(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 103823830 A
(43)申请公布日 2014.05.28

(21)申请号 201310574907.4

(22)申请日 2013.11.15

(30)优先权数据
13/678,077 2012.11.15 US

(71)申请人 国际商业机器公司
地址 美国纽约

(72)发明人 T·谢罗尔 I·M·密尔曼
M·奥伯霍菲尔 D·A·派荻拉

(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 金晓

(51)Int.Cl.
G06F 17/30(2006.01)
G06F 21/62(2013.01)

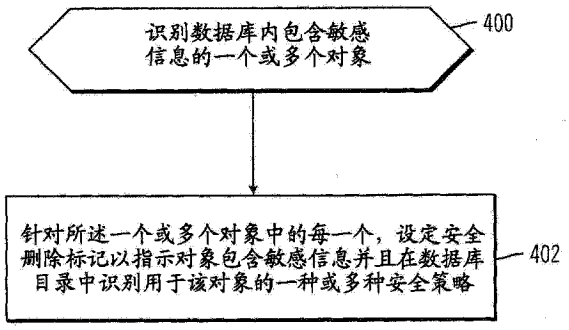
权利要求书2页 说明书14页 附图11页

(54)发明名称

用于销毁敏感信息的方法和系统

(57)摘要

提供了用于删除数据库内敏感信息的技术。识别数据库内通过语句访问的一个或多个对象。通过检查用于至少一个对象的标记而在识别的一个或多个对象中确定包含敏感信息的至少一个对象。识别与至少一个对象相关联的一种或多种安全策略。针对至少一个对象实施识别的一种或多种安全策略以删除敏感信息。



CN 103823830 A

1. 一种方法，包括：

识别数据库内通过语句访问的一个或多个对象；

通过检查用于至少一个对象的标记而确定在识别的一个或多个对象中的至少一个对象包含敏感信息；

识别与所述至少一个对象相关联的一种或多种安全策略；以及

针对所述至少一个对象实施所识别的一种或多种安全策略以删除敏感信息。

2. 如权利要求 1 所述的方法，其中所述语句包括指示针对通过所述语句访问的至少一个对象要执行安全删除并且识别了安全删除的级别的子句，并且其中所述级别用于识别明确安全删除过程细节的所述一种或多种安全策略。

3. 如权利要求 1 所述的方法，其中数据库目录存储所述标记以及指向用于所述至少一个对象的一种或多种安全策略的指针。

4. 如权利要求 1 所述的方法，进一步包括：

响应于在数据库内存储所述至少一个对象，

设定所述标记以指示所述对象包含敏感信息，其中所述标记在数据库目录内；并且

在删除该至少一个对象时存储要实施的所述一种或多种安全策略的位置。

5. 如权利要求 4 所述的方法，其中每一种安全策略都提供了默认的安全选择以及安全删除选择的可允许范围。

6. 如权利要求 1 所述的方法，其中所述对象包括表空间、表和索引中的一种。

7. 如权利要求 1 所述的方法，其中提供软件作为云环境中的服务。

8. 一种计算机系统，包括：

处理器；以及

连接至所述处理器的存储设备，其中所述存储设备在其中存储有程序，并且其中所述处理器配置为执行所述程序的指令以进行操作，其中所述操作包括：

识别数据库内通过语句访问的一个或多个对象；

通过检查用于至少一个对象的标记而确定在识别的一个或多个对象中的至少一个对象包含敏感信息；

识别与该至少一个对象相关联的一种或多种安全策略；以及

针对该至少一个对象实施识别的一种或多种安全策略以删除敏感信息。

9. 如权利要求 8 所述的计算机系统，其中所述语句包括指示针对通过所述语句访问的至少一个对象要执行安全删除并且识别了安全删除的级别的子句，并且其中所述级别用于识别明确安全删除过程细节的所述一种或多种安全策略。

10. 如权利要求 8 所述的计算机系统，其中数据库目录存储所述标记以及指向用于所述至少一个对象的一种或多种安全策略的指针。

11. 如权利要求 8 所述的计算机系统，进一步包括：

响应于在数据库内存储所述至少一个对象，

设定所述标记以指示所述对象包含敏感信息，其中所述标记在数据库目录内；并且

在删除该至少一个对象时存储要实施的所述一种或多种安全策略的位置。

12. 如权利要求 11 所述的计算机系统，其中每一种安全策略都提供了默认的安全选择以及安全删除选择的可允许范围。

13. 如权利要求 8 所述的计算机系统，其中所述对象包括表空间、表和索引中的一种。

14. 如权利要求 8 所述的计算机系统，其中软件即服务 SaaS 被提供以执行系统操作。

用于销毁敏感信息的方法和系统

技术领域

[0001] 本发明的实施例涉及确保销毁例如数据库系统内的敏感信息。

背景技术

[0002] 如今，在很多的商用软件系统例如分层、纵列和关系数据库系统以及分布式 / 大数据处理基础设施内都存有个人身份信息 (PII)。常规的系统可以通过例如访问利用验证和授权的限制来保护 PII。

[0003] 另外，常规的系统可以通过例如加密来保护PII。这样的加密包括在待机(备份等)时的数据加密和在传输时的数据加密（例如通过加密通信信道（譬如安全套接层 (SSL)、通过加密传送数据（消息加密）、通过加密通信信道和传送数据的组合以及通过审计跟踪）。

[0004] 某些常规的系统检测数据库内的 PII。但是，PII 仅是敏感信息的一个示例，并且还有其他类型的敏感信息（例如工资信息、性能评估、机密的产品计划等）。

[0005] 在常规的数据库系统内，敏感信息（例如PII）一旦不再需要就应该被销毁。但是，某些常规系统无法完全销毁此类敏感信息。例如，如果包含敏感信息的表在数据库内被弃用，但是并未采取措施来重写硬盘内存储该表的适当区域，那么这就会在硬盘内留下易于通过硬盘检测工具获取的敏感信息。

[0006] 单节点数据库系统可以表述为安装在服务器上的具有 4 个表空间的数据库，其中表空间 TS1 包含表 T1、T2 和 T3，其中表空间 TS2 包含表 T4、T5 和 T6，其中表空间 TS3 包含表 T7、T8 和 T9，以及其中表空间 TS4 包含表 T10 和 T11。作为用于数据库的存储器，设有两个存储系统，每一个都包含六块硬盘，在这两个存储系统内 :其中八块硬盘拥有通过操作系统管理的文件系统并且四块硬盘用作裸设备 (raw device)，这就意味着在这四块硬盘上没有通过操作系统管理的文件系统。

[0007] 参照单节点数据库系统，假设已经利用四个裸设备通过以下的语句 1(Statement1) 创建了表空间 TS4 :

[0008] Statement1

[0009] CREATE TABLESPACE T4

[0010] MANAGED BY DATABASE

[0011] USING(DEVICE′ /dev/rhdisk0′ 10000,

[0012] DEVICE′ /dev/rhdisk1′ 10000,

[0013] DEVICE′ /dev/rhdisk2′ 10000,

[0014] DEVICE′ /dev/rhdisk3′ 10000)

[0015] 通过 Statement1 在表空间 TS4 内创建了表 T10 和表 T11。假设表 T10 包含敏感信息（例如 PII）并且被弃用。在此情况下，采用文件系统以供删除 PII 的常规技术无法用于确保安全地删除四个裸设备中曾包含敏感信息的部分（例如通过将敏感信息若干次地重写为零等）以使得不能用磁盘检测工具来恢复所述信息。这是因为操作系统和文件系统无法影响由数据库管理的用作裸设备的硬盘。

[0016] 继续介绍单节点数据库系统的示例，假设已经通过以下的语句 2(Statement2) 建立了表空间 TS1 ：

[0017] Statement2

[0018] CREATE TABLESPACE T1

[0019] MANAGED BY DATABASE USING(FILE ' C.\db2\file1 ' 1M,FILE ' D:\db2\file2' 1M)

[0020] AUTORESIZE YES

[0021] INCREASESIZE2M

[0022] MAXSIZE100M

[0023] 在此情况下，表空间 TS1 使用初始容量为 1 兆字节 (MB)、增长速率为 2 兆字节且最大容量为 100 兆字节的两个文件容器。文件容器可以描述为文件系统内的文件。这就意味着表空间 TS1 内的表 T1、T2 和 T3 能够共同分配到 200MB 的最大容量 (2 个文件容器，每一个都有 100 兆字节的最大容量)。现假设 T2 是包含敏感信息的表并且 T2 已被弃用。与使用语句 1 的情况有所不同，目前在操作系统和数据库之间存在文件系统层。但是，只有数据库才知道两个文件容器文件 1 和文件 2 中有哪些部分被数据库使用并且因此需要清理 (例如通过将适当的部分重写为零等) 以确保无法恢复敏感信息。所以采用文件系统以供检测 PII 的公知技术无法用于确保安全地删除包含敏感信息的部分。

[0024] 多节点数据库系统包括多个节点。节点可以描述为独立的计算设备例如服务器系统。对于本示例，数据库通过多个节点分区。作为用于数据库的存储器，设有通过网络附加存储 (NAS) 访问的三个存储系统，每一个存储系统都包含六块硬盘，在两个存储系统内 :六块硬盘拥有通过操作系统管理的文件系统，六块硬盘用作裸设备并且没有通过操作系统管理的文件系统，以及四块硬盘拥有加密文件系统 (EFS)。

[0025] 表空间可以跨越一个或多个节点。分区组子句可以用于以精细分级 (fine granular) 的方式调节表空间可跨越的节点数量。表可以划分到若干个分区上。

[0026] 如果与文件系统技术例如全局并行文件系统 (GPFS) 相结合，那么在涉及到的存储设备和文件系统之间还有另外的抽象层，抽象层对文件空间的使用者例如数据库隐藏了底层物理存储硬件的细节以提高业务弹性。

[0027] 类似于单节点数据库系统，对于多节点数据库系统来说同样难以在表空间被弃用时销毁敏感信息。

[0028] 在常规的系统中，只有数据库才知道硬盘 / 文件系统中的哪些部分属于表所有并且应该被清理以用于销毁敏感信息。

[0029] 某些常规的系统使用了文件系统加密技术。这样的文件系统加密技术在对数据库有高端性能要求的情况下可能无法使用，原因在于其性能影响和输入 / 输出 (I/O) 操作都是对任何数据库操作的性能约束。而且，在裸设备的情况下并未涉及文件系统，因此这些文件系统加密技术也不可用。

发明内容

[0030] 提供了用于删除数据库内敏感信息的方法、计算机程序产品和系统。识别数据库内通过语句访问的一个或多个对象。通过检查用于至少一个对象的标记而在识别的一个或

多个对象中确定包含敏感信息的至少一个对象。识别与至少一个对象相关联的一种或多种安全策略。针对至少一个对象实施识别的一种或多种安全策略以删除敏感信息。

附图说明

[0031] 现参照附图进行说明，其中相似的附图标记始终用于表示对应的部件：

[0032] 图 1 根据某些实施例示出了计算环境。

[0033] 图 2 根据某些可选实施例示出了计算环境。

[0034] 图 3 根据某些实施例示出了数据库目录中的表示例。

[0035] 图 4 根据某些实施例以流程图示出了用于在数据库目录内存储数据的操作。

[0036] 图 5 根据某些实施例以流程图示出了用于通过安全删除敏感信息来处理语句的操作。图 5 由图 5A 和图 5B 构成。

[0037] 图 6 根据某些实施例以流程图示出了用于实施一种或多种安全策略的操作。

[0038] 图 7 根据某些实施例示出了单服务器的计算环境。

[0039] 图 8 根据某些可选实施例示出了单服务器的计算环境。

[0040] 图 9 根据某些实施例描绘了云计算节点。

[0041] 图 10 根据某些实施例描绘了云计算环境。

[0042] 图 11 根据某些实施例描绘了抽象模型层。

具体实施方式

[0043] 给出本发明各种实施例的说明是为了进行介绍而并不是为了穷举或受限于公开的实施例。多种修改和变形对于本领域技术人员来说显而易见且并不背离所述实施例的范围和实质。本文使用的术语被选择用于更好地阐述实施例的原理、跟市场上现有技术相比的实际应用或技术进步或者使其他的本领域技术人员能够理解本文公开的实施例。

