

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 957 843**

51 Int. Cl.:

H04L 9/40 (2012.01)
H04L 45/302 (2012.01)
H04L 67/63 (2012.01)
G06F 9/50 (2006.01)
G06F 21/62 (2013.01)
G06Q 20/02 (2012.01)
G06Q 20/22 (2012.01)
G06Q 20/38 (2012.01)
G06Q 40/04 (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 86 Fecha de presentación y número de la solicitud internacional: **15.12.2015** **PCT/CA2015/000599**
87 Fecha y número de publicación internacional: **23.06.2016** **WO16095012**
96 Fecha de presentación y número de la solicitud europea: **15.12.2015** **E 15868754 (1)**
97 Fecha y número de publicación de la concesión europea: **07.06.2023** **EP 3234792**

54 Título: **Verificación de procesos de datos en una red de recursos informáticos**

30 Prioridad:

15.12.2014 US 201462091971 P
22.04.2015 US 201562151182 P

45 Fecha de publicación y mención en BOPI de la
traducción de la patente:
26.01.2024

73 Titular/es:

ROYAL BANK OF CANADA (100.0%)
1 Place Ville Marie 6th Floor North Wing
Montreal, QC H3C 3A9, CA

72 Inventor/es:

PITIO, WALTER MICHAEL;
IANNACCONE, PHILIP;
BROWN, JAMES;
BETTEN, JEFFREY ROY y
MORRIS, HEATHER GIUSEPPINA AIOSA

74 Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

ES 2 957 843 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Verificación de procesos de datos en una red de recursos informáticos

5 Campo

La presente descripción se refiere en general a sistemas, métodos, dispositivos y medios para la verificación o gestión de procesos de datos por diversos recursos informáticos en red. En modalidades particulares, la descripción se refiere a la verificación de procesos de datos que involucran sistemas o dispositivos intermedios.

10 Aspectos del material descrito en esta solicitud se refieren a la tenencia, transferencia y/o administración de valores y otros intereses financieros. Aspectos de dicha tenencia, transferencia y/o administración pueden estar sujetos a regulación por parte de organismos gubernamentales y otros. La presente descripción se realiza únicamente en términos de posibilidades lógicas, de programación y de comunicaciones, sin tener en cuenta consideraciones legales, estatutarias o reglamentarias. Nada de lo aquí expuesto tiene la intención de ser una declaración o representación de que cualquier sistema, método o proceso propuesto o discutido aquí, o su uso, cumple o no cumple con cualquier estatuto, ley, regulación u otro requisito legal en cualquier jurisdicción; ni debe ser interpretado como tal.

20 Introducción

En diversas formas de sistemas de procesamiento de datos en red o distribuidos, a menudo se enrutan procesos complejos y/o múltiples relacionados con órdenes de clientes a múltiples recursos informáticos para su distribución, difusión o ejecución.

25 Algunos de estos sistemas de procesamiento de datos distribuidos manejan simultáneamente grandes volúmenes de procesos de datos para numerosos clientes. Las instrucciones de diferentes clientes pueden implicar procesos de datos similares y pueden requerir que los procesos de datos se comuniquen y/o se ejecuten en recursos informáticos sin revelar ninguna información sobre el sistema cliente que dio las instrucciones originales.

30 En dicho entorno, verificar los procesos de datos relacionados para un cliente puede ser un desafío.

El documento US 2006/224431 muestra un sistema, método y producto de programa informático para el procesamiento de datos en la gestión de la cadena de suministro utilizando un sistema central de procesamiento de datos que integra una pluralidad de funcionalidades para la determinación de socios y sistemas, así como la verificación de disponibilidad. Al recibir una solicitud que incluye una pluralidad de artículos de un cliente, se generan identificadores únicos y se asignan en relación con los artículos del cliente en respuesta a la solicitud. Cada solicitud se divide en una pluralidad de subsolicitudes, donde cada subsolicitud se asigna a un sistema interno o externo mediante las reglas. En caso de que se utilice una comunicación sincrónica, la combinación dinámica de los subresultados se realiza en tiempo de ejecución. Si se emplea la comunicación asíncrona, las subrespuestas se agregan en una base de datos hasta que se hayan recibido todas las subrespuestas. La cantidad de recursos solicitados se ajusta en ambos casos en función de la información recibida del sistema central de procesamiento de datos.

45 El documento US 2008/040602 muestra sistemas y métodos para comunicar información médica sensible y/o confidencial mediante el uso de codificación. Se transmite una solicitud de datos médicos sensibles, donde la solicitud incluye una clave pública para codificación como un nodo XML. La clave pública puede ser utilizada por la parte que responde para cifrar al menos una parte de la respuesta y responder a la solicitud. La única parte en la ruta de la red que puede descifrar el mensaje es el originador de la solicitud, ya que el solicitante tendrá la clave privada que se requiere para descifrar los datos de respuesta.

50 Sumario

Aspectos de la presente descripción proporcionan sistemas, métodos y mecanismos de instrucciones ejecutables por ordenador (por ejemplo, estructuras de programación legibles por máquina no transitorias) como conjuntos de instrucciones codificadas en software y datos, para la gestión del procesamiento de datos por múltiples recursos informáticos en red.

En particular, por ejemplo, la presente descripción proporciona sistemas, métodos y conjuntos de instrucciones codificadas útiles para la verificación o monitoreo de órdenes o solicitudes enrutadas y/o en proceso de ser enrutadas para su procesamiento por diversos recursos informáticos en red.

La invención se define en las reivindicaciones independientes. Otras modalidades están definidas por las reivindicaciones dependientes.

65 Muchas otras características y combinaciones de las mismas con respecto a las modalidades descritas en este documento aparecerán para aquellos expertos en la materia después de leer la presente descripción.

Descripción de las figuras

En las figuras, se ilustran ejemplos de modalidades de la invención. Se entiende expresamente que la descripción y los dibujos son únicamente con fines ilustrativos y como ayuda para comprender, y no pretenden ser una definición de los límites de la invención.

Las Figuras 1A y 1B muestran aspectos de un sistema de ejemplo y flujo de trabajo para gestionar procesos de datos en una red de recursos informáticos.

La Figura 2 muestra aspectos de un sistema de ejemplo y flujo de trabajo para gestionar procesos de datos en una red de recursos informáticos.

La Figura 3 muestra un ejemplo de formato de registro.

La Figura 4 muestra aspectos de un sistema de ejemplo y flujo de trabajo para gestionar procesos de datos en una red de recursos informáticos.

La Figura 5 muestra aspectos de un sistema de ejemplo y flujo de trabajo para gestionar procesos de datos en una red de recursos informáticos.

La Figura 6 muestra aspectos de un sistema de ejemplo y flujo de trabajo para gestionar procesos de datos en una red de recursos informáticos.

La Figura 7 muestra aspectos de un sistema de ejemplo y flujo de trabajo para gestionar procesos de datos en una red de recursos informáticos donde se utilizan más de un sistema intermediario entre un instructor y un destino.

La Figura 8 muestra aspectos de un sistema de ejemplo y flujo de trabajo para gestionar procesos de datos en una red de recursos informáticos donde un sistema tiene múltiples sistemas internos en los que se pueden procesar órdenes.

La Figura 9 muestra aspectos de un sistema y flujo de trabajo de ejemplo para gestionar procesos de datos en una red de recursos informáticos donde un sistema tiene múltiples sistemas internos en los que se pueden procesar órdenes.

