一应用系统 AS_j 或使明显位 A(CC#) 存储在其数据库 DB_{ASj} 中的任何应用系统需要检索信用卡号 CC# 的事件。

[0117] 为此，在步骤 31 第一应用系统 AS_j 从其数据库接收索引 ID。然后，在步骤 32 它向服务器系统 SS 发送索引 ID。服务器系统 SS 从其数据库 DB_{SS} 检索用索引 ID 定位的隐藏位 C(CC#)（步骤 33 和步骤 34）。服务器系统 SS 进一步向第一应用系统 AS_j 发送隐藏位 C(CC#)（步骤 35）。

[0118] 第一应用系统 AS_j 从其数据库 DB_{ASj} 检索用索引 ID 定位的明显位 A(CC#)。最后，第一应用系统 AS_j 组合了明显位 A(CC#) 和从服务器系统 SS 收到的隐藏位 C(CC#)，以便重建信用卡号 CC#（步骤 36）。

[0119] 图 4 展示了第二事件，其中在先前尚未产生和存储用索引 ID 定位的明显信用卡号 A(CC#) 的任何应用系统 AS_k 处，需要检索信用卡号 CC#。所述任何应用系统 AS_k 所以不同于第一应用系统 AS_j，而且在下文中被指定为第二应用系统 AS_k。

[0120] 各种应用系统 $ASi_{i=1..n}$ 按照它们提供的服务种类而被分类。这些应用系统 $ASi_{i=1..n}$ 彼此知道并且能够识别它们各自需要的数据类型。当第一应用系统 AS_j 收到对其他应用系统有用的数据时，那么第一应用系统 AS_j 就将这个数据向所述其他应用系统发送。

[0121] 一旦有用数据在第一应用系统 AS_j 可用，所述数据的传输就可以自动地运行。

[0122] 例如，一旦由 AS_j 产生了明显位 A(CC#) 并且一旦在 AS_j 从服务器系统 SS 收到了索引 ID，那么 AS_j 就将明显位 A(CC#) 和索引 ID 这两者发送到被分类为需要明显位 A(CC#) 和索引 ID 的一切应用系统（步骤 41 和步骤 42）。

[0123] 然后被提供了所述有用数据的每个应用系统都能够使用它。例如，第二应用系统 AS_k 一旦从 AS_j 收到了明显位 A(CC#) 和索引 ID 二者（步骤 42）时，它就能够获得信用卡号 CC#。更确切地说，收到索引 ID 后，第二应用系统 AS_k 就向服务器系统 SS 发送这个索引 ID（步骤 43）。服务器系统 SS 从其数据库 DB_{SS} 检索用索引 ID 定位的隐藏位 C(CC#)（步骤 44 和步骤 45）。服务器系统 SS 进一步向第二应用系统 AS_k 发送隐藏位 C(CC#)（步骤 46）。然后，第二应用系统 AS_k 组合从第一应用系统 AS_j 收到的明显位 A(CC#) 和从服务器系统 SS 收到的隐藏位 C(CC#)，以便重建信用卡号 CC#（步骤 47）。最后，第二应用系统 AS_k 的应用能够使用信用卡号 CC#。

[0124] 优选情况下，第二应用系统 AS_k 在其数据库 DB_{ASk} 中存储用索引 ID 定位的明显信用卡号 A(CC#)（步骤 48）。因此，下次第二应用系统 AS_k 将能够获得信用卡号 CC#，而不需要第一应用系统 AS_j 转发明显位 A(CC#)。

[0125] 这个实施例暗示，明显位 A(CC#) 与索引 ID 被一起传输。在一切应用都由单一组织运行，并且其中多个应用系统之间的互动对用户完全透明的环境中这个实施例尤其有利。

尤其是最终用户（持卡者）不被假设为访问向其信用卡号 CC# 分配的索引 ID。

[0126] 正如图 3 和图 4 使用情况下的展示，绝对不会交换也不会存储完整的信用卡号 CC#。信用卡号 CC# 仅仅在所考虑的应用系统 AS_k 处理需要所述信用卡号 CC# 的过程时，才在所述考虑的应用系统 AS_k 上该信用卡号 CC# 的使用期间可用。典型情况下，信用卡号 CC# 被存储在处理存储器中而不在别处。一旦所述使用完成，信用卡号 CC# 就被除去。此外，明显位 A(CC#) 和隐藏的 C(CC#) 不存储在同一数据库中。所以，搜寻网络或窃取数据库的任何一个，都不能够获得信用卡号 CC#。