[0044] 图 1 根据某些实施例示出了多服务器的计算环境。服务器 100a...100n（其中 a 和 n 代表正整数）耦合至企业服务总线 (ESB)150。每一台服务器 100a...100n 都包含数据库 110a...110n。每一个数据库 110a...110n 都包括一个或多个表空间，其中每一个表空间都存储有一张或多张表 112a...112n。每一个数据库 110a...110n 还包括数据库目录 114a...114n 和数据库 I/O 层 116a...116n。

[0045] 每一台服务器 100a...100n 都耦合至存储系统。在各种实施例中，不同的服务器可以耦合至不同数量的存储系统。在图 1 中，服务器 100a 耦合至存储系统 120b...120m（其中 b 和 m 代表正整数）。每一个存储系统 120b...120m 都包括一个或多个文件系统设备 122b...122m 以及一个或多个裸存储设备 124b...124m。在图 1 中，服务器 100n 耦合至存储系统 130c...130p（其中 c 和 p 代表正整数）。每一个存储系统 130c...130p 都包括一个或多个文件系统设备 132c...132p 以及一个或多个裸存储设备 134c...134p。

[0046] 另外，安全策略系统 160、敏感信息检测器 162 和轻型目录访问协议 (LDAP) 系统 164 耦合至 ESB150。服务器 100a...100n 通过 ESB150 与安全策略系统 160、敏感信息检测器 162 和 LDAP 系统 164 交互。LDAP 系统 164 用于识别数据库和服务器的用户以及明确用户所在的组（其中组成员用于在访问数据库和服务器时使用的授权规则）。在某些实施例中，数据库系统可以通过与 LDAP 系统 164 相集成而向企业级的 LDAP 系统 164 委派用于验

证用户的任务。由于验证是在数据库执行授权特许之前就已完成，因此 LDAP 系统 164 被包括用于整体描述访问过程以及 LDAP 储存库内已知注册用户所用的策略。

[0047] 图 2 根据某些可选实施例示出了计算环境。在图 2 中，服务器 200a 包括在四个表空间内拥有十一张表 (T1-T11) 的数据库 210a。类似地，服务器 200n 包括在四个表空间内拥有十一张表 (T1-T11) 的数据库 210n。而且，服务器 200a 耦合至存储系统 220b, 220m，并且每一个存储系统 220b, 220m 都包括四个文件系统设备（每一个都用“FS”表示）和两个裸设备（每一个都用“R”表示）。类似地，服务器 200n 耦合至存储系统 230c, 230p，并且每一个存储系统 230c, 230p 都包括四个文件系统设备（每一个都用“FS”表示）和两个裸设备（每一个都用“R”表示）。

[0048] 实施例提供了：

[0049] • 数据库目录的扩展；

[0050] • 针对数据库发布的语句（例如结构化查询语言 (SQL) 语句）所用的语句语法的扩展；

[0051] • 数据库 I/O 层的扩展；

[0052] • 安全策略系统；

[0053] • 敏感信息检测器；以及

[0054] • 将这些组件整合为统一的端到端 (e2e) 的紧密集成解决方案。

[0055] 数据库目录的扩展

[0056] 数据库目录包括包含表相关元数据的表（“OBJECT_TABLES”）、包含索引相关元数据的表（“OBJECT_INDEX”）以及包含表空间相关元数据的表（“OBJECT_TABLESPACE”）。在实施例中，每一张表（“OBJECT_TABLES”、“OBJECT_INDEX”和 OBJECT_TABLESPACE）都包括安全删除栏，其为每一个对象（例如 TABLE、INDEX、TABLESPACE）存储了安全删除标记（“indicator”）以指示该对象是否包含敏感信息。在某些实施例中，安全删除标记是布尔型标记 (Boolean flag)。安全删除标记的一种设定（例如设定为真或“1”）表示对象包含敏感信息，而安全删除标记的另一种设定（例如设定为假或“0”）则表示对象不包含敏感信息。

[0057] 此外，在实施例中，每一张表（“OBJECT_TABLES”、“OBJECT_INDEX”和 OBJECT_TABLESPACE）都包括存储一种或多种相关安全策略的位置的安全策略栏（也就是域）。在某些实施例中，（与对象相关联的）安全策略栏的每一行都包含指向可应用于该对象的安全策略的一个或多个指针（例如统一资源定位符 (URL)）。在实施例中，指向可应用安全策略的指针可以从外部管理。这就允许随时改变安全策略并且在运行时执行安全策略。

[0058] 在各种实施例中，（不同于表、索引和表空间的）其他对象也可以在数据库目录内拥有以安全删除栏和安全策略栏扩展的表。

[0059] 图 3 根据某些实施例示出了数据库目录中的示例表 300。表 300 包括对象标识符 310、安全删除栏 320 和安全策略栏 330。省略号表示表 300 可以包括其他的栏。

[0060] 图 4 根据某些实施例以流程图示出了用于在数据库目录内存储数据的操作。控制开始于模块 400，其中敏感信息检测器识别数据库内存储敏感信息的一个或多个对象。在模块 402，针对所述一个或多个对象中的每一个，敏感信息检测器设定安全删除标记以指示对象包含敏感信息并在数据库目录中识别用于该对象的一种或多种安全策略。

[0061] 因此，在某些实施例中，敏感信息检测器在每一个数据库内执行周期性审计以搜索包含敏感信息的对象，并且如果找到就在数据库目录中设定安全删除标记以指示对象包含敏感信息。

[0062] 语句语法的扩展

[0063] 实施例通过向语句中加入“DELETE SECURE LEVEL”来扩展针对数据库发布的语句的语法。使用“DELETE SECURE LEVEL”就表示要执行数据库的安全删除，并且“LEVEL”识别要执行的安全清除的程度。例如，某些标准考虑了用随机数或零来一次性重写，从而足以安全地删除磁盘上的数据。这可以认为是级别 1。其他的标准可以利用多次写操作以不同的数据模式来重写数据。这可以认为是级别 2。例如，以下的列表包括（例如在 SQL 内）具有扩展语法的示例性语句，但是实施例并不局限于这些示例：

[0064] • DROP TABLE[...]DELETE SECURE LEVEL<INT>

[0065] • DROP INDEX[...]DELETE SECURE LEVEL<INT>

[0066] • DROP TABLESPAC[...]DELETE SECURE LEVEL<INT>

[0067] • ALTER TABLESPACE[...]DELETE SECURE LEVEL<INT>

[0068] • ADMIN_MOVE_TABLE[...]DELETE SECURE LEVEL<INT>

[0069] 在各种实施例中，数据库内可以有包含敏感信息的其他对象（例如数据库可以用来处理的临时表或临时表空间）。因此，上述列表是非穷举性的，并且可以将其他的语句扩展为在各种数据库的实施方式中包括“DELETE SECURE LEVEL”的使用。

[0070] “DELETE SECURE”是供访问数据库的语句使用的可选子句。如果在语句中列出了“DELETE SECURE”的选项，那么根据选择的级别 (LEVEL) 用多种方式中的一种来完成敏感信息的安全销毁。以下是安全销毁敏感信息的示例：

[0071] • 释放裸设备（例如在 DROP TABLESPACE 或 ALTER TABLESPACE 的语句之后）

[0072] •释放文件容器（例如在用 DROP TABLESPACE 或 ALTER TABLESPACE 指令释放文件系统中的文件时）

[0073] • 释放文件中的某些部分（例如在 DROP TABLE 或 ADMIN_MOVE_TABLE 之后）

[0074] 对于不同的操作系统平台，能够有不同的实施方式可供用于安全销毁敏感信息。而且，在某些实施例中，根据由来自所有可用技术集合的安全策略概括的要求，可用技术的子集是可允许的。在某些实施例中，数据库对于每一种操作系统平台都包括至少一种实施方式并且对于另外的技术提供附加库。

[0075] 图 5 根据某些实施例以流程图示出了用于通过安全删除敏感信息来处理语句的操作。图 5 由图 5A 和图 5B 构成。控制开始于模块 500，其中数据库接收的语句可以包括指示要执行安全删除并且识别安全删除级别的子句（例如“DELETE SECURE”子句）。如上所述，“DELETE SECURE”子句是可选的，并且有时候语句的作者可能会忘记将“DELETE SECURE”子句包括在内。无论语句中是否包括“DELETE SECURE”子句，数据库都执行敏感信息的安全删除。在模块 502，数据库处理语句。例如，如果语句是要弃用表，那就将表弃用。在模块 504，数据库识别由语句访问的对象。在模块 506，数据库利用跟数据库目录内的每一个对象相关联的安全删除标记来确定如果有的话是哪些识别的对象包含敏感信息。也就是说，对于每一个识别的对象，数据库都检查数据库目录以确定安全删除标记是否被设定为指示该对象包含有敏感信息。

[0076] 在模块508，数据库确定是否有任何对象已被识别为包含敏感信息。如果已经识别了这样的对象，那么处理就继续前往模块510（图5A），否则处理即告完成。

[0077] 在模块510，数据库从识别对象中的第一个识别对象开始选择下一个识别对象。在模块512，针对选中的对象，数据库从用于该对象的数据库目录中获取一种或多种安全策略。在模块512，如果（在模块500接收的）语句包括指示要执行安全删除并且识别安全删除级别的子句，那么该信息就由数据库用于选择一种或多种安全策略。如果语句并不包括这样的子句，那么数据库就选择默认的安全策略。在模块514，针对选中的对象，数据库实施一种或多种安全策略。在模块516，数据库确定是否已经选择了所有的识别对象。如果是这样，那么处理即告完成，否则处理就继续前往模块510。

[0078] 在某些实施例中，对于模块514中的操作，一种或多种安全策略如何执行取决于多种因素，例如文件系统（由此还有相关的操作系统）与裸磁盘和其他底层的技术细节。因此，模块514中的策略执行操作可以由于这些技术细节而有所不同。

[0079] 图6根据某些实施例以流程图示出了用于实施一种或多种安全策略的操作。控制开始于模块600，其中数据库确定对象是否存储在文件系统内。如果是这样，那么处理就继续前往模块602，否则处理就继续前往模块604。在模块602，数据库针对文件系统实施一种或多种安全策略。

[0080] 在模块604，数据库确定对象是否存储在加密的文件系统内。如果是这样，那么处理就继续前往模块606，否则处理就继续前往模块608。在模块606，数据库针对加密的文件系统实施一种或多种安全策略。

[0081] 在模块608，数据库确定对象是否存储在裸磁盘内。如果是这样，那么处理就继续前往模块610，否则处理就继续检查用于对象的存储器类型并且针对这种类型的存储器实施一种或多种安全策略（这在图6中用省略号表示）。在模块610，数据库针对裸磁盘实施一种或多种安全策略。