La Figura 10 es una tabla que ilustra un posible escenario donde se utiliza un esquema de módulo 7 (por ejemplo, donde se utiliza un divisor de 7 en el contexto de una operación de módulo) y 4 de las entidades estuvieron involucradas en el manejo del orden.

La Figura 11 es un esquema en bloque que muestra aspectos de un sistema o dispositivo de ejemplo.

La Figura 12 es un ejemplo de flujo de trabajo que muestra aspectos de un método de ejemplo desde una perspectiva intermedia.

La Figura 13 es un ejemplo de flujo de trabajo que muestra aspectos de un método de ejemplo desde la perspectiva de un supervisor.

La Figura 14 es un ejemplo de flujo de trabajo que muestra aspectos de un método de ejemplo desde la perspectiva de un instructor.

Descripción detallada

En un sistema de procesamiento de datos en red o distribuido, un dispositivo instructor puede enviar una solicitud de procesamiento de datos a un dispositivo intermediario para ejecutar la solicitud de procesamiento de datos en uno o más dispositivos de destino. Por ejemplo, en una modalidad, un dispositivo instructor puede enviar una solicitud para ejecutar una carga de trabajo informática a un administrador de recursos distribuidos para su ejecución en uno o más recursos distribuidos. En otro ejemplo, un dispositivo instructor puede enviar una solicitud para ejecutar una operación financiera a un dispositivo intermediario, como un intermediario electrónico, para su ejecución en uno o más dispositivos de negociación electrónica en red.

En algunas modalidades, los dispositivos intermediarios pueden hacer que la solicitud de procesamiento de datos del dispositivo instructivo se ejecute en cualquier número de recursos distribuidos de procesamiento de datos. En algunas situaciones, cuando los dispositivos intermediarios forman parte o comprenden sistemas independientes de los dispositivos clientes, los dispositivos intermediarios pueden tomar decisiones con respecto a la ejecución de la solicitud de procesamiento de datos del dispositivo instructivo sin ninguna supervisión directa del dispositivo cliente. En algunos casos, una entidad asociada con el dispositivo intermediario puede tener motivaciones diferentes o conflictivas en comparación con una entidad asociada con el dispositivo instructor. Por ejemplo, un administrador de recursos

distribuido que maneja cargas de trabajo de múltiples dispositivos instructores puede estar configurado para dividir los recursos de procesamiento de datos entre las cargas de trabajo de muchos dispositivos instructores, mientras que un dispositivo instructor en particular preferiría que todos los recursos estuvieran dedicados a las cargas de trabajo del dispositivo instructor.

De manera similar, un sistema intermediario electrónico puede beneficiarse de diferentes comisiones, reembolsos, ejecución de solicitudes de operaciones de dispositivos instructores preferidos o más rentables. Estas motivaciones pueden afectar la forma en que se configura un dispositivo intermedio para manejar solicitudes de procesamiento de datos que pueden no estar alineadas con las instrucciones o los mejores intereses de un dispositivo instructivo.

En términos generales, en algunas modalidades, la presente descripción proporciona sistemas, dispositivos, métodos y medios para verificar o gestionar de otra manera la ejecución de procesos de datos en una red de recursos informáticos. En algunos casos, esta verificación puede proporcionar una indicación sobre el rendimiento de un dispositivo intermediario en la ejecución de una solicitud de procesamiento de datos de un dispositivo instructivo y/o información relacionada con cómo el intermediario ha asignado y/o enrutado la solicitud a uno o más recursos informáticos.

En algunas modalidades, los aspectos de los sistemas, dispositivos, métodos y medios descritos aquí pueden proporcionar anonimato para la información relacionada con las solicitudes de procesamiento de datos de diferentes dispositivos instructores. En algunos casos, los aspectos de la presente descripción pueden reducir la probabilidad de que un tercero pueda obtener información relacionada con las solicitudes de procesamiento de datos desde un dispositivo instructor.

La Figura 1A muestra aspectos de un sistema de ejemplo 100A para verificar o gestionar procesos de datos en una red de recursos informáticos. En algunas modalidades, el sistema 100 puede incluir uno o más sistemas instructores, como los sistemas informáticos cliente 102 en la Figura 1A. Un sistema instructor puede incluir uno o más dispositivos instructores (sistemas informáticos cliente) configurados para transmitir una solicitud de procesamiento de datos (por ejemplo, una solicitud principal) a un segundo sistema (por ejemplo, sistemas informáticos de intermediario 104). La solicitud de procesamiento de datos puede, en algunos ejemplos, ser ejecutada por uno o más recursos informáticos (por ejemplo, lugares de comercio electrónico 108a..n).

En algunas modalidades, la solicitud de procesamiento de datos puede ser una solicitud u otro mensaje que incluye datos que incluyen uno o más parámetros o requisitos que definen el proceso de datos que el sistema instructor busca que se ejecute. El sistema instructor 102 también puede estar configurado para mantener un registro de transacciones (por ejemplo, almacenado dentro de una base de datos o en varios dispositivos de almacenamiento de datos legibles por ordenador).

El segundo sistema puede, en algunos ejemplos, ser un sistema intermediario configurado para recibir la solicitud de procesamiento de datos del sistema instructor; generar una o más solicitudes secundarias, cada una para ejecutar al menos una parte de la solicitud de procesamiento de datos recibida; y enrutar la(s) solicitud(es) secundaria(s) para su ejecución por uno o más recursos informáticos. En algunas modalidades, el sistema intermediario puede ser un intermediario electrónico, un sistema de gestión de recursos distribuidos, o cualquier otro sistema o dispositivo que pueda actuar como intermediario, agente, proxy o nodo para ejecutar la solicitud de procesamiento de datos.

Debe entenderse que el término "sistema", como se hace referencia, por ejemplo, a sistemas instructores, sistemas intermediarios, sistemas supervisores, sistemas informáticos clientes, sistemas informáticos intermediarios, etc., puede referirse a uno o más dispositivos, sistemas, enlaces de comunicación o alguna combinación de los mismos. En algunos ejemplos, un único dispositivo físico puede incluir aspectos de múltiples sistemas, por ejemplo, un único dispositivo informático puede ejecutar un proceso de datos para un primer sistema y también alojar un servidor para un segundo sistema.

Por el contrario, el término "dispositivo" o "servidor" puede referirse a un solo dispositivo, varios dispositivos, enlaces de comunicación, sistemas, procesos informáticos o cualquier combinación de los mismos.

Los términos "sistemas y dispositivos instructores", "intermediario" y "destino" se refieren a las relaciones entre los diversos componentes en el sistema general. Por ejemplo, un sistema informático intermediario 104 puede ser un sistema intermediario para un sistema informático instructor de cliente 102; sin embargo, para un proceso de múltiples saltos, el sistema informático intermediario 104 también puede ser un sistema instructor que envía una solicitud a un segundo sistema intermediario de intermediación. De manera similar, el segundo sistema intermediario puede ser un dispositivo de destino desde la perspectiva del sistema instructor, y también puede actuar como intermediario para el primer sistema intermediario.

En algunas modalidades, los sistemas y dispositivos instructores, intermediario, destino y supervisor pueden referirse a componentes electrónicos dentro de un solo sistema, como el sistema informático intermediario 104. Por ejemplo, como se describe aquí o de otra manera, el sistema informático intermediario puede incluir múltiples componentes

informáticos internos, como enrutadores inteligentes que pueden ser denominados sistemas/dispositivos instructores, intermediario, destino y/o supervisor.

5 Los aspectos de los sistemas y métodos descritos aquí pueden aplicarse en diversos campos, por ejemplo, el comercio financiero.