[0127] 图 3 和图 4 的使用情况还展示了几个分布式应用系统能够交换数据，以便使所考虑的应用系统 AS_k 能够获得所需要的信用卡号 CC#，尽管到目前为止还从未给这个给定的应用提供所述信用卡号 CC# 或者提供明显位 A(CC#)。所以，本发明提供了安全的方法，一旦在所述分布式环境的任何一个应用系统已经输入了信用卡号 CC#，所述方法消除了消费者重新输入所述信用卡号 CC# 的需要。另外，各种应用系统之间的数据交换对用户完全透明。

[0128] 以下参考图 5 和图 6 详细介绍了展示与信用卡号 CC# 有关的应用性数据检索的使用情况。这些应用性数据意在由至少某个应用系统使用。另外，所述应用性数据不要求高级别的安全性。所以，应用性数据能够被原样存储在给定应用的数据库中。例如，应用性数据可以与用户概况数据（用户忠诚度程序、用户偏爱、用户照片等）相关。

[0129] 在图 5 展示的事件中，需要使用应用性数据的应用系统已经将其存储并将其定位在其数据库中。这样的应用系统在以下第一应用系统 AS_j 中被指定。

[0130] 在步骤 51 第一应用系统 AS_j 接收信用卡号 CC#。然后，它从所述信用卡号 CC# 产生隐藏位 C(CC#) 和编码的信用卡号 H(CC#)。在步骤 52，它向服务器系统 SS 发送隐藏位 C(CC#) 和编码的信用卡号 H(CC#)。然后，服务器系统 SS 从其数据库 DB_{SS} 检索隐藏位 C(CC#) 和编码的信用卡号 H(CC#) 二者所对应的索引 ID（步骤 53 和步骤 54）。然后服务器系统 SS 向第一应用系统 AS_j 转发索引 ID（步骤 55）。收到索引 ID 后，第一应用系统 AS_j 便检索用索引 ID 定位的应用性数据（步骤 56 和步骤 57）。最后，第一应用系统 AS_j 的应用能够使用该应用性数据。

[0131] 在图 6 展示的事件中，需要使用应用性数据的应用系统的数据库没有将所述应用性数据存储或定位在其数据库中。这样的应用系统在以下第二应用系统 AS_k 中被指定。

[0132] 在步骤 61 第二应用系统 AS_k 接收信用卡号 CC#。步骤 62、63、64、65 本质上与以上详细介绍的步骤 52、53、54、55 一致。在步骤 65 第二应用系统 AS_k 从服务器系统 SS 接收索引 ID。在已经检查了其数据库 DB_{ASk} 没有存储用所收到的索引定位的应用性数据之后，第二应用系统 AS_k 便向第一应用系统 AS_j 发送这个索引 ID（步骤 66）。第一应用系统 AS_j 搜索其数据库 DB_{ASj} 并检索用索引 ID 定位的应用性数据（步骤 67 和步骤 68）。然后第一应用系统 AS_j 向第二应用系统 AS_k 转发该应用性数据（步骤 69）。最后该应用性数据在第二应用系统 AS_k 的应用处可供使用。

[0133] 有利的情况中，第二应用系统 AS_k 在其数据库 DB_{ASk} 中存储用索引 ID 定位的应用性数据。

[0134] 因此，倘若已经在任何数据库中定位并存储了应用性数据，并且倘若信用卡号已经被输入了一次，就能够快速地检索到应用性数据。

[0135] 这允许容易地和用户友好地使用应用性数据，因此使得应用对用户更具有吸引

力。另外，各种应用系统之间的数据交换对用户完全透明。

[0136] 如同与信用卡检索有关的若干使用情况，在针对应用性数据检索的使用情况下，窃取信用卡的风险被显著降低，因为无论是应用系统 AS_j、AS_k 还是服务器系统 SS 都不保留完整的信用卡号 CC#。另外，在任何应用系统 $ASi_{i=1..n}$ 与服务器系统 SS 之间的单次传输或者在两个应用系统 AS_j、AS_k 之间的单次传输中都不曾传送完整的信用卡号 CC#。

[0137] 在优选实施例中，存储系统在应用系统至少包括处理和交易模块。正如在图 2 至图 6 的具体实施例的展示，该系统包括在每个应用系统的代理组件。根据另一个实施例，仅仅某些应用系统才可以关联到代理组件。该代理组件是安全存储系统的一部分。该代理操作以下步骤的至少某些步骤，这些步骤的用意是，在包括所述代理组件的应用系统中发生：