[0082] 在某些实施例中，“DELETE SECURE”子句的实施如下：

[0083] • 对于数据库目录内具有敏感信息的每一个对象，激活安全删除标记并且识别一种或多种安全策略。安全策略定义了SECURE_DELETE选择的可允许范围以及默认选择。

[0084] • 如果作者在访问包含敏感信息的至少一个对象的语句中忘记了DELETE SECURE可选子句，为此设定安全删除标记以指示对象包含敏感信息（例如在弃用包含敏感信息的表时），那么数据库就确定用默认选择来安全删除对象。

[0085] •如果作者明确设定了DELETE SECURE子句并且识别了级别，那么所述级别就指明了（例如来自可允许选择集合的）一种或多种安全策略。在某些实施例中，作者可以查询数据库目录以获取可允许选择的集合。

[0086] 数据库I/O层的扩展

[0087] 数据库I/O层调用执行安全删除操作的库来根据需要重写硬盘区域以确保准确删除。在某些实施例中，这样的调用符合事务处理型数据库的原子性、一致性、隔离性、持久性（ACID）的性质，可以在后台执行，并且可以有弹性地应对断电。

[0088] 安全策略系统

[0089] 在某些实施例中，安全策略系统由数据库管理程序或其他用户实现一种或多种安全策略的创建。每一种安全策略都定义了用于销毁保密信息的具体措施。在某些实施例中，

安全策略等价于级别。例如，安全策略可以指明要将保密信息重写三次。在某些其他的实施例中，可以导入一种或多种安全策略作为相关安全标准的一部分。

[0090] 图 7 根据某些实施例示出了单服务器的计算环境。在图 7 中，服务器 700 包括数据库 710。数据库 710 包括一个或多个表空间，其中每一个表空间都存储有一张或多张表 712。数据库 710 还包括数据库目录 714、数据库 I/O 层 716、敏感信息检测器 740 和安全管理器 742。安全管理器 742 包括安全策略系统 744。

[0091] 服务器 700 耦合至存储系统 720b...720m（其中 b 和 m 代表正整数）。每一个存储系统 720b...720m 都包括一个或多个文件系统设备 722b...722m 以及一个或多个裸存储设备 724b...724m。

[0092] 图 8 根据某些可选实施例示出了单服务器的计算环境。在图 8 中，服务器 800 包括在四个表空间内拥有十一张表 (T1-T11) 的数据库 810。而且，服务器 800 耦合至存储系统 820b,820m，并且每一个存储系统 820b,820m 都包括四个文件系统设备（每一个都用“FS”表示）和两个裸设备（每一个都用“R”表示）。

[0093] 在某些实施例中，安全管理器控制数据库的安全方面。在某些实施例中，安全管理器通过围绕安全销毁敏感信息的策略概念来进行扩展。在这样的实施例中，敏感信息检测器 162 被移入数据库内。然后安全管理器即可控制例如敏感信息检测器应该如何频繁地在数据库内搜索敏感信息，还可以控制能够触发敏感信息检测器以启动搜索敏感信息的数据库用户。

[0094] 在某些实施例中，每一台服务器（例如 100a...100n，200a，200n，300，400）都有（图 9 示出的）计算节点 910 的结构并且构成云环境的一部分。在某些可选实施例中，服务器并不是云环境的一部分。

[0095] 实施例提供了安全销毁敏感信息的技术向数据库系统内的紧密集成以确保安全删除硬盘上的敏感区域。

[0096] 实施例在数据库内发现敏感信息，在数据库目录内将表或表空间标记为包含敏感信息，并且将由表或表空间使用的空间链接至底层的物理设备。在实施例中，数据库通过用于文件系统的适当接口来触发真正的“销毁”操作。在实施例中，数据库在事务日志文件内触发真正的“销毁”。实施例提供策略语言以允许明确不同的安全级别。

[0097] 实施例由于与数据库的紧密集成而确保在已不再需要的时候删除敏感信息，这样就以低运行成本降低了敏感信息泄密的风险。

[0098] 实施例在数据库内提供了供数据库安全销毁敏感信息的操作，例如：DROP TABLESPACE，ALTER TABLESPACE（例如可以利用该语句来弃用容器），DROP TABLE，DROP INDEX（例如索引结构内的字段可以包含有敏感信息），ONLINE TABLE MOVE，DROP DATABASE。

[0099] 实施例在同样具有硬盘持久性的数据库事务日志内提供敏感信息的安全销毁。实施例为使用不涉及任何文件系统的裸设备的数据库提供敏感信息的安全销毁，并且此时文件系统不知道有那些包含敏感信息的部分属于表空间内的表。

[0100] 实施例在无法使用硬盘 / 文件系统加密和 / 或数据库加密时确保敏感信息的准确删除。

[0101] 实施例在数据库开始使用后检测到敏感信息时（例如在审计期间，此时转移到另

一个数据库系统已经不现实）提供敏感信息的安全销毁。对于这些情况，因为数据已经被未加密地物理创建，所以硬盘 / 文件系统的加密和数据库的加密都无法使用。

[0102] 实施例通过允许创建策略以告知数据库如何处理敏感信息并利用数据库目录内的元数据将表或表空间标记为包含敏感信息来提供敏感信息的安全销毁。

[0103] 实施例可以在先前并非敏感的新规则可能变为敏感时、在公司扩张到拥有严格数据隐私法律的国家（例如美国公司扩张到欧洲国家）时、在审计表明数据库系统包含敏感信息并且应该遵循更严格的安全控制时使用。尽管在这些情况下可能会限制访问，但是实施例提供了敏感信息的安全删除。实施例避免了将数据从使用未加密文件系统的一个数据库转移到使用加密文件系统的另一个数据库的需要（出于成本和时间的原因这样做可能很困难）。

[0104] 对于数据库来说，未能安全删除敏感信息就难以区分丢弃的硬盘是否仍然包含敏感信息，将公司置于安全风险中。而且通过访问到文件系统层带来的内部攻击（但是不必到达数据库，原因在于很多企业都有独立的操作系统和数据库管理团队）或许能够在硬盘上发现敏感信息，这里从数据库的观点看就已经用 DROP 操作删除了数据。

[0105] 实施例确保准确删除云计算基础设施内的敏感信息，其中在来自云服务提供商的基础设施内配置数据库系统。

[0106] 实施例强化了数据库 I/O 层以根据 SOL 语言的改进在各种操作期间销毁敏感信息。在某些实施例中，数据库是关系数据库管理系统 (RDBMS)。

[0107] 云环境

[0108] 应该预先理解的是尽管本公开包括关于云计算的详细说明，但是本文所述教导的实施并不局限于云计算环境。相反，本发明的实施例能够结合目前已知或今后开发的任何其他类型的计算环境实施。

[0109] 云计算是一种交付用于对可配置计算资源（例如网络、网络带宽、服务器、处理器、内存、存储、应用程序、虚拟机和服务）的共享池实现便捷的按需网络访问的服务模型，所述可配置计算资源能够以最小的管理代价或者通过跟服务供应商的交互而被快速提供和释放。这种云模型可以包括至少五种特性、至少三种服务模型以及至少四种部署模型。

[0110] 特性如下所述：

[0111] 按需自助服务：云用户可以根据需要自动地单方面提供计算能力例如服务器时间和网络存储而无需与服务供应商人工交互。

[0112] 广泛的网络访问：功能可通过网络获得并且可通过不同的瘦客户端平台或胖客户端平台（例如移动电话、笔记本电脑和 PDA）都能推广使用的标准机制来访问。

[0113] 资源池化：供应商的计算资源被池化以利用多租户模型服务于多个用户，其中不同的实体资源和虚拟资源根据需求来动态地分配和重新分配。存在位置独立性的概念因为用户一般无法控制或者获知所提供资源的确切位置，但是可以明确在更高抽象层级（例如国家、州或数据中心）的位置。

[0114] 快速弹性：功能可以快速和有弹性地提供，在某些情况下可以自动地提供，用于快速扩展和迅速释放以快速收缩。对于用户来说，可供使用的功能经常表现为无限制并且可以随时以任意数量购买。

[0115] 可度量的服务：云系统通过在适用于服务类型（例如存储、处理、带宽和活跃用户

账户）的某一抽象层级上调节计量能力来自动控制和优化资源的使用。资源的使用可以被监测、控制和汇总以为所用服务的供应商和用户提供透明度。

[0116] 服务模型如下所述：

[0117] 软件即服务（SaaS）：提供给用户的功能是使用供应商在云基础设施上运行的应用程序。可以从各种不同的客户端设备通过瘦客户端界面例如网页浏览器（譬如基于网页的电子邮件）来访问应用程序。用户并不管理或控制底层的云基础设施，其中包括网络、服务器、操作系统、存储或者乃至单独的应用程序功能，有限的用户指定的应用程序配置设定可以例外。

[0118] 平台即服务（PaaS）：提供给用户的功能是将用户创建或获取的利用供应商所支持的程序语言和工具创建的应用程序部署到云基础设施上。用户并不管理或控制底层的云基础设施，其中包括网络、服务器、操作系统或存储，但是要控制部署的应用程序并且还可能要控制托管环境配置的应用程序。

[0119] 基础设施即服务（IaaS）：提供给用户的功能是供给处理、存储、网络和其他基本计算资源，其中用户能够部署和运行可包括操作系统和应用程序在内的任意软件。用户并不管理或控制底层的云基础设施，但是要控制操作系统、存储、部署的应用程序并且还可能要有限地控制选择的网络组件（例如主机防火墙）。

[0120] 部署模型如下所述：

[0121] 私有云：云基础设施专为某一组织机构运行。它可以由该组织机构或第三方管理并且可以存在于内部部署或外部部署中。

[0122] 社区云：云基础设施由一些组织结构共享并支持具有共同诉求（例如使命、安全需求、政策和合规考量等）的特定社区。它可以由各组织机构或第三方管理并且可以存在于内部部署或外部部署中。

[0123] 公共云：云基础设施对公众或大的行业组织开放并且由销售云服务的组织机构所有。

[0124] 混合云：云基础设施由两种或多种云（私有云、社区云或公共云）组成，它们保持独立实体但通过能实现数据和应用程序的可移植性的标准技术或专利技术捆绑在一起（例如用于在云之间实现负载均衡的云爆发）。

[0125] 云计算环境通过着重于无国界、低耦合、模块化和语义互操作性来面向服务。云计算的核心是包括互连节点网络的基础设施。

[0126] 现参照图9，示出了云计算节点示例的示意图。云计算节点910仅为适用云计算节点的一个示例，并不意味着对本文所述本发明实施例的用途或功能的范围构成任何限制。无论如何，云计算节点910都能够实现和/或完成先前所述的任意功能。

[0127] 在云计算节点910中设有可用多种其他的通用或专用计算系统环境或配置操作的计算机系统/服务器912。可以适合于供计算机系统/服务器912使用的公知计算系统、环境和/或配置的示例包括但不限于个人计算机系统、服务器计算机系统、瘦客户端、胖客户端、手持设备或手提设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费电子产品、联网PC、小型计算机系统、大型计算机系统以及包括任意上述系统或设备的分布式云计算环境等。

[0128] 计算机系统/服务器912可以在计算机系统可执行指令的大体环境例如由计算机

系统执行的程序模块中描述。通常，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、逻辑、数据结构等。计算机系统 / 服务器 912 可以在分布式云计算环境中实现，在该环境中，任务由通过通信网络连接的远程处理设备完成。在分布式云计算环境中，程序模块可以位于包括内存存储设备的本地和远程计算机系统存储介质内。