10 Por ejemplo, una solicitud de procesamiento de datos de comercio electrónico puede incluir identificador(es) de interés (como un identificador utilizado por una o más bolsas para identificar una acción, un Comité de Procedimientos de Identificación de Valores Uniformes (CUSIP), un conjunto de monedas a intercambiar, etc.), un valor de cantidad (por ejemplo, cantidades o volúmenes) de los intereses a ser transados (incluyendo, por ejemplo, cualquier cantidad total y/o de reserva), un tipo de ejecución (por ejemplo, comprar, vender, hacer una oferta, ofrecer, etc.) a ser ejecutado o solicitado, tiempo de vigencia (por ejemplo, válido hasta cancelación, inmediato o cancelar, llenar o matar) y los términos de precio correspondientes. En algunos ejemplos, la solicitud de procesamiento de datos puede incluir datos que indiquen requisitos y/o preferencias específicas para ejecutar el proceso de datos, como los recursos informáticos preferidos o requeridos para utilizar, límites en el número de procesos de datos secundarios que se pueden generar a partir de la solicitud original, instrucciones de enrutamiento, parámetros de tiempo y cualquier otra instrucción para ejecutar el proceso de datos y/o instruir a un sistema intermediario.

20 En otro ejemplo, una solicitud de procesamiento de datos de carga de trabajo puede ser enviada desde un sistema instructor a un sistema de gestión de recursos distribuidos intermediario para su ejecución en uno o más recursos distribuidos gestionados o accesibles por el sistema intermediario.

25 En otros ejemplos, los sistemas y métodos descritos aquí pueden aplicarse a otros campos donde las instrucciones/órdenes se envían entre varias entidades, y un instructor o intermediario general puede desear validar y/o verificar que dicho enrutamiento se haya llevado a cabo de manera consistente y/o en interés del instructor o intermediario. Si bien se describen varias modalidades en relación con el comercio financiero (por ejemplo, utilizando una terminología de clienteintermediariolugar), se pueden utilizar otras aplicaciones en donde una terminología de clienteintermediariodestino puede ser más aplicable. Por ejemplo, el cliente puede ser el "instructor" en este caso, y el intermediario/destinos pueden ser uno o más agentes del "instructor" que pueden llevar a cabo diversas tareas y/o dirigirse a otros agentes. Puede haber varios niveles de intermediarios, etc., como múltiples niveles de intermediarios y/o componentes de enrutamiento dentro de intermediarios individuales.

35 La información y/o instrucciones pueden ser proporcionadas en forma de procesos de datos, los cuales pueden ser enrutados a través de varios enlaces de comunicación, como una red de recursos informáticos en donde los recursos informáticos pueden estar configurados para realizar diversas funciones, por ejemplo, a través de la ejecución de instrucciones interpretables por máquina.

40 En el contexto de una aplicación de comercio financiero clienteintermediariolugar, el sistema puede comprender un sistema de cliente, un sistema intermediario, un sistema supervisor y uno o más lugares (recursos de procesamiento de datos para comercio financiero). Un sistema de cliente puede enviar una solicitud a un sistema intermediario para que ocurra una o más transacciones financieras. La solicitud del cliente puede ser denominada como una solicitud principal, la cual puede ser transmitida a un sistema intermediario, el cual puede estar configurado para proporcionar una o más solicitudes secundarias relacionadas para provocar el enrutamiento de una o más transacciones financieras.

45 La solicitud del cliente puede ser denominada como una solicitud principal, la cual puede ser transmitida a un sistema intermediario, el cual luego proporciona una o más solicitudes secundarias relacionadas para provocar el enrutamiento de una o más transacciones financieras.

50 El enrutamiento de una o más transacciones financieras puede llevarse a cabo en el contexto del procesamiento de una o más transacciones financieras por uno o más lugares. Puede haber solicitudes que sean, por ejemplo, ejecutadas, parcialmente completadas, canceladas, rechazadas, reconocidas, etc.

55 En algunas situaciones, un sistema instructor 102 y un sistema intermediario 104 pueden ser operados por diferentes entidades o configurados de otra manera para operar utilizando reglas basadas en intereses competitivos. Como el sistema intermediario 104 puede tener cierta discreción u opciones para enrutamiento de una solicitud principal para su ejecución por uno o más recursos informáticos.

60 Por ejemplo, cuando una solicitud principal incluye un proceso de datos relacionado con transacciones financieras, un sistema informático intermediario de intermediarios puede tener varias opciones disponibles para dirigir la solicitud para su ejecución o procesarla de otra manera. En algunas jurisdicciones, las regulaciones pueden estipular que los intermediarios deben dirigir las órdenes de los clientes teniendo en cuenta los intereses del cliente (por ejemplo, obtener el mejor precio para el cliente) y los intermediarios deben seguir las instrucciones explícitas de enrutamiento de los clientes (por ejemplo, mejor precio, mejor ejecución, el uso de técnicas de enrutamiento de nivelación de latencia). Sin embargo, debido a la complejidad y anonimato incorporados en los sistemas actuales, la verificación de que se hayan seguido las instrucciones o los mejores intereses de un cliente es difícil o imposible. Además, en algunas

situaciones, las instrucciones del sistema instructor pueden cumplirse al mismo tiempo que se permite cierta discreción para el sistema intermediario.

En algunas situaciones, un sistema intermediario puede ser incentivado para dirigir órdenes de una manera que puede ser beneficiosa para el intermediario, pero puede no ser óptima para el interés del instructor. Por ejemplo, uno o más recursos informáticos de negociación financiera pueden estar asociados con intercambios que ofrecen reembolsos y/o otros incentivos a los intermediarios para ejecutar operaciones en su intercambio. En este escenario, se puede incentivar a un sistema intermediario para que enrute al menos una parte de una solicitud a un recurso informático para recopilar un reembolso ofrecido por la bolsa correspondiente.

En algunos otros escenarios, un sistema intermediarios puede enrutar órdenes a otros intermediarios y recibir pagos adicionales al vender el flujo de órdenes a diversas empresas de comercio. Por ejemplo, algunos lugares ofrecen un reembolso para aumentar los volúmenes de negociación e implementan esquemas de reembolso como un sistema "fabricantetomador". Se puede proporcionar un descuento a un intermediario por "fabricar" un mercado, y, por el contrario, se puede cobrar una tarifa a un intermediario por "tomar" un mercado. Se pueden contemplar otros esquemas de descuento.

Un conflicto potencial puede surgir cuando un intermediario tiene la opción de dirigir una solicitud de procesamiento a un recurso informático que ofrece un reembolso, pero el recurso informático que ofrece el reembolso puede no proporcionar la mejor ejecución para el instructor. También se pueden contemplar otros conflictos (por ejemplo, intermediarios que delegan órdenes de manera subóptima a otros intermediarios, o que lo hacen de manera ineficiente).

Por ejemplo, un intermediario que proporciona descuentos en recursos informáticos puede tener tiempos de ejecución largos o latencias, tasas de llenado más bajas o ser más propenso a ser objeto de operadores predatorios (por ejemplo, de alta frecuencia).

La metodología específica y/o el rendimiento de un intermediario en particular también pueden ser importantes para un cliente. Por ejemplo, un cliente puede desear comparar el rendimiento de un intermediario con otro, optando por proporcionar más órdenes al intermediario que parece tener un rendimiento más sólido que otro intermediario.