[0138] - 从信用卡号 CC# 产生明显位 A(CC#) 和隐藏位 C(CC#)，

[0139] - 从所述信用卡号 CC# 中产生编码的 H(CC#) 信用卡号，

[0140] - 向服务器系统 SS 发送隐藏位 C(CC#) 和编码的信用卡号 H(CC#)，

[0141] - 向服务器系统 SS 发送索引 ID 以进行进一步的信用卡号 CC# 检索，

[0142] - 向与应用系统相关联的数据库中发送明显位 A(CC#)，

[0143] - 从与应用系统相关联的数据库中检索明显位 A(CC#)，

[0144] - 产生若干消息，内含要从应用系统向服务器系统或向其他应用系统发送的数据，所述消息采用似 EDIFACT 格式，

[0145] - 读取从服务器系统或从其他应用系统收到的消息，所述消息是似 EDIFACT 格式。

[0146] 典型情况下，代理组件可以是中间件库。它提供了多种 API（应用程序编程接口），使应用系统的应用软件与服务器系统连接。代理组件还能够包括高速缓存机构。该高速缓存机构被安排在所述信用卡号 CC# 的处理期间存储信用卡号 CC#。每次处理时存在着一个高速缓存实例，以使得一旦该信用卡号 CC# 已经被应用系统的应用使用它就不再可用。