[0129] 如图 9 所示，云计算节点 910 中的计算机系统 / 服务器 912 是以通用计算设备的形式示出。计算机系统 / 服务器 912 中的组件可以包括但不限于一个或多个处理器或处理单元 916、系统内存 928 以及将包括系统内存 928 在内的各种系统组件耦合至处理器 916 的总线 918。

[0130] 总线 918 表示任意几种总线结构类型中的一种或多种，包括使用多种总线架构中任何一种的内存总线或内存控制器、外围总线、加速图形端口以及处理器或局部总线。作为示例而非限制性地，这样的架构包括工业标准架构 (ISA) 总线、微通道架构 (MCA) 总线、增强型 ISA(EISA) 总线、视频电子标准协会 (VESA) 局部总线和外围组件互连 (PCI) 总线。

[0131] 计算机系统 / 服务器 912 典型地包括各种计算机系统可读取介质。这样的介质可以是能由计算机系统 / 服务器 912 访问的任意可用介质，并且其包括易失性和非易失性介质，可移动和不可移动的介质。

[0132] 系统内存 928 可以包括易失性内存形式的计算机系统可读取介质例如随机存取存储器 (RAM)930 和 / 或高速缓冲存储器 932。计算机系统 / 服务器 912 可以进一步包括其他的可移动 / 不可移动、易失性 / 非易失性的计算机系统存储介质。仅作为示例，可以提供存储系统 934 用于从不可移动的非易失性磁介质（未示出且通常称为“硬盘驱动器”）读取并向其中写入。尽管未示出，但是可以提供用于从可移动的非易失性磁盘（例如“软盘”）读取并向其中写入的磁盘驱动器以及用于从可移动的非易失性光盘例如 CD-ROM、DVD-ROM 或其他光学介质读取或向其中写入的光盘驱动器。在这些情况下，每一种驱动器均可通过一种或多种数据介质接口连接至总线 918。正如以下进一步图示和介绍的那样，内存 928 可以包括具有一组（例如至少一个）配置为实现本发明实施例所述功能的程序模块的至少一种程序产品。

[0133] 具有一组（至少一个）程序模块 942 的程序 / 实用程序 940 作为示例而非限制地可以与操作系统、一种或多种应用程序、其他的程序模块以及程序数据一起存储在内存 928 中。操作系统、一种或多种应用程序、其他的程序模块和程序数据中的每一者及其某种组合可以包括网络环境的实现。程序模块 942 通常实现如本文所述的本发明实施例中的功能和 / 或方法。

[0134] 计算机系统 / 服务器 912 也可以与一种或多种外部设备 914 例如键盘、点击设备、显示器 924 等、使用户能够跟计算机系统 / 服务器 912 交互的一种或多种设备、和 / 或使计算机系统 / 服务器 912 能够与一种或多种其他的计算设备通信的任意设备（例如网卡、调制解调器等）通信。这样的通信可以通过输入 / 输出 (I/O) 接口 922 进行。另外，计算机系统 / 服务器 912 可以通过网络适配器 920 与一种或多种网络例如局域网 (LAN)、通用广域网 (WAN) 和 / 或公共网络（例如因特网）通信。如所描述的，网络适配器 920 通过总线 918 与计算机系统 / 服务器 912 中的其他组件通信。应该理解的是尽管未示出，但是其他的硬件和 / 或软件组件能够与计算机系统 / 服务器 912 结合使用。示例包括但不限于 :微代码、设备驱动器、冗余处理单元、外部磁盘驱动器阵列、RAID 系统、磁带驱动器和数据归档存

储系统等。

[0135] 现参照图 10，示出了说明性的云计算环境 1050。如所示出的，云计算环境 1050 包括一个或多个云计算节点 910，由云用户使用的本地计算设备例如个人数字助理 (PDA) 或手机 1054A、台式计算机 1054B、笔记本电脑 1054C 和 / 或车载计算机系统 1054N 可以与云计算节点通信。节点 910 可以彼此通信。它们可以在如上所述的一种或多种网络例如私有云、社区云、公共云或混合云或者其组合内被实体地或虚拟地分组（未示出）。这就允许云计算环境 1050 提供基础设施、平台和 / 或软件作为服务，云用户不需要为此在本地计算设备上保留资源。应该理解图 10 所示计算设备 1054A-N 的类型仅仅是为了说明并且计算节点 910 和云计算环境 1050 可以通过任意类型的网络和 / 或网络可寻址连接（例如利用网页浏览器）与任何类型的计算机化设备通信。

[0136] 现参照图 11，示出了由云计算环境 1050（图 10）提供的一组功能抽象层。应该预先理解图 11 中示出的组件、层和功能仅仅是为了说明而且本发明的实施例并不局限于此。如所描述的，提供了以下的层和对应的功能：

[0137] 硬件和软件层 1160 包括硬件组件和软件组件。硬件组件的示例包括：大型机，在一个示例中是 IBM® 的 zSeries® 系统；基于 RISC（简化指令集计算机）架构的服务器，在一个示例中是 IBM 的 pSeries® 系统；IBM 的 xSeries® 系统；IBM 的 BladeCenter® 系统；存储设备；网络和联网组件。软件组件的示例包括：网络应用服务器软件，在一个示例中是 IBM 的 WebSphere® 应用服务器软件；以及数据库软件，在一个示例中是 IBM 的 DB2® 数据库软件。（IBM、zSeries、pSeries、xSeries、BladeCenter、WebSphere 和 DB2 都是在全世界很多行政区域内注册的国际商业机器公司的商标）。

[0138] 虚拟层 1162 提供了一种抽象层，从中可以提供以下的虚拟实体示例：虚拟服务器；虚拟存储器；虚拟网络，包括虚拟专用网络；虚拟应用程序和操作系统；以及虚拟客户端。

[0139] 在一个示例中，管理层 1164 可以提供下述功能。资源供给提供用于在云计算环境中执行任务的计算资源和其他资源的动态获取。计量和定价在资源于云计算环境中被使用时提供费用跟踪并为这些资源消耗记账或计价。在一个示例中，这些资源可以包括应用软件许可证。安全性为云用户和任务提供身份验证以及为数据和其他资源提供保护。用户入口为用户和系统管理员提供对云计算环境的访问。服务级别管理提供云计算资源的分配和管理以满足所需的服务级别。服务级别协议 (SLA) 计划和实行为云计算资源提供预设置并获取云计算资源，为此根据 SLA 预测未来需求。

[0140] 工作负载层 1166 提供了可以使用云计算环境的功能示例。可由该层提供的工作负载和功能的示例包括：映射和导航；软件开发和生命周期管理；虚拟课堂教育传输；数据分析处理；事务处理；以及安全删除处理。

[0141] 因此，在某些实施例中，提供根据本文所述实施例的实现安全删除敏感信息的软件或程序作为云环境中的服务。

[0142] 更多的实施例细节

[0143] 所属技术领域的技术人员知道，本发明的各个方面可以实现为系统、方法或计算机程序产品。因此，本发明的各个方面可以具体实现为以下形式，即：完全的硬件实施方式、

完全的软件实施方式(包括固件、驻留软件、微代码等),或硬件和软件方面结合的实施方式,这里可以统称为“电路”、“模块”或“系统”。此外,在一些实施例中,本发明的各个方面还可以实现为在一个或多个计算机可读介质中的计算机程序产品的形式,该计算机可读介质中包含计算机可读的程序代码。

[0144] 可以采用一个或多个计算机可读介质的任意组合。计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件,或者任意以上的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括:具有一个或多个导线的电连接、便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM 或闪存)、光纤、便携式紧凑盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本文件中,计算机可读存储介质可以是任何包含或存储程序的有形介质,该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

[0145] 计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号,其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式,包括——但不限于——电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质,该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

[0146] 计算机可读介质上包含的程序代码可以用任何适当的介质传输,包括——但不限于——无线、有线、光缆、RF 等等,或者上述的任意合适的组合。

[0147] 可以以一种或多种程序设计语言的任意组合来编写用于执行本发明操作的计算机程序代码,所述程序设计语言包括面向对象的程序设计语言—诸如 Java、Smalltalk、C++等,还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中,远程计算机可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)—连接到用户计算机,或者,可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。

[0148] 下面将参照根据本发明实施例的方法、装置(系统)和计算机程序产品的流程图和/或框图描述本发明。应当理解,流程图和/或框图的每个方框以及流程图和/或框图中各方框的组合,都可以由计算机程序指令实现。这些计算机程序指令可以提供给通用计算机、专用计算机或其它可编程数据处理装置的处理器,从而生产出一种机器,使得这些计算机程序指令在通过计算机或其它可编程数据处理装置的处理器执行时,产生了实现流程图和/或框图中的一个或多个方框中规定的功能/动作的装置。

[0149] 也可以把这些计算机程序指令存储在计算机可读介质中,这些指令使得计算机、其它可编程数据处理装置、或其他设备以特定方式工作,从而,存储在计算机可读介质中的指令就产生出包括实现流程图和/或框图中的一个或多个方框中规定的功能/动作的指令的制造品(article of manufacture)。

[0150] 计算机程序指令也可以载入到计算机、其他可编程数据处理装置或其他设备以促使在计算机、其他可编程装置或其他设备上执行一系列操作处理(例如操作或步骤),从而

生成计算机实施的过程，使得在计算机或其他可编程装置上执行的指令提供用于实现在流程图和 / 或框图的一个或多个模块中列举的功能 / 动作的过程。

[0151] 实施所述操作的代码可以进一步在硬件逻辑或电路内（例如集成电路芯片、可编程门阵列 (PGA)、专用集成电路 (ASIC) 等）实现。硬件逻辑可以耦合至处理器以执行操作。

[0152] 除非另有明确说明，否则彼此通信的设备不必彼此间连续通信。另外，彼此间通信的设备可以直接通信或者通过一种或多种媒介间接通信。

[0153] 对有若干部件彼此通信的实施例的说明并不意味着需要所有这样的部件。相反，介绍多种可选部件是为了说明本发明可行实施例的多样性。

[0154] 而且，尽管过程步骤、方法步骤、算法等可能是按一定的先后顺序进行介绍，但是这些过程、方法和算法也可以设置为以交错的顺序工作。换句话说，任何可能已介绍过的步骤次序或顺序都并不必然表示需要用这样的顺序来执行所述步骤。本文中介绍的过程步骤可以用任何实用的顺序执行。而且，部分步骤可以同时执行。

[0155] 在本文中介绍单个设备或物件时，显而易见的是可以使用多于一个设备 / 物件（无论它们是否协作）以代替单个设备 / 物件。类似地，在本文中介绍多于一个设备或物件（无论它们是否协作）时，显而易见的是可以使用单个设备 / 物件来代替多于一个的设备或对象或者可以使用不同数量的设备 / 物件来代替图示数量的设备或程序。设备的功能和 / 或特性可选地可以通过一种或多种其他的并未明确描述为具有这些功能 / 特性的设备来实施。因此，本发明的其他实施例不必包括所述设备自身。

[0156] 流程图中示出的操作给出了按照一定顺序进行的某些事件。在可选实施例中，某些操作可以按照不同的顺序执行、修改或删除。而且，可以向上述逻辑中增加操作并且仍然适用于所述实施例。此外，本文中介绍的操作可以顺序执行或者某些操作可以并行处理。更进一步地，操作可以由单个处理单元或者由分布式处理单元执行。