Como la solicitud de un instructor puede ser enviada a través de múltiples sistemas intermediarios, puede involucrar muchos componentes de enrutamiento independientes y recursos informáticos, y la generación de varias solicitudes secundarias y terciarias, puede ser difícil o imposible ver, verificar, validar, gestionar o monitorear el enrutamiento de una solicitud del cliente. Además, puede ser difícil determinar si el precio/cantidad resultante obtenido a petición del cliente fue favorable para el cliente en vista de las condiciones del mercado prevalecientes, si el sistema intermediario cumplió con los estándares de rendimiento o si el intermediario siguió las instrucciones establecidas por la solicitud del cliente.

Otro factor en la gestión o monitoreo de recursos informáticos en red es la capacidad de mantener la confidencialidad del procesamiento de datos de un sistema instructor en relación con terceros. Por ejemplo, la relación entre las órdenes de los intermediarios y las órdenes de los clientes puede ser utilizada por un tercero para determinar varias características y/o aspectos de las órdenes, incluyendo la identidad de las partes, información sobre las solicitudes de operaciones, algoritmos utilizados, cómo se dividen y se dirigen las órdenes, la relación entre las órdenes, etc. La filtración de esta información puede tener impactos perjudiciales potenciales en las tasas de llenado y en la efectividad futura de la estrategia de enrutamiento y/o algoritmo, ya que la tercera parte podría realizar operaciones oportunísticas basadas en esta información. Los clientes pueden ser particularmente sensibles a cualquier filtración de estrategia de cartera o posición.

En términos generales, en algunas modalidades, la presente descripción proporciona sistemas, dispositivos, métodos y medios para verificar o gestionar de otra manera la ejecución de procesos de datos en una red de recursos informáticos. En algunos casos, esta verificación puede proporcionar una indicación sobre el rendimiento de un dispositivo intermediario en la ejecución de una solicitud de procesamiento de datos de un dispositivo instructivo y/o información relacionada con cómo el intermediario ha asignado y/o enrutado la solicitud a uno o más recursos informáticos.

En algunas modalidades, los aspectos de los sistemas, dispositivos, métodos y medios descritos aquí pueden proporcionar anonimato para la información relacionada con las solicitudes de procesamiento de datos de diferentes dispositivos instructores. En algunos casos, los aspectos de la presente descripción pueden reducir la probabilidad de que un tercero pueda obtener información relacionada con las solicitudes de procesamiento de datos desde un dispositivo instructor.

Aspectos de algunas modalidades pueden implicar la configuración y/o provisión de un sistema informatizado para supervisar el enrutamiento de órdenes, donde la función de supervisión puede llevarse a cabo mediante el uso de una o más claves que pueden estar asociadas con las órdenes enrutadas.

Estas una o más claves pueden estar aseguradas, codificadas, truncadas u ocultas de alguna otra manera de modo que las claves no afecten la confidencialidad de la solicitud o la información asociada a las solicitudes. En algunas modalidades, las claves pueden ser utilizadas para codificar datos de solicitud y metadatos.

Con referencia a la Figura 1A, un sistema instructor como el sistema informático cliente 102 incluye uno o más procesadores que pueden estar distribuidos en uno o más dispositivos. Los procesadores están configurados para transmitir a un sistema intermediario (como el sistema informático intermediario 104) una solicitud principal. La solicitud principal puede incluir al menos un proceso de datos principal que puede ser ejecutado por uno o más recursos informáticos (como lugares 108a..n).

En algunas modalidades, el procesador del instructor envía una clave instructora (CK) al sistema informático intermediario junto con la solicitud principal. La clave instructora y la solicitud principal pueden ser enviadas en el mismo mensaje. Por ejemplo, la clave instructora puede ser una etiqueta o un valor almacenado en un encabezado u otro campo asociado con el mensaje de solicitud principal. En otro ejemplo, la clave instructora y la solicitud principal pueden enviarse en varios mensajes utilizando cualquier mecanismo en el que el sistema informático intermediario pueda correlacionar los dos.

En algunos ejemplos, la clave instructora (CK) puede generarse de cualquier manera como se describe aquí o de otra forma. En algunas modalidades, la clave instructora (CK) puede ser única para la solicitud principal particular, generándose diferentes claves instructoras para diferentes solicitudes y para enviar a diferentes dispositivos intermediarios.

El sistema intermediario, como el sistema informático intermediario 104, puede incluir uno o más procesadores que pueden estar distribuidos en uno o más dispositivos. Los procesadores están configurados para recibir la solicitud principal y la clave instructora CK.

Los procesadores del sistema intermediario generan una o más solicitudes secundarias para enrutamiento hacia uno o más dispositivos de destino. Las solicitudes secundarias incluyen proceso de datos secundario para ejecutar al menos una parte del proceso de datos principal. Por ejemplo, una solicitud principal puede incluir un proceso de datos para ejecutar una transacción de 10 000 acciones de la acción ABC, y los procesadores pueden generar múltiples solicitudes secundarias para ejecutar porciones de las 10 000 acciones en diferentes dispositivos de destino (como recursos informáticos en bolsas de valores, otros intermediarios, mercados opacos, etc.). En otro ejemplo, una solicitud principal puede incluir un proceso de datos para calcular 10 mil millones de operaciones, y los procesadores pueden generar múltiples solicitudes secundarias para ejecutar porciones de las 10 mil millones de operaciones en diferentes dispositivos de destino (como recursos de computación compartidos o distribuidos, u otros servidores de computación en la nube o sistemas de gestión de recursos distribuidos). Cada solicitud secundaria puede incluir o estar asociada de otra manera con la clave instructora CK.

Los procesadores intermediarios están configurados para dirigir cada solicitud secundaria a un dispositivo de destino correspondiente 108 en conjunto con la clave instructora CK (que, en este ejemplo, también puede ser referida como clave de destino).

El sistema 100A incluye un servidor o sistema supervisor 190 que obtiene las solicitudes secundarias a través del enrutamiento de las solicitudes secundarias desde el sistema intermediario 104 y los dispositivos de destino. El servidor supervisor puede obtener las solicitudes secundarias a través de uno o más dispositivos supervisores 106.

En algunos ejemplos, los dispositivos supervisores 106 pueden incluir uno o más dispositivos de escucha que están configurados para interceptar, escuchar, raspar o acceder de otra manera a las comunicaciones en una ruta entre el sistema intermediario 104 y los dispositivos de destino. Por ejemplo, los dispositivos de escucha pueden incluir analizadores de red, dispositivos de derivación, interceptores, monitores, recolectores, raspadores y similares, que pueden obtener datos de solicitudes secundarias de manera en tiempo real, retrasada y/o a granel. En algunos ejemplos, el dispositivo de escucha puede ser un dispositivo físico como un dispositivo de escucha en un enlace de comunicación físico. En otros ejemplos, el dispositivo de escucha puede ser un proceso ejecutándose en un procesador en un nodo de red que puede escuchar y transmitir copias de los datos de solicitud secundaria a un servidor supervisor 190. En algunas modalidades, el sistema supervisor recibe las interceptaciones de un dispositivo de escucha existente, y en algunas modalidades, el sistema supervisor incluye el dispositivo de escucha.

En algunos ejemplos, los dispositivos supervisores 106 pueden incluir un dispositivo intermediario o proxy que recibe solicitudes secundarias y las dirige tanto a los dispositivos de destino como al sistema supervisor 190.