[0147] 通过操作信用卡号 CC# 的处理和数据交换，该代理组件显著方便了本发明的系统中任何应用的集成。

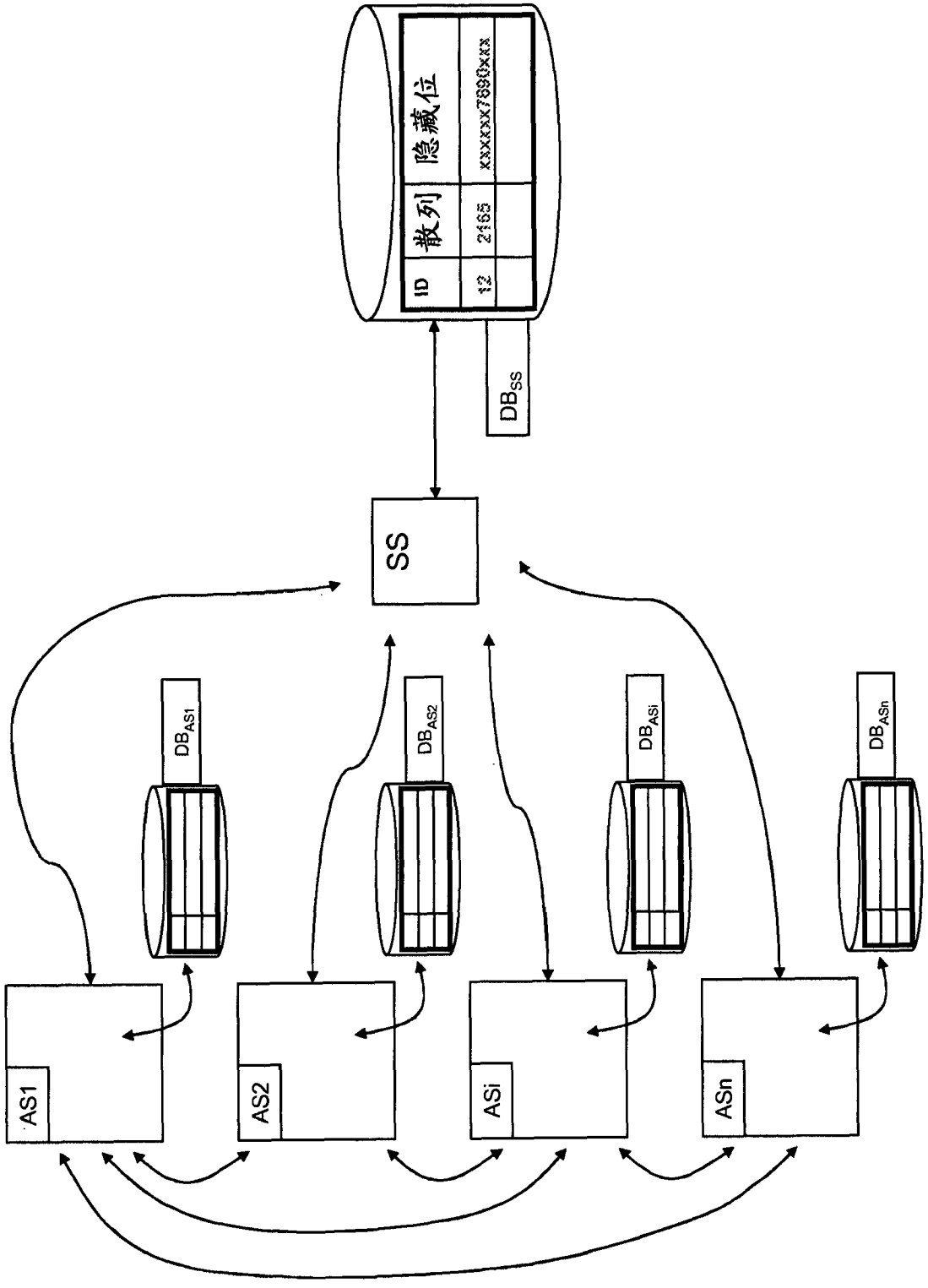

ID
散列
隐藏位
12
2165
xxxxxx7890xxx
DBSS
SS
DBAS1
DBAS2
DBASi
DBASn
AS1
AS2
ASi
ASn

图 1

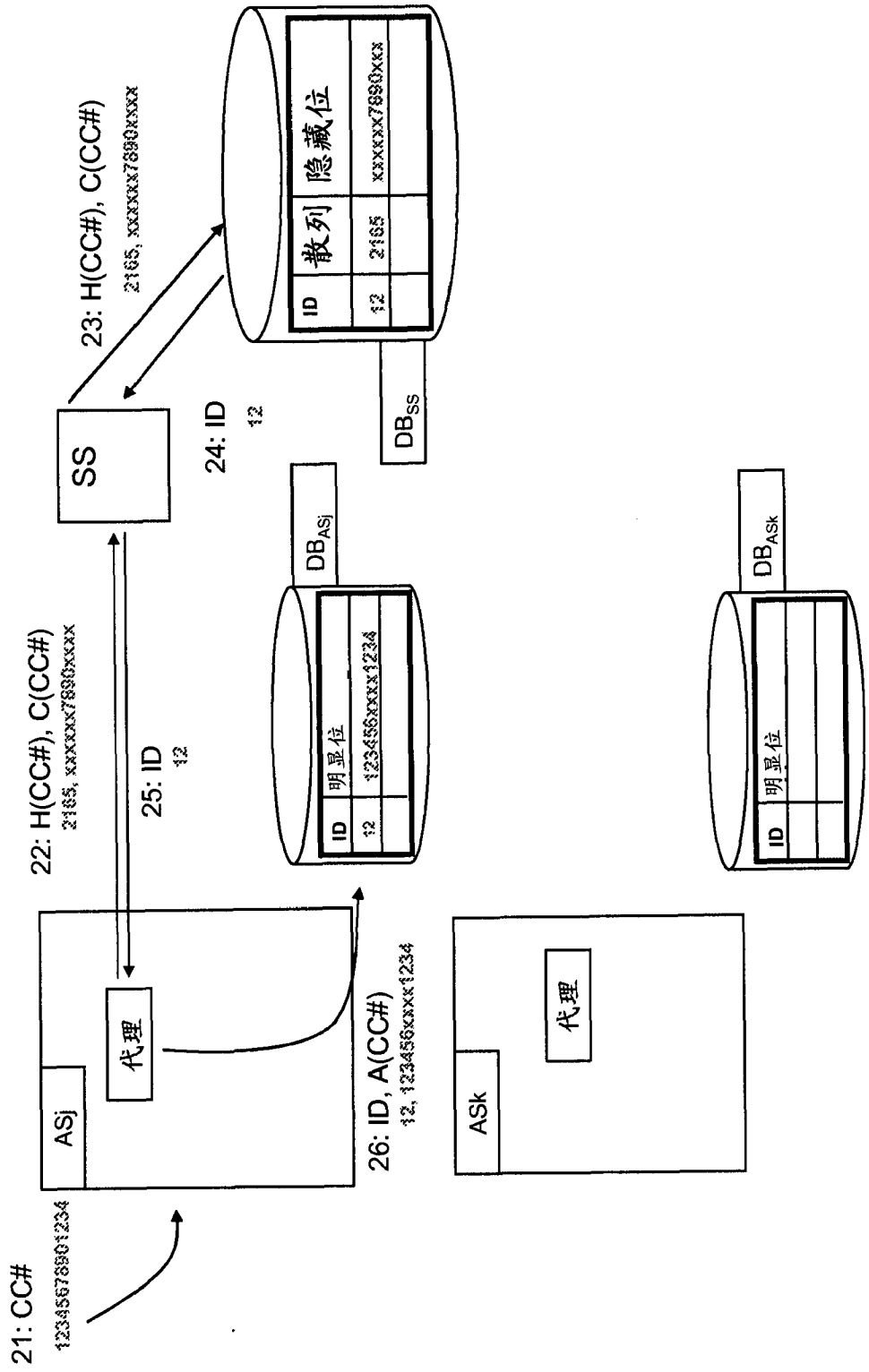

21: CC#
1234567890123 4
ASj
代理
22: H(CC#), C(CC#)
2165, xxxxxx7890xxxx
23: H(CC#), C(CC#)
2165, xxxxxx7890xxxx
SS
24: ID
12
25: ID
12
26: ID, A(CC#)
12, 123456xxxx1234
DBSS
ID
12
散列
2165
隐藏位
xxxxxx7890xxxx
DBASj
ID
12
明显位
123456xxxx1234
DBASk
ID
明显位
ASk
代理