[0157] 本文中所用术语仅仅是为了描述特定的实施例，而并不是要限制本发明。如本文中所用，单数形式“一”、“一个”和“这个”应理解为也包括复数形式，上下文中清楚地另有说明除外。进一步应该理解的是术语“包括”和 / 或“包含”在本说明书中使用时明确了所述特征、整体、步骤、操作、元件和 / 或部件的存在，但是并不排除存在或加有一个或多个其他的特征、整体、步骤、操作、元件、部件和 / 或其群组。

[0158] 除非另有明确说明，否则术语“一个实施例”、“实施例”、“多个实施例”、“所述实施例”、“所述多个实施例”、“一个或多个实施例”、“一些实施例”和“一个实施例”是指“本发明的一个或多个（但并不是全部的）实施例”。

[0159] 除非另有明确说明，否则术语“包含”、“包括”、“具有”及其变形是指“包括但不限于”。

[0160] 除非另有明确说明，否则列举的项目列表并不意味着任何或全部的项目互相排斥。

[0161] 以下权利要求中的对应结构、材料、动作和所有装置或步骤以及功能元件的等价形式都应理解为包括用于实现与其他权利要求中明确主张的元素相结合的功能的任意结构、材料或动作。本发明的实施例介绍是为了解释和说明而给出，并不是为了穷举或者将本发明限制为所公开的形式。多种修改和变形对于本领域技术人员来说显而易见且并不背离本发明的范围和实质。选择和介绍实施例是为了清楚地解释本发明的原理和实际应用，并

且使本领域其他技术人员能够理解本发明以得到具有适用于特定预期用途的各种修改的不同实施例。

[0162] 附图中的流程图和框图显示了根据本发明的多个实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段或代码的一部分，所述模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和／或流程图中的每个方框、以及框图和／或流程图中的方框的组合，可以用执行规定的功能或动作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0163] 以上给出的对本发明实施例的介绍是为了进行解释和说明。不应将其理解为穷举或者将实施例限制为公开的具体形式。根据上述教导可能得到多种修改和变形。应该理解实施例的范围不应由这些具体实施方式限定，而是应该由本文所附的权利要求限定。以上的说明内容、示例和数据提供了制备和使用实施例组成部分的完整描述。由于无需背离本发明的实质和范围即可实现很多的实施例，因此实施例应体现在本文所附的权利要求或任何随后提交的权利要求及其等价形式中。

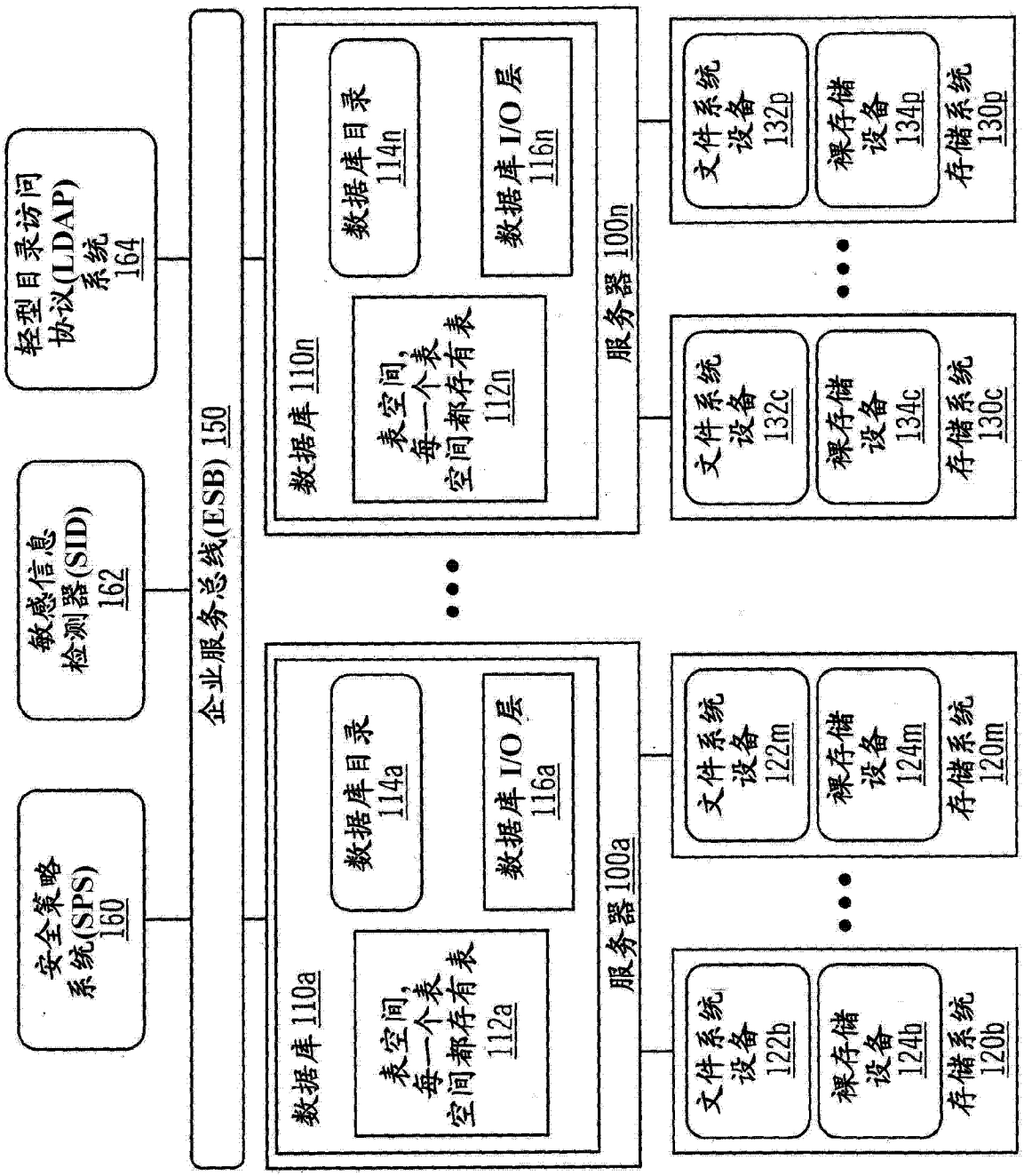

安全策略系统(SPS) 160
敏感信息检测器(SID) 162
轻型目录访问协议(LDAP)系统 164
企业服务总线(ESB) 150
数据库 110a
表空间，每一个表空间都存有表 112a
数据库目录 114a
数据库 I/O 层 116a
服务器 100a
文件系统设备 122b
裸存储设备 124b
存储系统 120b
文件系统设备 122m
裸存储设备 124m
存储系统 120m
数据库 110n
表空间，每一个表空间都存有表 112n
数据库目录 114n
数据库 I/O 层 116n
服务器 100n
文件系统设备 132c
裸存储设备 134c
存储系统 130c
文件系统设备 132p
裸存储设备 134p
存储系统 130p

图 1

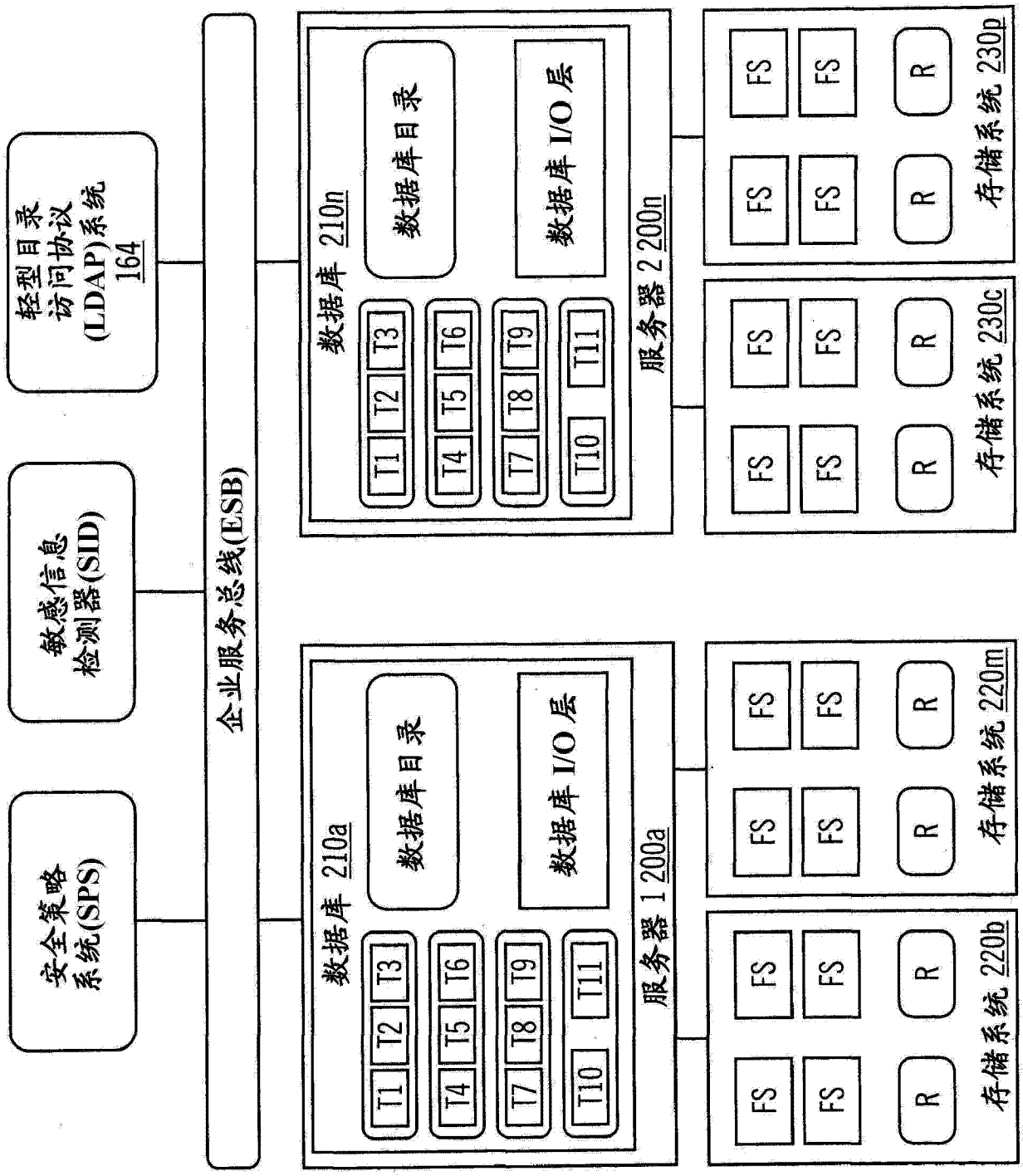

安全策略
系统(SPS)
敏感信息
检测器(SID)
轻型目录
访问协议
(LDAP)系统
164
企业服务总线(ESB)
服务器 1 200a
数据库 210a
T1
T2
T3
T4
T5
T6
T7
T8
T9
T10
T11
数据库目录
数据库 I/O 层
服务器 2 200n
数据库 210n
FS
R
存储系统 220b
存储系统 220m
存储系统 230c
存储系统 230p