En algunas modalidades, los dispositivos supervisores 106 pueden estar configurados para eliminar la información de clave secundaria o de destino de las órdenes secundarias, reformatear y/o aplicar cualquier instrucción de procesamiento intermedio del dispositivo intermediario o instructor antes de enviar la solicitud secundaria a los dispositivos de destino (por ejemplo, si el destino tiene requisitos estrictos sobre cómo se formatea y/o se proporciona la información, de manera que elementos adicionales de información harían que la información no cumpla con los

requisitos del destino (por ejemplo, un lugar que solo acepta mensajes con un esquema estricto y rechaza otros mensajes por estar malformados).

5 En algunas modalidades, los dispositivos de destino 106 pueden ser capaces de procesar, ignorar o manejar de otra manera la información clave de destino incluida en las órdenes secundarias, por lo que los dispositivos supervisores 106 pueden permitir que las solicitudes secundarias se enrutan a los dispositivos de destino 106 con las claves de destino intactas.

10 Si bien el servidor supervisor 190 se muestra como un sistema separado, en algunos ejemplos, el servidor supervisor 190 puede ser uno o más procesos o dispositivos que operan en un sistema intermediario y/o un dispositivo de destino. Por ejemplo, en algunas modalidades, el sistema supervisor puede ser un proceso (o dispositivo) que se ejecuta en el sistema intermediario y que escucha o maneja las solicitudes secundarias a medida que se están enrutando desde el sistema intermediario.

15 En otro ejemplo, el sistema supervisor puede incluir un proceso o dispositivo que opera en el dispositivo de destino, como un recurso informático de una bolsa de valores. En algunos ejemplos, los propios recursos informáticos, como los recursos informáticos de la bolsa de valores, pueden estar configurados para manejar claves de destino y pueden enviar tanto solicitudes secundarias como mensajes de respuesta al sistema supervisor junto con las claves de destino.

20 En algunos ejemplos, el sistema supervisor puede ser un sistema distribuido con componentes en o integrados de alguna otra manera con los sistemas del instructor, intermediario y destino.

25 El sistema supervisor 190 puede recibir y almacenar datos de solicitud secundarias y datos asociados con las solicitudes secundarias en uno o más dispositivos de almacenamiento de datos 110. En algunas modalidades, el sistema supervisor puede recopilar, recopilar, reformatear u procesar de otra manera los datos recibidos para que sean adecuados para su almacenamiento y acceso.

30 El sistema supervisor 190 almacena los datos de solicitud recibidos junto con la(s) clave(s) de destino correspondiente(s). Por ejemplo, en la Figura 1A, los datos asociados con cada solicitud secundaria 1..N se almacenan en conjunto con la clave de destino CK.

En algunas modalidades, los datos asociados con una solicitud secundaria pueden ser codificados con la clave de destino o algún derivado de la misma.

35 En algunas modalidades, además de los detalles de la solicitud secundaria (por ejemplo, la solicitud de procesar una orden de 100 acciones de ABC en el lugar 108a), los datos asociados con una solicitud secundaria también pueden incluir metadatos. En algunos ejemplos, los datos asociados con una solicitud secundaria pueden incluir uno o más registros de tiempo de cuándo la solicitud secundaria fue recibida/enviada/reenviada por el sistema supervisor.

40 En algunos ejemplos, los datos asociados con una solicitud secundaria pueden incluir un identificador para identificar un mecanismo mediante el cual los datos de la solicitud secundaria fueron obtenidos por el supervisor. Por ejemplo, el identificador puede indicar que los datos de la solicitud secundaria fueron obtenidos a través de un dispositivo de escucha o un dispositivo proxy. En algunos casos, el identificador puede proporcionar una indicación de si los datos de la solicitud secundaria se obtuvieron en tiempo real (por ejemplo, a través de un dispositivo de escucha) o con un posible retraso (por ejemplo, en lotes) para evaluar potencialmente la precisión de cualquier marca de tiempo.

45 En algunos casos, el identificador puede indicar si los datos de la solicitud secundaria fueron recibidos de forma independiente por el sistema supervisor (por ejemplo, mediante un dispositivo de escucha) o a través de una copia o mecanismo de entrega por parte del sistema intermediario. Esto puede, en algunos ejemplos, proporcionar una indicación sobre el nivel de confianza o el grado en que los datos tienen el potencial de ser manipulados por el dispositivo intermediario.

50 En algunos ejemplos, los metadatos asociados con una solicitud secundaria pueden incluir información de fecha/hora, tipo de transacción en la solicitud (por ejemplo, acciones, opciones, bonos, etc.), tipo de mensaje en la solicitud (por ejemplo, compra, venta, cotización, confirmación, etc.), información de protocolo, región, información necesaria para interpretar el mensaje o cualquier otra información para clasificar o que sea relevante para una solicitud.

55 En algunas modalidades, los datos de solicitud secundaria pueden incluir datos de uno o más mensajes de respuesta de los dispositivos de destino 108 asociados con las solicitudes secundarias correspondientes. Por ejemplo, los mensajes de respuesta pueden incluir confirmaciones, rechazos, ejecuciones, confirmaciones, órdenes abiertas, etc. En algunos ejemplos, los datos pueden incluir tasas de llenado, precios, volúmenes o cualquier otro dato adecuado para evaluar o monitorear la ejecución de una solicitud de procesamiento de datos.

60 El(los) procesador(es) del sistema supervisor se puede(n) configurar para comunicar los datos de solicitud secundaria almacenados a uno o más dispositivos solicitantes. En algunos ejemplos, los dispositivos solicitantes pueden estar asociados con un sistema instructor 102, un organismo regulador o cualquier otra entidad.

En algunas modalidades, el(los) procesador(es) del sistema supervisor puede(n) estar configurado(s) para difundir o de otra manera hacer que los datos de solicitud estén disponibles públicamente.

En algunas modalidades, el sistema supervisor puede ser configurado para enviar los datos de solicitud a los dispositivos solicitantes a medida que estén disponibles. En otras modalidades, el sistema supervisor puede configurarse para enviar datos solo cuando un dispositivo solicitante lo solicite explícitamente (pull). Combinaciones y variaciones de esto son posibles.

Para preservar la confidencialidad, en algunas modalidades, el sistema supervisor solo puede enviar datos de solicitud secundaria correspondientes a la(s) clave(s) de destino proporcionada(s) por el dispositivo solicitante.

En modalidades en las que el sistema supervisor codifica los datos de solicitud recibidos con las claves de destino correspondientes, el sistema supervisor puede transmitir o enviar de otra manera todos los datos codificados a cualquier número de dispositivos solicitantes. En algunas modalidades, los dispositivos solicitantes pueden decodificar únicamente los datos codificados correspondientes a una clave de destino que posee el dispositivo solicitante. Por ejemplo, el sistema instructor 102, que tiene almacenada la clave instructora CK y sabe que está asociada con la solicitud principal particular, puede identificar las partes de los datos codificados que están asociadas con las órdenes secundarias basándose en la orden principal, ya que son las únicas partes que pueden ser decodificadas exitosamente con la clave instructora CK.

En algunas modalidades, el sistema supervisor puede estar configurado para codificar únicamente partes de los datos asociados con una solicitud. Por ejemplo, los metadatos de la región o los metadatos del tipo de transacción pueden almacenarse sin cifrar. En algunos ejemplos, las porciones no codificadas de los datos pueden ser utilizadas como un parámetro que un dispositivo solicitante puede usar para reducir el conjunto de datos que se recibe en una solicitud.

Como se ilustra en este ejemplo y a lo largo de todo el documento, la presente descripción puede, en algunas modalidades, proporcionar procesos, sistemas e interacciones técnicas particulares entre sistemas que permiten un rastro virtual de migas de pan o clave(s) que pueden permitir el monitoreo o gestión de una solicitud principal y las solicitudes secundarias asociadas a medida que son asignadas por diferentes sistemas informáticos para su ejecución en un recurso informático.