图 2

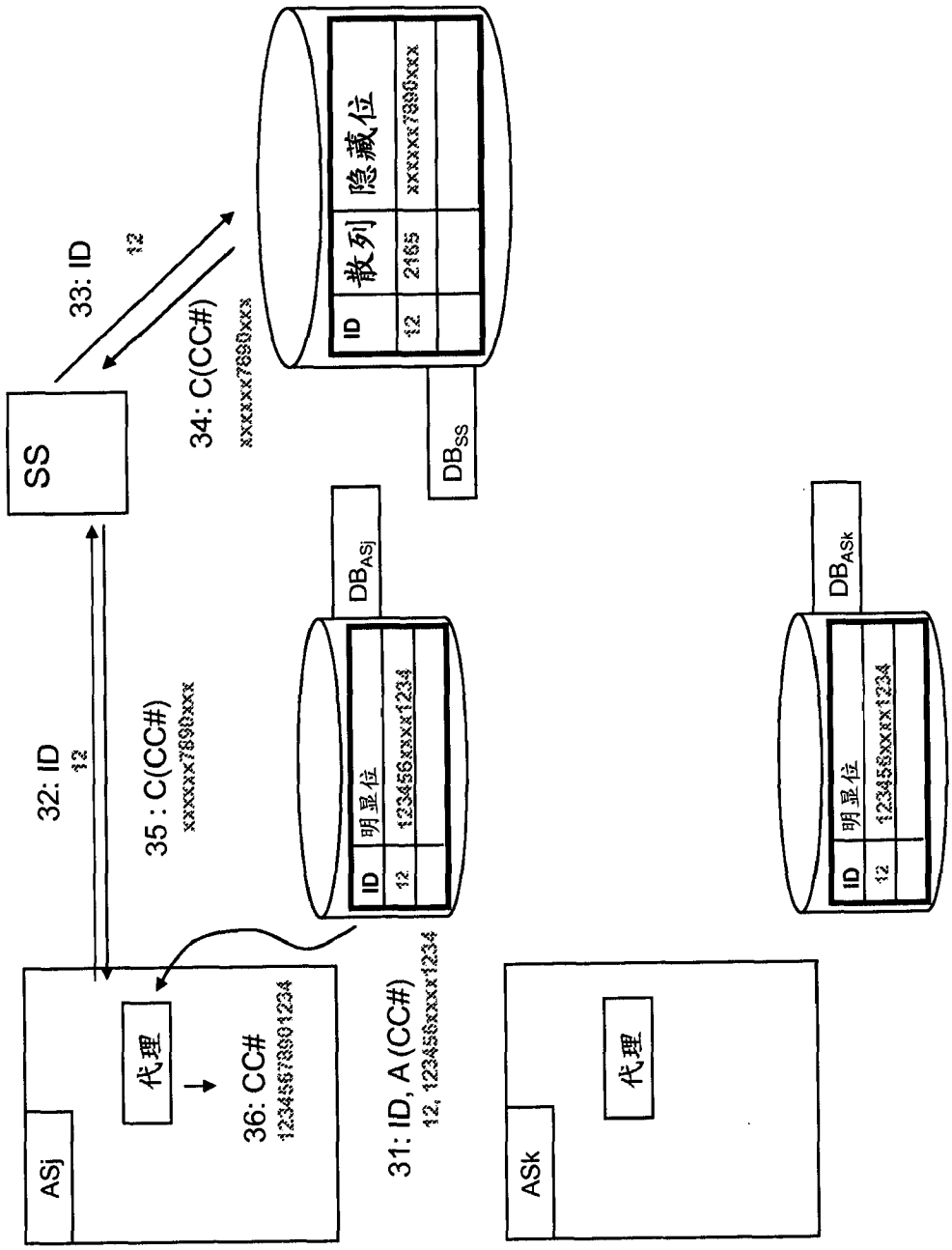

SS
33: ID
12
34: C(CC#)
xxxxxx7890xxx
32: ID
12
35 : C(CC#)
xxxxxx7890xxx
ASj
代理
36: CC#
1234567890 1234
31: ID, A (CC#)
12, 123456xxxx1234
ASk
代理
ID
散列
隐藏位
12
2165
xxxxxx7890xxx
DBSS
ID
明显位
12
123456xxxx1234
DBASj
ID
明显位
12
123456xxxx1234
DBASk