图 2

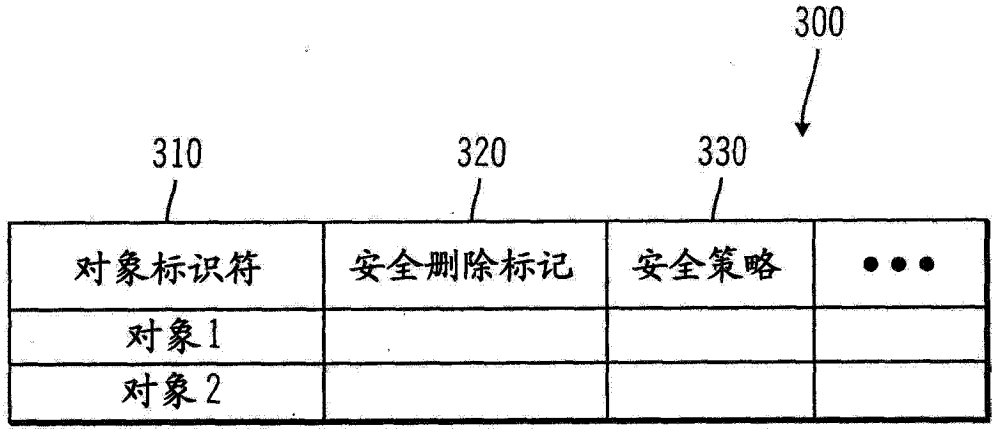

300
310
320
330
对象标识符
安全删除标记
安全策略
• • •
对象 1
对象 2

图 3

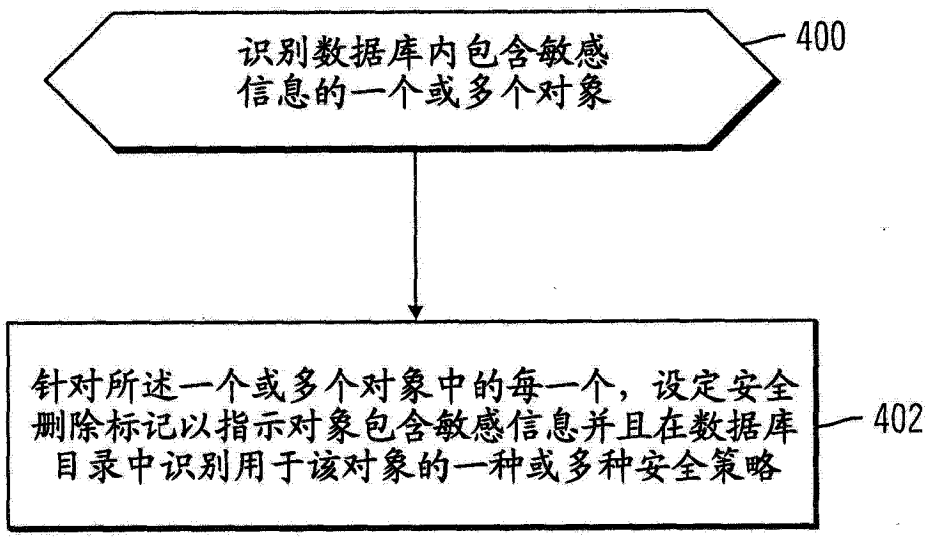

识别数据库内包含敏感信息的一个或多个对象
400
针对所述一个或多个对象中的每一个，设定安全删除标记以指示对象包含敏感信息并且在数据库目录中识别用于该对象的一种或多种安全策略
402

图 4

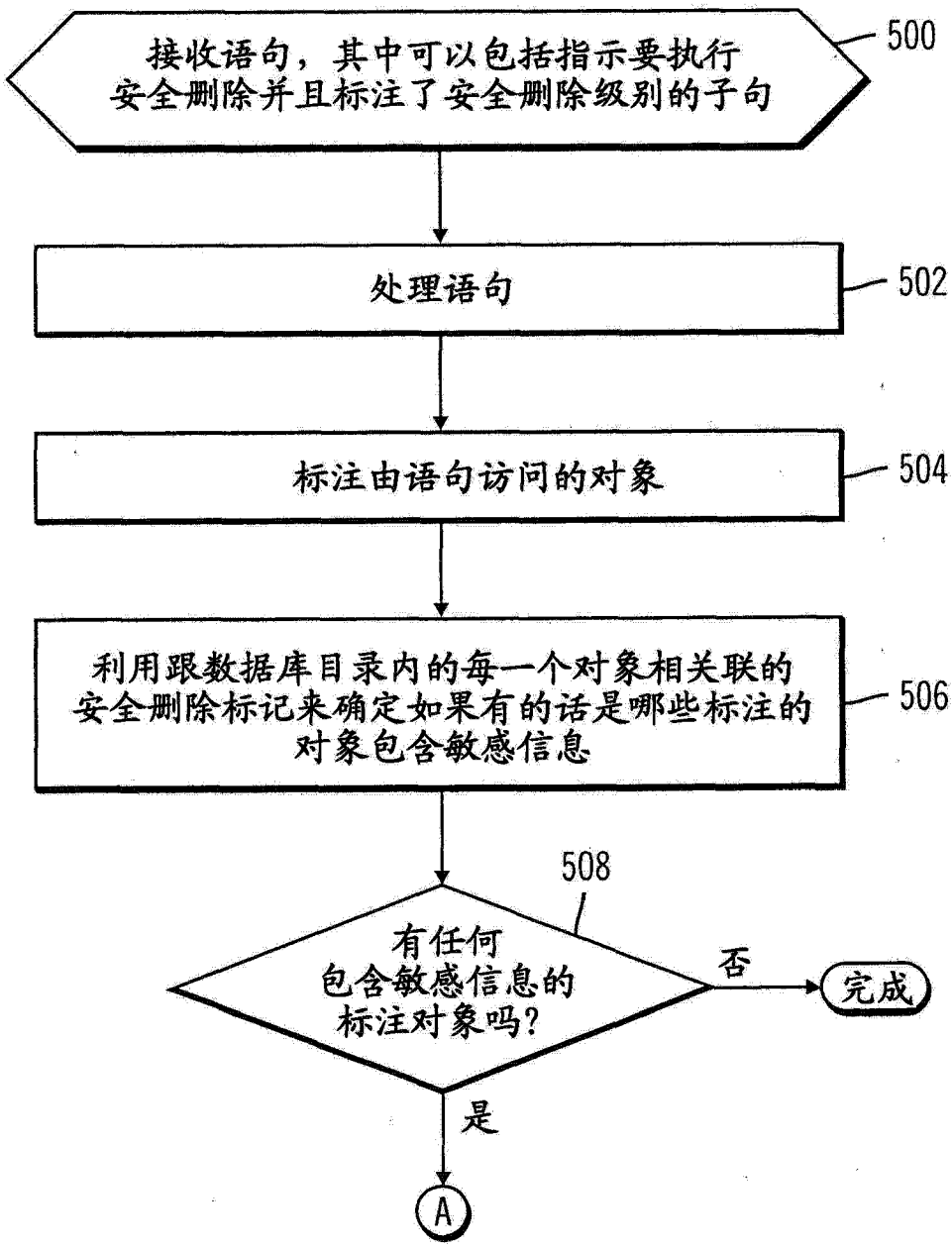

接收语句，其中可以包括指示要执行安全删除并且标注了安全删除级别的子句
500
处理语句
502
标注由语句访问的对象
504
利用跟数据库目录内的每一个对象相关联的安全删除标记来确定如果有的话是哪些标注的对象包含敏感信息
506
508
有任何包含敏感信息的标注对象吗?
否
完成
是
A

图 5A

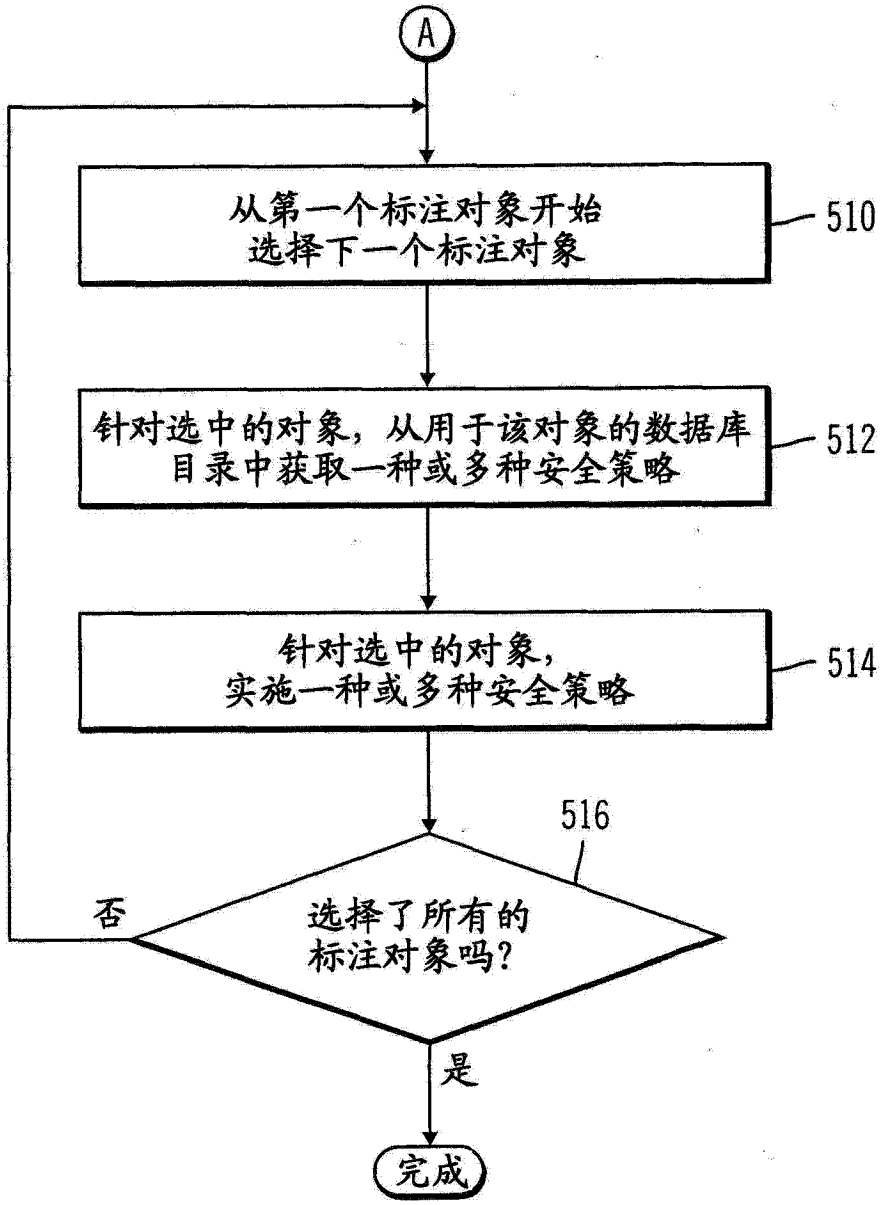

A
从第一个标注对象开始
选择下一个标注对象
510
针对选中的对象，从用于该对象的数据库
目录中获取一种或多种安全策略
512
针对选中的对象，
实施一种或多种安全策略
514
516
选择了所有的
标注对象吗?
否
是
完成