Puede haber varias aproximaciones disponibles. Por ejemplo: (1) el cliente puede proporcionar una clave a un intermediario para su uso en relación con las órdenes del cliente, (2) un intermediario puede crear una clave para ser proporcionada de vuelta al cliente, y (3) un intermediario puede crear una clave específica del intermediario y utilizar una combinación de la clave específica del intermediario y la clave cliente para asegurar la información. En algunas modalidades, la clave cliente puede considerarse una "clave instructora", y el dispositivo informático del cliente puede considerarse el "dispositivo instructor".

El sistema de ejemplo 100A de la Figura 1A ilustra una posible modalidad que verifica la ruta de las solicitudes de los clientes. Sin embargo, como se ilustra en parte por la siguiente discusión, puede haber diferentes implementaciones técnicas que pueden tener diferentes compensaciones en términos de velocidad de procesamiento, requisitos computacionales, completitud de datos, niveles de confidencialidad entre los sistemas, etc.

Las consideraciones pueden incluir compensaciones entre la robustez del seguimiento (especialmente en topologías más complejas donde puede haber múltiples niveles de sistemas intermediarios o distribución de solicitudes principales entre componentes informáticos dentro de una entidad, por ejemplo, diferentes motores de enrutamiento dentro de un único sistema intermediario) y la necesidad de rendimiento computacional dentro de un umbral particular (por ejemplo, en un sistema de negociación donde los precios y las oportunidades de ejecución pueden ser fugaces, los retrasos de milisegundos en el procesamiento clave pueden no ser aceptables) y la interoperabilidad (por ejemplo, algunos intermediarios en una serie de intermediarios pueden estar configurados para interoperar con un supervisor, mientras que otros no).

Puede que no sea deseable revelar una relación entre un sistema instructor y las órdenes secundarias asociadas a su solicitud principal a un recurso informático (por ejemplo, de manera que un intercambio solo tenga conocimiento de qué órdenes provienen de un intermediario en particular, pero no sepa a qué sistema de cliente corresponde cada orden) o a un tercero. De manera similar, un sistema intermediario (por ejemplo, un sistema informático intermediario) puede no desear revelar a un destino cómo se enrutan y procesan las solicitudes principales a través de un enrutador de órdenes algorítmico o inteligente (SOR).

En algunas modalidades, un problema técnico a resolver puede incluir cómo gestionar los datos (o identificadores de los mismos) que viajan en un sistema informático en red de manera que no se exponga la identidad de un sistema instructor, el algoritmo de enrutamiento de un sistema intermediario o las relaciones entre las solicitudes secundarias, al mismo tiempo que se proporciona un supervisor (como se describe aquí) y/o un recurso informático para procesar o ejecutar las respectivas solicitudes secundarias, y al mismo tiempo que se permite al sistema instructor verificar las actividades del intermediario con respecto a una solicitud del instructor. Se debe evitar que terceros recuperen, reconstruyan o extraigan el historial de solicitudes y procesamiento de un instructor y/o intermediario. En un sistema

financiero, exponer los datos de solicitud puede suponer riesgos para la información propietaria y/o confidencial del instructor o del intermediario, como estrategias de negociación y/o enrutamiento, lugares preferidos, información de órdenes, etc.

- 5 Posibles ventajas asociadas con algunas modalidades pueden incluir la verificación de órdenes de clientes con una exposición mínima y/o reducida de identidades, actividades y/o estrategias; la verificación de solicitudes de instructores sin revelar en exceso estrategias y/o algoritmos intermediarios; y la capacidad de realizar verificación y/o correlación en un gran número de solicitudes de instructores.
- 10 Sin embargo, la verificación de las solicitudes del instructor de manera segura puede requerir un nivel de facilidad y conveniencia para implementar. Puede haber varias ventajas asociadas con la utilización de la infraestructura de comunicación existente y/o sin la necesidad de desplegar una infraestructura de seguridad significativa. Por ejemplo, en algunas modalidades, puede que no sea necesario un organismo de certificación.
- 15 Algunas modalidades descritas a lo largo de esta especificación pueden proporcionar arquitecturas, sistemas, métodos y/o productos de sistemas informáticos que pueden ofrecer algunos o todos los siguientes beneficios potenciales:
 - puede haber flexibilidad en la implementación y/o estructura de la arquitectura y el sistema, ya que las modalidades pueden ser adecuadas para su uso con diversas combinaciones y permutaciones de relaciones instructor/intermediario/destino;
 - 20 ▪ el uso de un registro de transacciones verificable que puede ser generado por un sistema supervisor que opera de forma independiente y que, en algunas modalidades, puede ser útil en varios aspectos, como responder a consultas de auditoría, revisiones automáticas y/o informes sobre características de enrutamiento de órdenes, etc.;
 - 25 ▪ algunas modalidades no requieren una integración significativa por parte de los recursos informáticos (por ejemplo, lugares de negociación financiera), lo cual puede ser importante dependiendo del número de destinos contemplados;
 - 30 ▪ algunas modalidades incluyen la integración mediante recursos informáticos, lo cual puede reducir/evitar la necesidad de implementar un sistema supervisor;
 - 35 ▪ varios métodos de codificación y/o codificación pueden ser adecuados para su uso, por ejemplo, firmas digitales, códigos simples, pares de codificación/clave básicos, el algoritmo RSA, generación de números pseudoaleatorios, etc., se pueden utilizar entre el cliente/intermediario/lugar;
 - 40 ▪ en algunas modalidades, los parámetros de las claves seguras han sido diseñados de tal manera que se garantiza la privacidad, (por ejemplo, en algunas modalidades, incluso si se utilizan funciones hash conocidas); y
 - 45 ▪ en algunas modalidades, los sistemas, arquitecturas y métodos descritos a lo largo de la especificación pueden ser desarrollados teniendo en cuenta la necesidad de tamaños de archivo manejables, complejidad computacional y/o tiempos de cálculo, con el fin de, por ejemplo, mantener comunicaciones manejables y/o seguridad computacionalmente factible (por ejemplo, los recursos están limitados por la cantidad de tiempo disponible y la potencia de procesamiento computacional; en algunos contextos, cada nano/microsegundo cuenta, mientras que en otros, puede ser importante que el procesamiento se realice de manera receptiva para garantizar la relevancia del análisis).
- 50 Los sistemas de instrucción pueden estar asociados con diversas entidades que pueden generar solicitudes, como clientes individuales, instituciones financieras, fondos de cobertura, fondos de pensiones, fondos soberanos, corporaciones, asociaciones, empresas individuales, inversores institucionales, etc.
- 55 Los sistemas intermediarios pueden estar asociados con varias entidades que pueden organizar una o más transacciones financieras basadas en órdenes de clientes, como un intermediario de bolsa, una firma de intermediario, un representante registrado, un asesor de inversiones, una casa de bolsa, un intermediario de valores, entre otros. Los sistemas informáticos intermediarios pueden enviar solicitudes a los dispositivos de destino directamente o indirectamente a través de otros sistemas intermediarios.
- 60 Los dispositivos de destino pueden incluir recursos informáticos que pueden estar asociados con diversas bolsas de valores, sistemas de negociación alternativos (ATS), mercados opacos, instalaciones de negociación multilateral, redes de cruce, bolsas nacionales, bolsas regionales, redes de comunicación electrónica, plataformas de distribuidores simples u otros lugares registrados o no registrados, etc.
- 65 En algunos ejemplos, la información de solicitud puede ser comunicada a través de una variedad de técnicas y/o protocolos, como el protocolo de Intercambio de Información Financiera (FIX), archivos de texto, archivos planos, archivos de base de datos, archivos binarios, cadenas de caracteres, etc. La información puede ser comunicada, por

ejemplo, utilizando varios protocolos propietarios y/o protocolos binarios, como los que se utilizan en los intercambios y/o lugares.