图 3

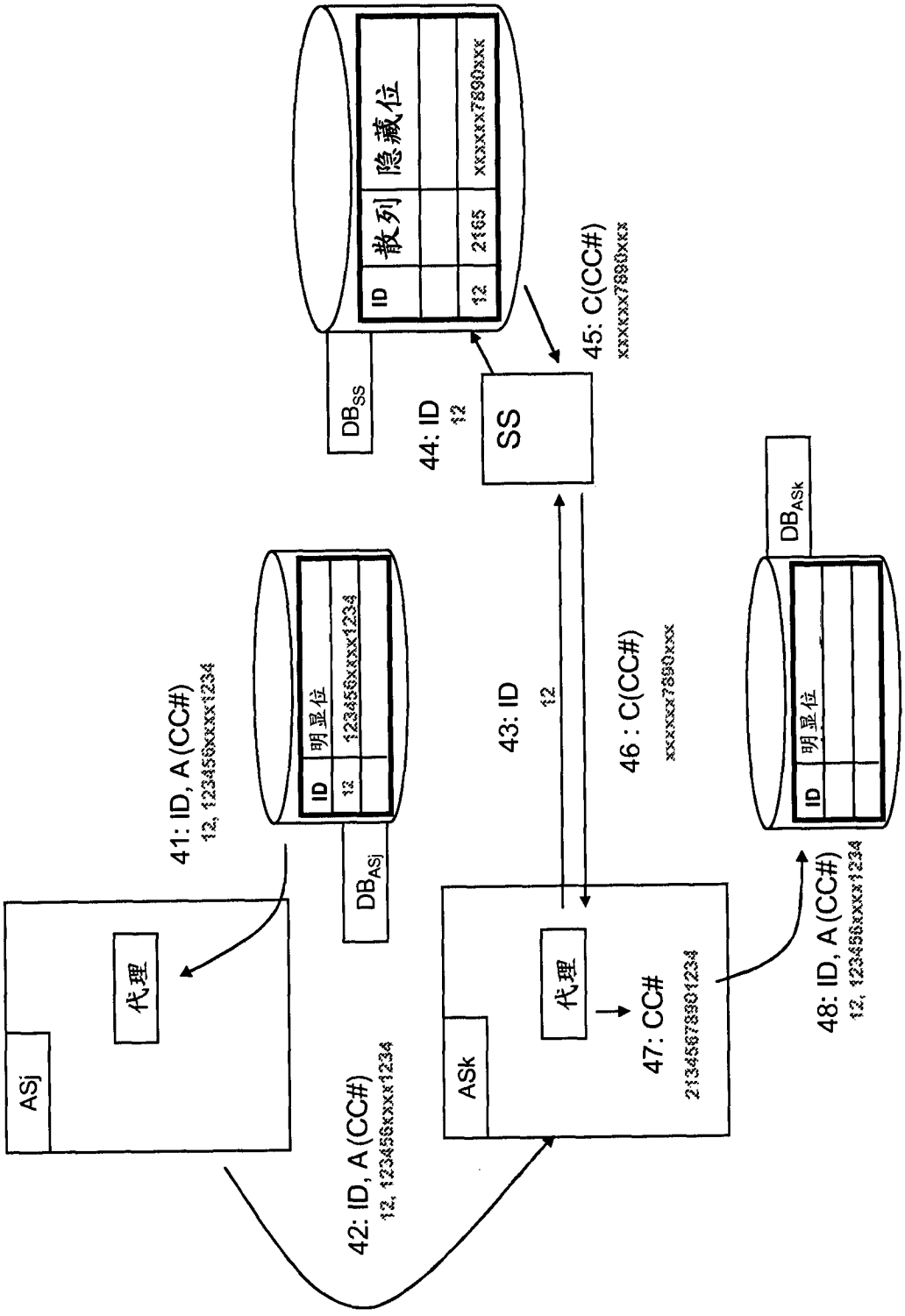

ID
散列
隐藏位
12
2165
xxxxxx7890xxx
DBSS
44: ID
12
SS
45: C(CC#)
xxxxxx7890xxx
DBASj
ID
明显位
12
123456xxxx1234
41: ID, A(CC#)
12, 123456xxxx1234
43: ID
12
46 : C(CC#)
xxxxxx7890xxx
DBASk
ID
明显位
ASj
代理
ASk
代理
47: CC#
2134567890 1234
48: ID, A(CC#)
12, 123456xxxx1234
42: ID, A(CC#)
12, 123456xxxx1234