图 5B

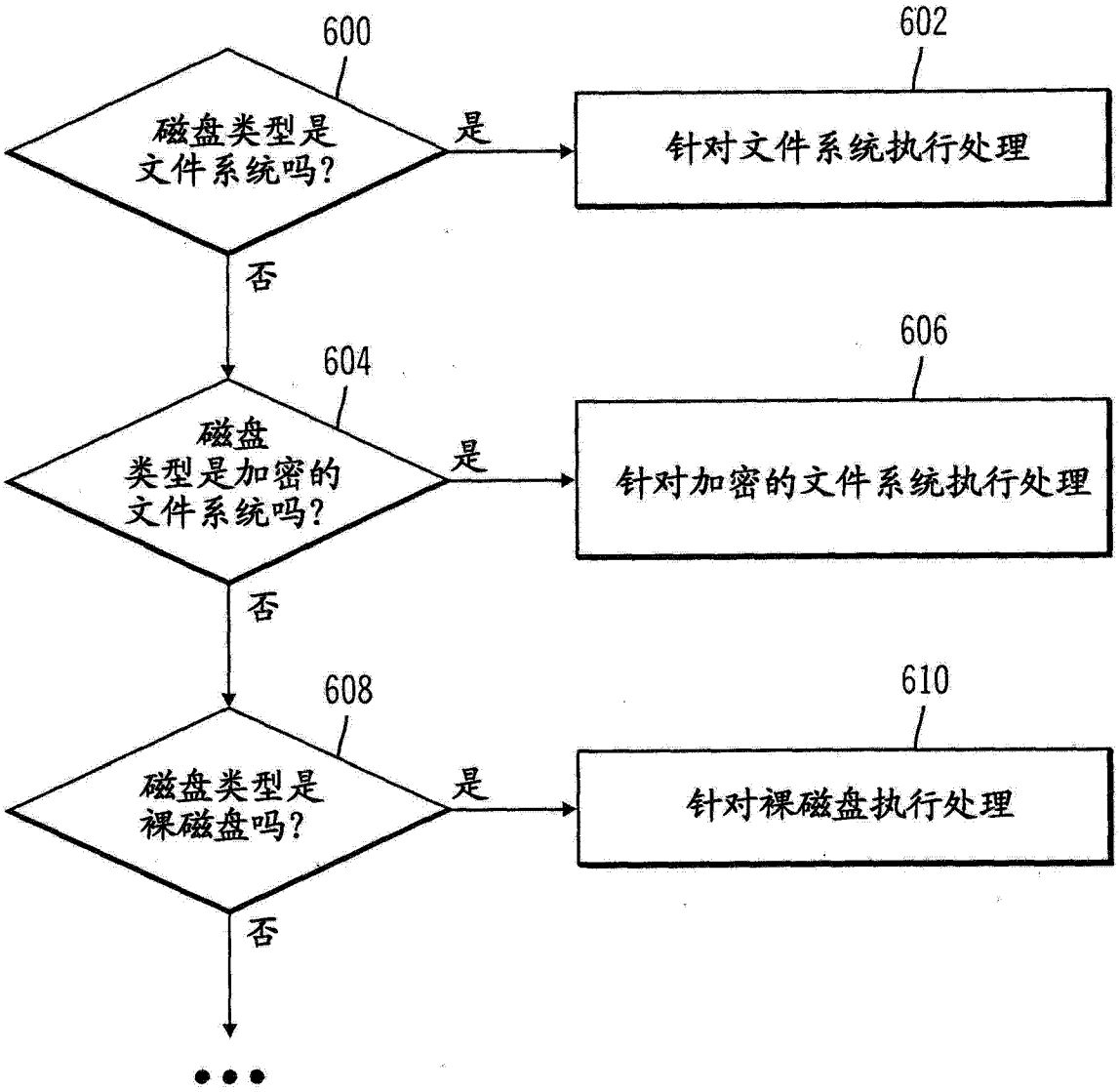

600
磁盘类型是
文件系统吗?
是
602
针对文件系统执行处理
否
604
磁盘
类型是加密的
文件系统吗?
是
606
针对加密的文件系统执行处理
否
608
磁盘类型是
裸磁盘吗?
是
610
针对裸磁盘执行处理
否

图 6

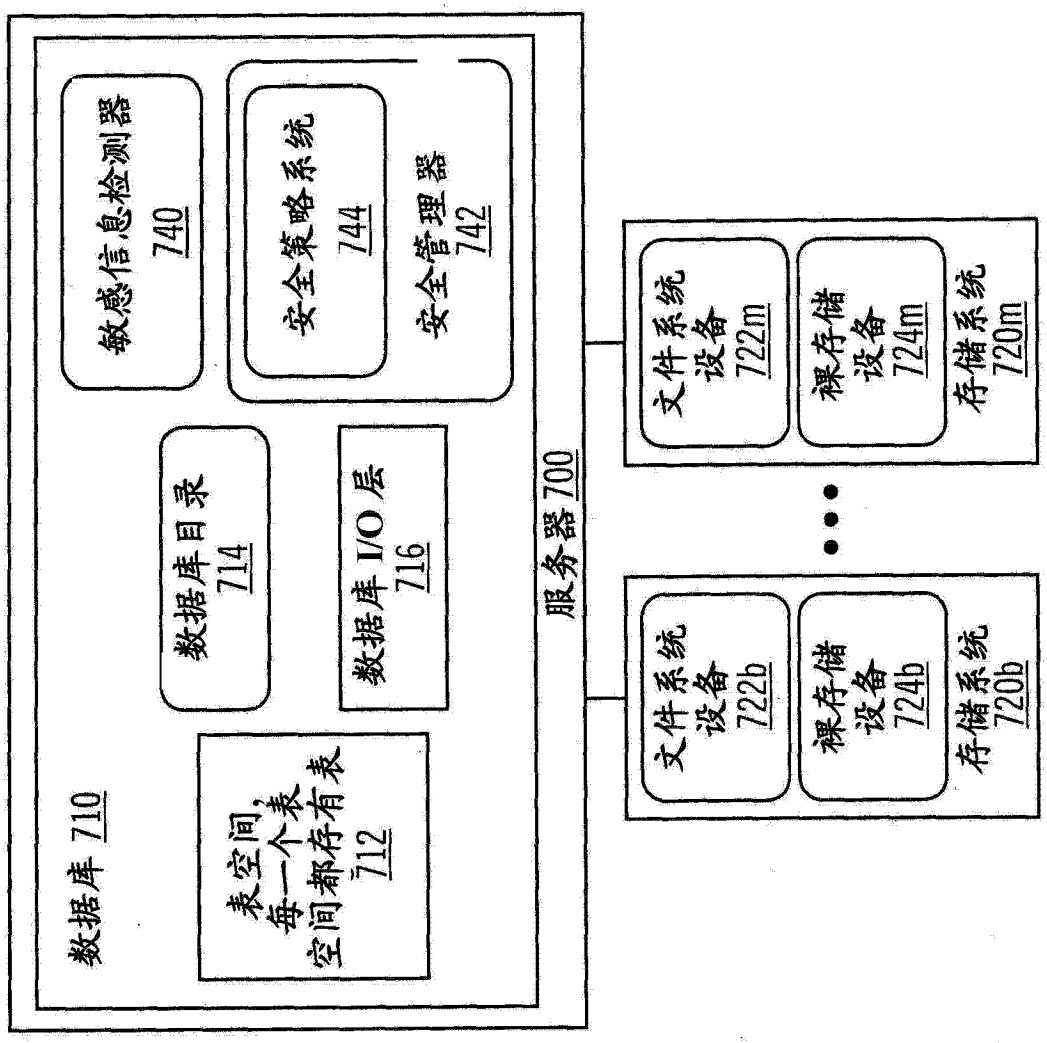

数据库 710
表空间，每一个表空间都存有表 712
数据库目录 714
数据库 I/O 层 716
敏感信息检测器 740
安全管理器 742
安全策略系统 744
服务器 700
文件系统设备 722b
裸存储设备 724b
存储系统 720b
文件系统设备 722m
裸存储设备 724m
存储系统 720m

图 7

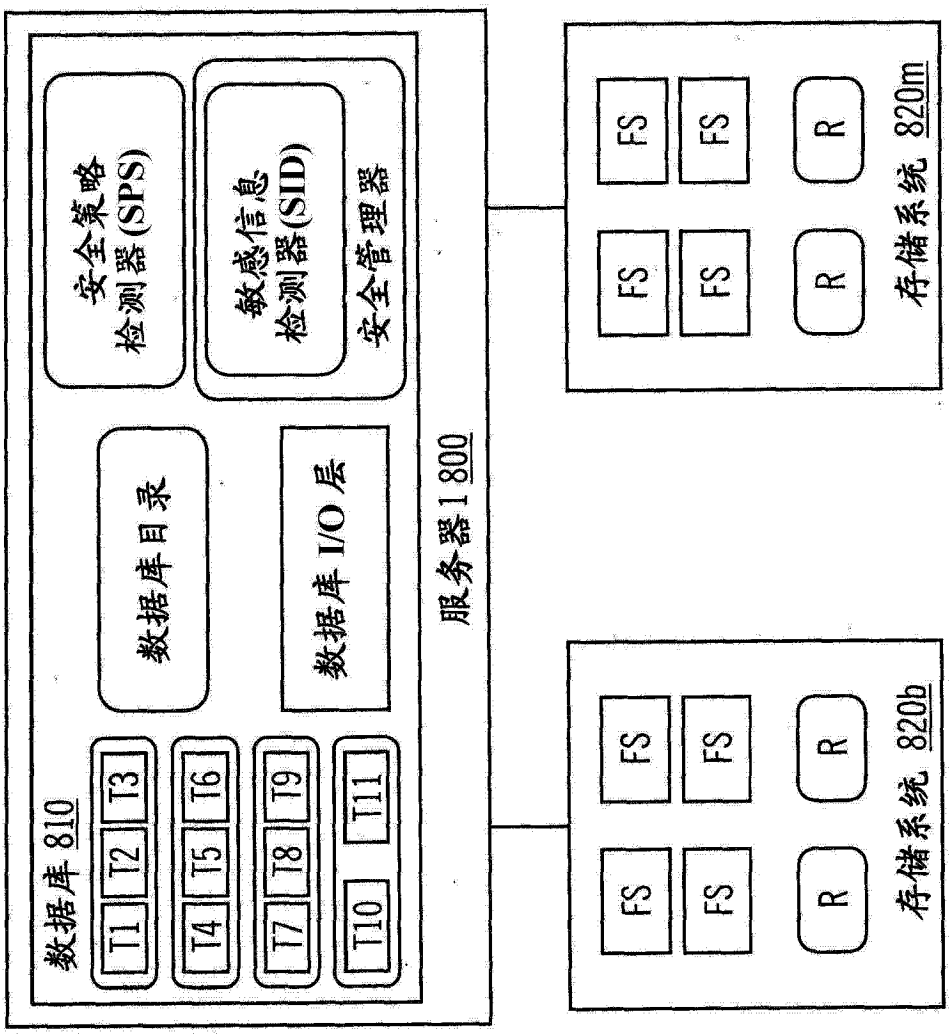

数据库 810
T1
T2
T3
T4
T5
T6
T7
T8
T9
T10
T11
数据库目录
数据库 I/O 层
安全策略检测器 (SPS)
敏感信息检测器(SID)
安全管理器
服务器 1 800
FS
R
存储系统 820b
存储系统 820m