5 En algunas modalidades, los datos también pueden ser codificados antes de la comunicación para proporcionar otro nivel de seguridad. La arquitectura puede utilizar varios esquemas para cifrar datos, como pares de claves pública/privada, etc.

10 Debe entenderse que las variaciones de diferentes aspectos de los sistemas, dispositivos, métodos y medios de ejemplo descritos aquí pueden aplicarse, cuando corresponda, a cualquiera de las otras modalidades en cualquier permutación o combinación.

La Figura 1B muestra aspectos de otro ejemplo de sistema 100B y flujo de datos para gestionar procesos de datos en una red de recursos informáticos.

15 Similar al ejemplo de la Figura 1A, en la Figura 1B, un sistema instructor 102 envía una solicitud principal a un sistema intermediario 104 junto con una clave instructora CK_1 . Sin embargo, en lugar de generar solicitudes secundarias con la misma clave de destino CK como se muestra en la Figura 1A, el sistema intermediario 104 en la Figura 1B selecciona una secuencia de claves de destino ($CK_1 \dots CK_N$) y asocia cada clave de destino con una de las solicitudes secundarias.

20 En algunas modalidades, seleccionar la secuencia de claves de destino puede incluir generar las segundas y siguientes claves de destino en la secuencia aplicando una función de codificación como una función hash $hf()$ a la clave anterior en la secuencia.

25 De esta manera, los datos asociados con cada solicitud secundaria se almacenan y/o codifican con una clave de destino diferente pero relacionada.

30 En algunas modalidades, cualquiera de las funciones de codificación descritas o ilustradas aquí (por ejemplo, hf_1 , hf_2 , hf_3) puede incluir cualquier función o algoritmo que genere una cadena pseudoaleatoria basada en una entrada de manera que la misma entrada resulte en la misma salida de cadena pseudoaleatoria. Al aplicar repetidamente la función de codificación a la salida de la cadena pseudoaleatoria, se puede generar o regenerar una secuencia de claves. En algunos ejemplos, la función de codificación puede producir una salida con una longitud definida basada en cualquier entrada.

35 Un dispositivo solicitante, como el sistema instructor 102, puede acceder y/o decodificar cada solicitud secundaria recreando la secuencia de claves de destino aplicando la misma función de codificación utilizada por el dispositivo intermediario a la clave instructora que envió junto con la solicitud principal.

40 Para identificar los datos de solicitud secundaria asociados con la solicitud principal, el sistema instructor puede enviar solicitud(es) que incluyan cada una de las claves de destino recreadas para recibir un conjunto de datos que incluya los datos de solicitud secundaria correspondientes a esas claves. Alternativamente o adicionalmente, el dispositivo solicitante puede intentar decodificar un conjunto de datos públicos o más ampliamente disponibles del sistema supervisor utilizando las claves de destino recreadas y las porciones decodificadas exitosamente asociadas con la solicitud principal.

45 Dado que el dispositivo solicitante puede no saber cuántas solicitudes secundarias fueron generadas por el dispositivo intermediario, el dispositivo solicitante puede configurarse para continuar solicitando y/o decodificando conjuntos de datos asociados con claves de destino adicionales en la secuencia hasta que se contabilice toda la solicitud de procesamiento de datos principal.

50 En algunos casos, la aplicación de diferentes claves de destino puede oscurecer la relación entre las solicitudes secundarias a los dispositivos de destino y/o terceros que acceden a los datos desde el sistema supervisor.

55 En otras modalidades, se pueden utilizar otras técnicas de selección de clave de destino. Por ejemplo, en lugar de una función hash que se comparte o se conoce comúnmente entre el instructor y los sistemas intermediarios, en algunas modalidades, los dos sistemas pueden compartir un generador de números aleatorios o un conjunto de números aleatorios, y las claves de destino pueden generarse en función de una semilla o índice comunicado con la solicitud principal.

60 Otros mecanismos mediante los cuales las claves parecen no estar correlacionadas con un tercero, pero pueden ser utilizadas por el intermediario y/o instructor para identificar o generar claves relacionadas, pueden ser utilizados.

65 En algunas modalidades, las claves pueden generarse utilizando diversas técnicas, como técnicas criptográficas, funciones de hash, pares de claves de codificación, individualmente o en combinación. En algunas modalidades, las claves se generan utilizando diversas combinaciones y/o permutaciones de diferentes técnicas, junto con la aplicación de diversas técnicas adicionales de ofuscación, como el relleno, el salado, etc.

Las claves (por ejemplo, "migas de pan" o secuencias aleatorias de símbolos) y/o técnicas de codificación/codificación, en algunas modalidades, pueden tener una codificación en cascada y/o secuencial sucesiva (por ejemplo, "derivados" derivados) realizada sobre ellas de manera que se puedan utilizar ventajosamente propiedades de codificación en capas. Por ejemplo, una clave "semilla" particular puede ser recodificada (por ejemplo, rehaseada) con una función de codificación repetidamente para generar varias claves relacionadas que serían difíciles de reproducir para un tercero sin conocer la "semilla" o una clave dentro de la cadena de claves, y/o la técnica de codificación utilizada (y las técnicas de sal/relleno correspondientes). De manera similar, más de una clave puede combinarse para crear "claves secundarias" a partir de más de una clave "semilla" en cada nivel, lo que dificulta aún más la capacidad de terceros para identificar asociaciones. Tales claves pueden considerarse "claves de indexado", y por ejemplo, pueden generarse utilizando una "clave instructora" (por ejemplo, una clave proporcionada por un cliente) y una "clave intermediaria" (por ejemplo, una clave proporcionada por un intermediario).

En algunas modalidades, las claves de destino pueden, por ejemplo, establecerse seleccionando (y/o generando) una secuencia de claves de un conjunto de claves disponibles, seleccionadas en base a una metodología y/o método particular. Tal metodología y/o método pueden, en algunas modalidades, ser compartidos entre un sistema supervisor, un dispositivo instructor (por ejemplo, un dispositivo cliente), dispositivos intermediarios, etc.

Las técnicas criptográficas utilizadas incluyen tanto el codificación como el uso de funciones hash seguras. Varias funciones unidireccionales y/o bidireccionales pueden ser utilizadas, por ejemplo, en algunas modalidades, el texto codificación puede ser procesado para derivar la cadena de origen, mientras que en otras modalidades, el texto codificación no puede ser utilizado para derivar la cadena de origen (por ejemplo, una función hash unidireccional, donde los intentos de revertir la función hash a partir de un resultado como una suma de comprobación pueden producir uno o más resultados colisionantes). Como ejemplos, las funciones criptográficas pueden incluir algoritmos de hash seguros (SHA), el algoritmo de resumen de mensajes (MD), etc.

La selección de una técnica criptográfica puede ser importante dependiendo del número de posibles entradas esperadas y salidas requeridas. Por ejemplo, las colisiones de hash pueden llevar a resultados de verificación inexactos o a procesamiento adicional.