图 4

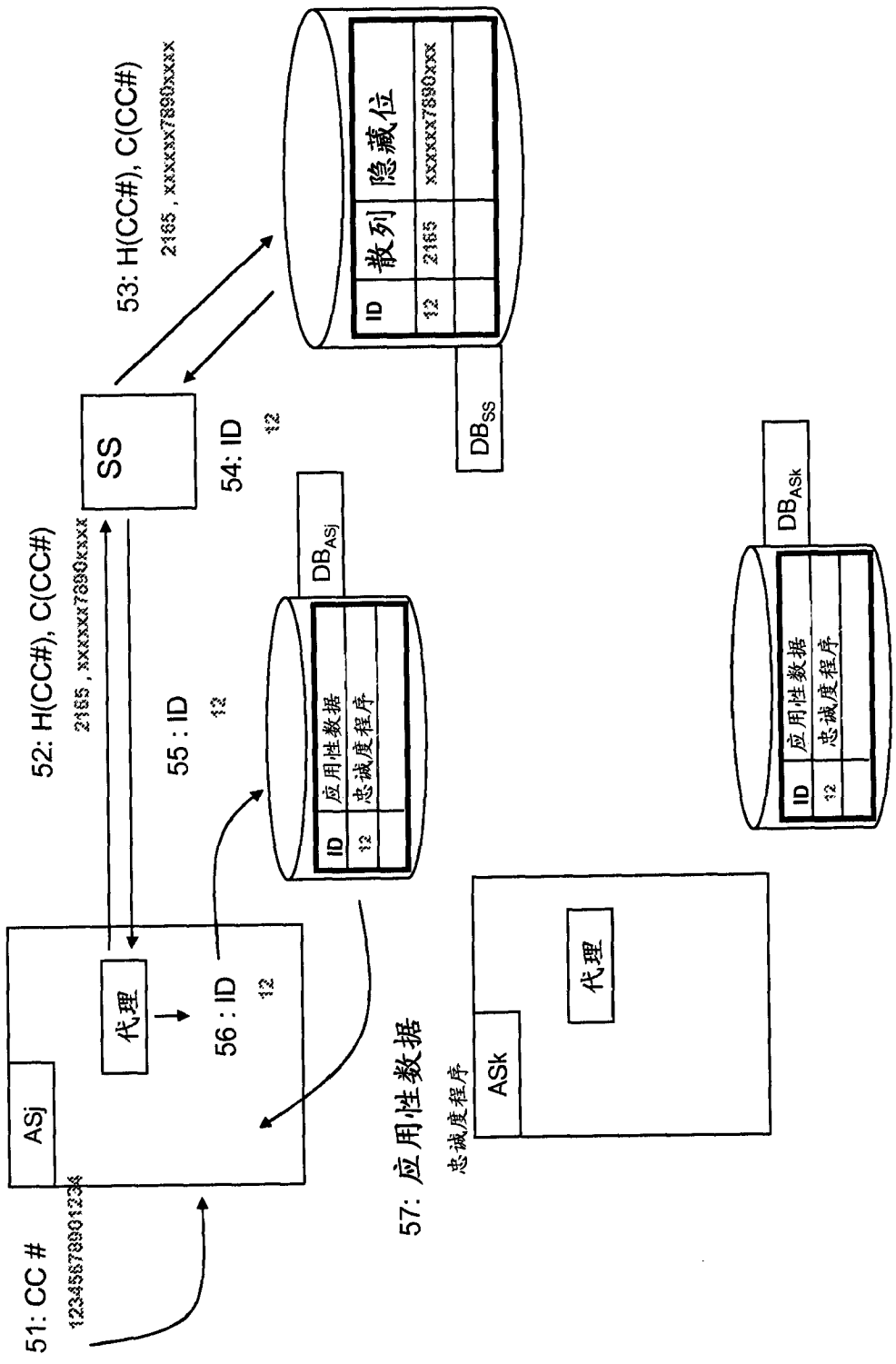

51: CC #
1234567890123456
ASj
代理
52: H(CC#), C(CC#)
2165 , xxxxxx7890xxxx
53: H(CC#), C(CC#)
2165 , xxxxxx7890xxxx
SS
54: ID
12
55 : ID
12
56 : ID
12
DBSS
ID
散列
隐藏位
12
2165
xxxxxx7890xxxx
DBASj
ID
应用性数据
忠诚度程序
12
57: 应用性数据
忠诚度程序
ASk
代理
DBASk
ID
应用性数据
忠诚度程序
12