图 8

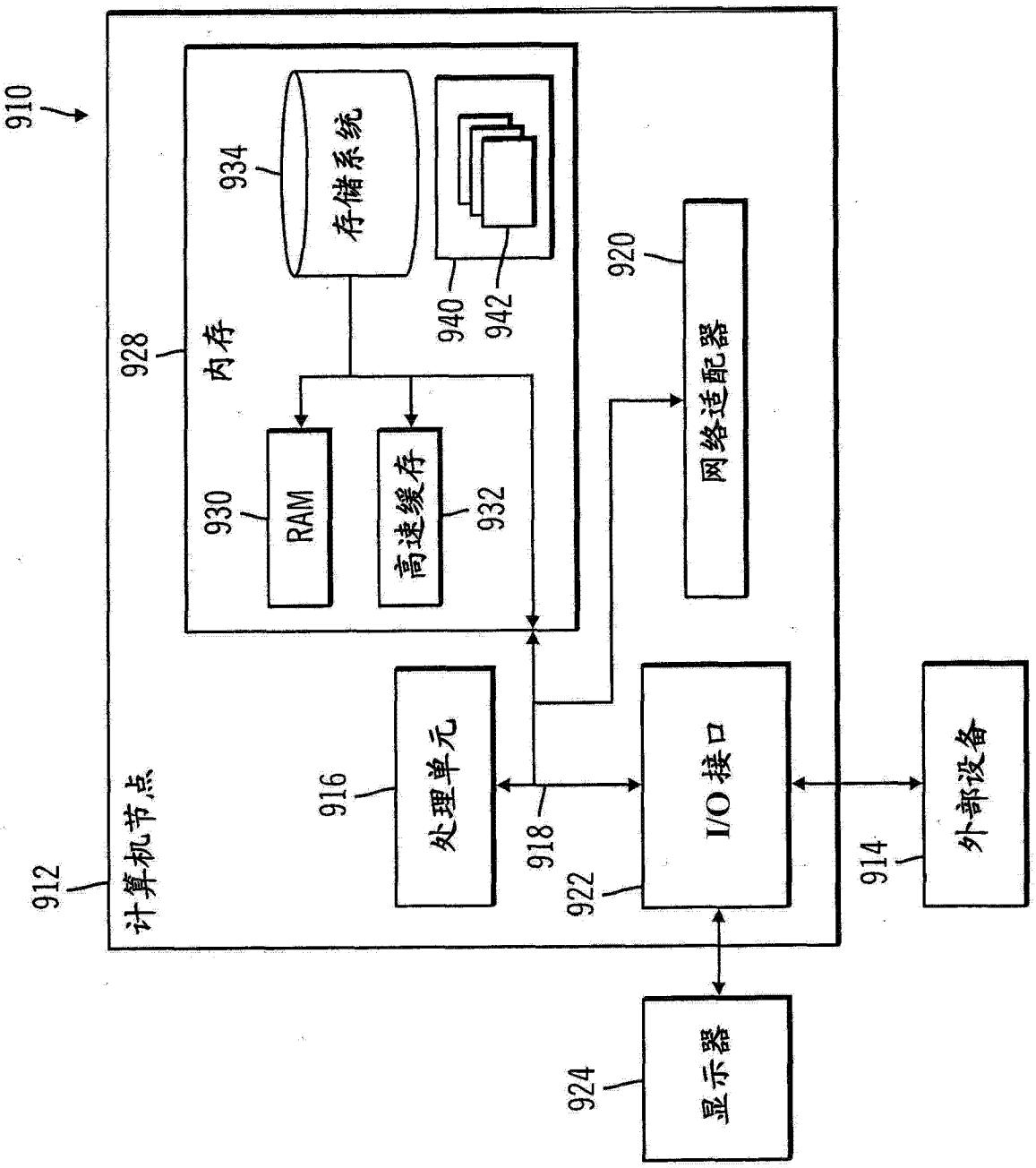

910
计算机节点
912
928
内存
934
存储系统
940
942
930
RAM
932
高速缓存
920
网络适配器
916
处理单元
918
922
I/O 接口
914
外部设备
924
显示器

图 9

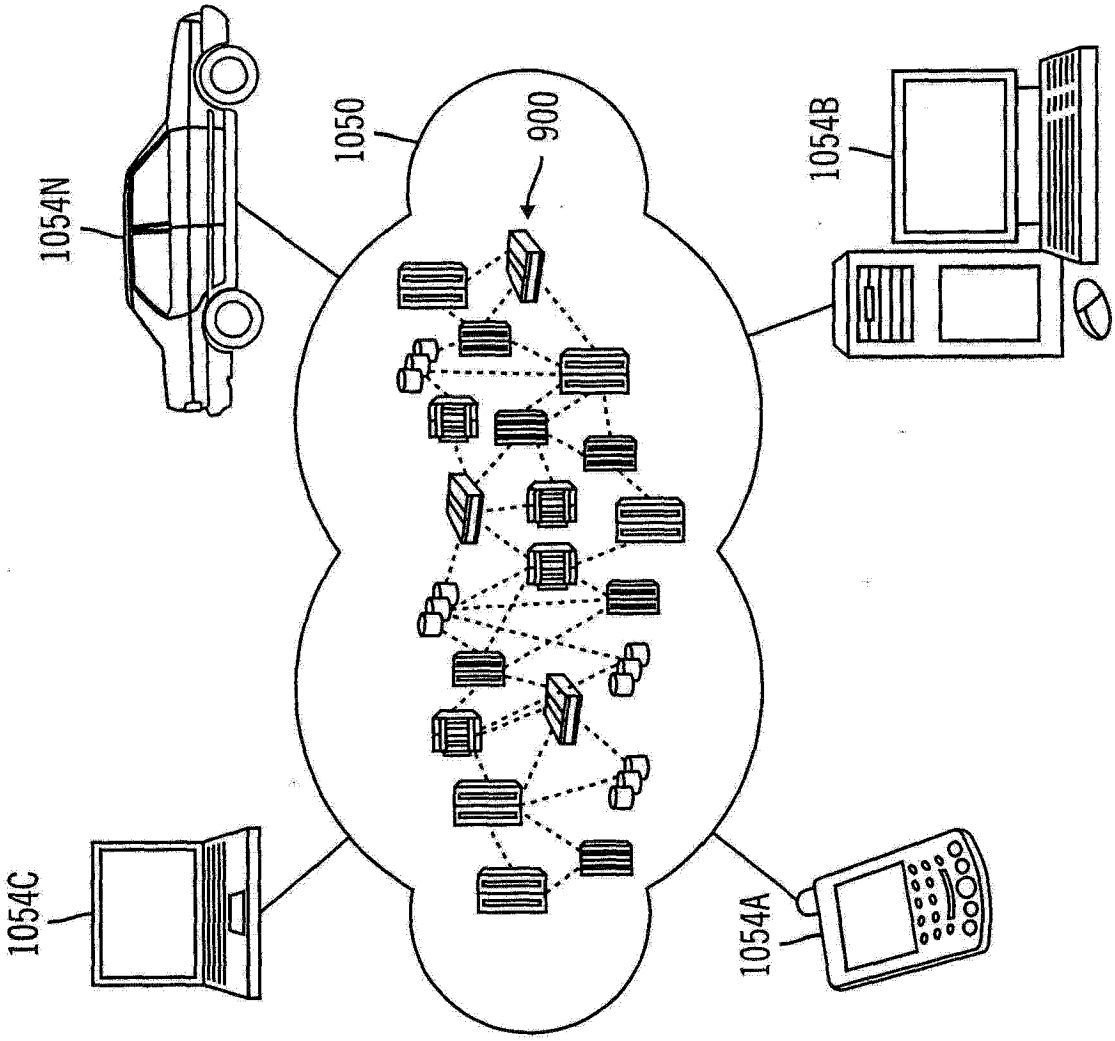


图 10

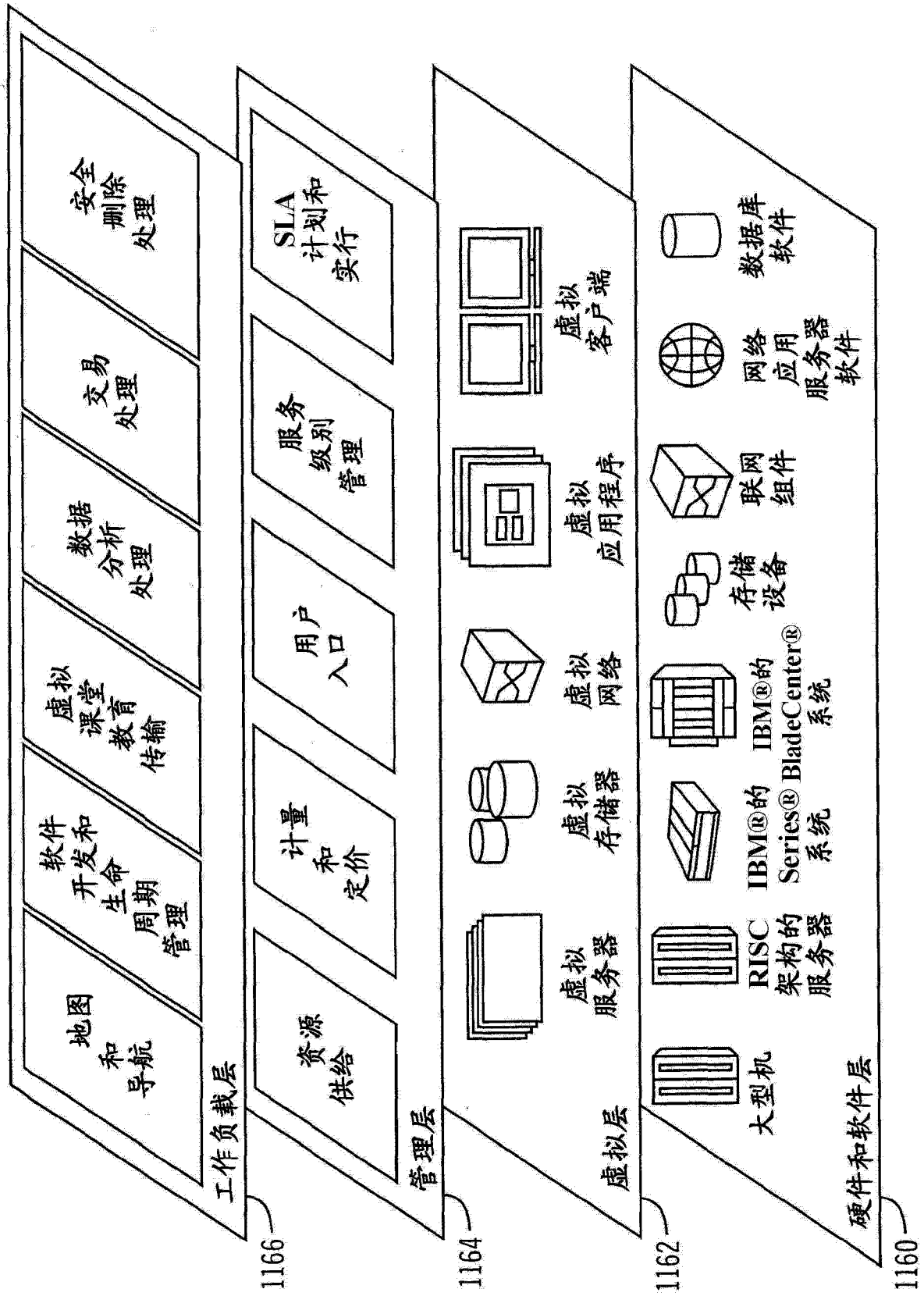

工作负载层
地图和导航
软件开发和生命周期管理
虚拟课堂教育传输
数据分析处理
交易处理
安全删除处理
1166
管理层
资源供给
计量和定价
用户入口
虚拟存储器
虚拟网络
虚拟应用程序
服务级别管理
SLA计划和实行
1164
虚拟层
虚拟服务器
RISC架构的服务器
IBM®的Series® BladeCenter®系统
存储设备
联网组件
虚拟客户端
网络应用服务器软件
数据库软件
1162
硬件和软件层
大型机
1160

图 11