图 5

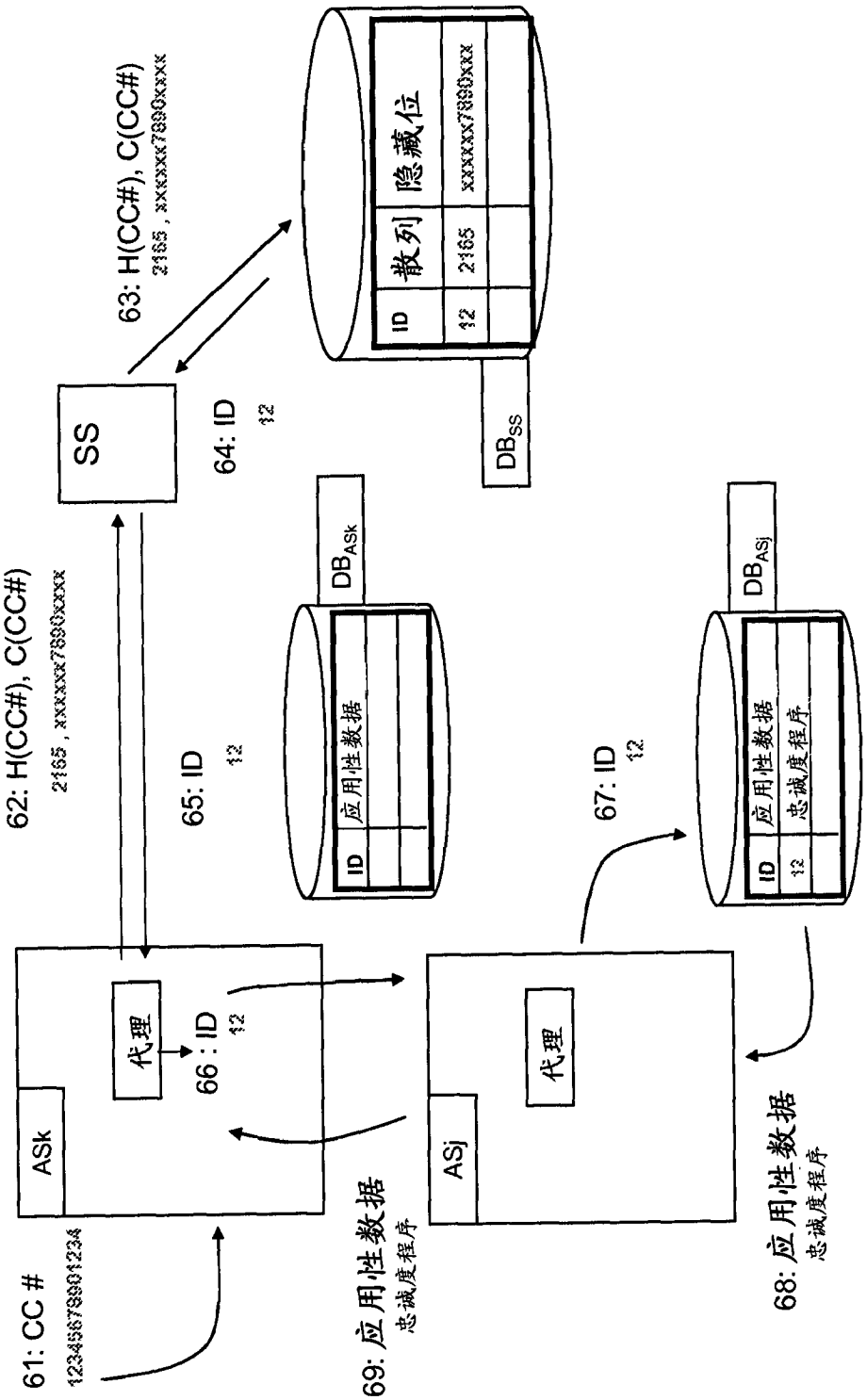

63: H(CC#), C(CC#)
2165 , xxxxxx7890xxxx
SS
64: ID
12
ID
散列
隐藏位
12
2165
xxxxxx7890xxxx
DBSS
62: H(CC#), C(CC#)
2165 , xxxxxx7890xxxx
65: ID
12
DBASk
ID
应用性数据
67: ID
12
DBASj
ID
应用性数据
忠诚度程序
12
ASk
代理
66 : ID
12
ASj
代理
61: CC #
1234567890123
69: 应用性数据
忠诚度程序
68: 应用性数据
忠诚度程序

图 6