Las claves pueden estar compuestas, por ejemplo, por una serie de códigos (por ejemplo, números aleatorios) que pueden ser pregenerados y compartidos entre un cliente y un intermediario. El intermediario puede asociar una orden de salida o un conjunto de instrucciones que es generado por el intermediario utilizando el código de acuerdo con su diseño. En algunas modalidades, el código es simplemente un conjunto de números generados predefinidos que se comparten entre un intermediario y un cliente. Los números pueden ser aleatorios (por ejemplo, ambas partes pueden compartir libros de códigos) elegidos en base a un codificación y/o algoritmo matemático, etc., y proporcionados en forma de tabla de búsqueda. Una posible debilidad con este enfoque puede ser la facilidad de descodificación y/o acceso malicioso en vista de las técnicas modernas de descodificación de códigos y de predicción de códigos (por ejemplo, un ataque de fuerza bruta utilizando un diccionario). Sin embargo, las claves pregeneradas pueden reducir los tiempos de cálculo necesarios para seleccionar/generar claves de destino. No es raro que una solicitud principal se divida en miles de solicitudes secundarias, y la generación secuencial de claves de destino sobre la marcha puede resultar en retrasos que no son aceptables, especialmente para solicitudes de procesamiento de datos sensibles al tiempo, como solicitudes de operaciones financieras. Para aumentar la seguridad, las secuencias de claves pregeneradas pueden ser cambiadas periódicamente, y la generación de estas claves puede, en algunas modalidades, ser realizada en momentos u horas de menor actividad cuando las solicitudes de comercio no son procesadas.

En algunas modalidades, el sistema 100B puede utilizar una única clave maestra CK inicial por instructor y continuar utilizando claves subsiguientes en la secuencia de CK maestra para órdenes subsiguientes. En algunas modalidades, ese sistema 100B puede utilizar un CK separado por cada solicitud principal. Con el fin de reducir la cantidad de tráfico de datos entre el instructor y el intermediario, solo se puede comunicar un único CK entre los sistemas del instructor y el intermediario, a partir del cual el sistema receptor puede determinar todas las claves secundarias. En algunos ejemplos, el sistema intermediario también puede comunicar al sistema instructor una cantidad de solicitudes secundarias que se generaron para una solicitud principal, de modo que el sistema instructor pueda determinar cuántas claves secundarias volver a crear y/o cuántas solicitudes secundarias identificar en un conjunto de datos del sistema supervisor para la verificación de enrutamiento.

En otra modalidad, un sistema instructor puede enviar una solicitud principal junto con una secuencia de claves instructoras pregeneradas para su uso en la selección de claves de destino. En algunos casos, esto puede reducir o eliminar el tiempo de procesamiento requerido por el sistema intermediario para generar claves de destino, lo cual puede mejorar los tiempos de procesamiento y potencialmente mejorar los resultados de los procesos de datos ejecutados.

En algunas modalidades, donde se reduce o no se emplea el anonimato, las claves pueden estar disponibles públicamente o compartidas con terceros particulares, como en el caso en que se requiera o se desee la supervisión de terceros, la supervisión del gerente del intermediario u otro gerente, o la supervisión pública del enrutamiento de solicitudes.

Un sistema instructor 102 puede estar configurado para recibir los datos de solicitud del sistema supervisor, descifrar los datos y/o correlacionar los datos con los datos de solicitud principal mantenidos en el registro de transacciones o solicitudes del sistema instructor (por ejemplo, en la base de datos). La correlación con datos y solicitudes principales puede incluir la determinación de relaciones entre varias solicitudes secundarias y/o entre solicitudes principales y solicitudes secundarias.

En algunas modalidades, el sistema instructor puede estar configurado para determinar si las solicitudes secundarias enviadas por los sistemas intermediarios 104 se enrutaron de acuerdo con una o más instrucciones de enrutamiento, o de acuerdo con condiciones para la mejor ejecución de la orden en relación con las condiciones del mercado prevalecientes en el momento de la orden.

En algunas modalidades, el sistema instructor 102 puede incluir uno o más dispositivos o procesadores configurados para gestionar las solicitudes de procesamiento de datos. Por ejemplo, los procesadores pueden, independientemente de cualquier entrada de un usuario del sistema instructor, generar/seleccionar claves instructora para enviar con las solicitudes principales, acceder a datos del sistema supervisor, asociar datos de solicitudes secundarias con las solicitudes principales basándose en las claves instructora y generar informes de verificación. Por ejemplo, el sistema instructor 102 puede incluir una aplicación de software o un dispositivo físico que puede realizar estas funciones de forma independiente o de manera transparente a un sistema instructor tradicional.

En algunas modalidades, puede que no haya un componente supervisor separado. Más bien, los sistemas informáticos de destino 108 (como los lugares 108a..n) pueden estar configurados para proporcionar datos de órdenes secundarias (por ejemplo, datos de mercado, instrucciones de órdenes) codificados utilizando una o más claves de destino. Los sistemas informáticos de destino 108 pueden configurarse para comunicar la información a los sistemas instructores 102. Por ejemplo, los sistemas informáticos de un intercambio pueden estar configurados para publicar públicamente todas las transacciones (incluyendo órdenes, cancelaciones, reemplazos y ejecuciones), y también para codificar las transacciones con las claves correspondientes recibidas del intermediario. Los sistemas instructores pueden acceder a las transacciones publicadas de forma pública, descifrarlas utilizando el conjunto de claves del sistema instructor y/o identificar todas las transacciones relacionadas con el instructor.

Algunas modalidades pueden incentivar a varios participantes en el desempeño de sus respectivos roles, por ejemplo, un instructor puede generar claves para verificar que un intermediario esté realizando las acciones especificadas (puede utilizarse para verificar no solo lugares, sino también cualquier otra directiva de orden). Un instructor puede, por ejemplo, utilizar el sistema de forma individualizada y/o incluir solicitudes en las que los instructores indiquen si deben utilizar o en qué medida utilizar las funciones de supervisión del sistema 100A.

Con respecto a los intermediarios, la negativa a generar las secuencias clave y asignarlas a las solicitudes puede ser percibida por los instructores como una admisión de no seguir las directivas del instructor y podría resultar en la pérdida del flujo de solicitudes/órdenes. Los intermediarios que pueden ser objeto de auditorías por violaciones regulatorias pueden potencialmente utilizar el sistema para ayudar a cumplir con los requisitos regulatorios y de auditoría. Con respecto a los recursos informáticos de destino, puede haber algunos lugares que deseen proporcionar capacidades a sus clientes para poder verificar que las solicitudes que se suponía que debían ser enviadas al lugar por el instructor fueron enrutadas correctamente por el intermediario.

El sistema puede ser implementado de varias formas, como una implementación basada en un proxy de red, en la cual un proxy de red del lado del instructor puede ser configurado para seleccionar un BK₀ y generar confirmaciones (ACK), y/o un proxy de red del lado del destino/ubicación que puede ser configurado para generar un DK/AI a partir de claves (por ejemplo, una clave cliente y/o varias claves de intermediarios) que recibe e inserta en la etiqueta saliente.

El sistema puede ser utilizado en conjunto con varios sistemas que pueden ser configurados para proporcionar diversas funcionalidades de enrutamiento, como el tiempo de orden o algoritmos de enrutamiento inteligente. En algunos ejemplos, los instructores pueden incluir instrucciones para el uso de dichas funciones en sus solicitudes principales.

Aunque se describe en el contexto de validar que las órdenes secundarias se ejecutaron de acuerdo con las mejores prácticas de ejecución con respecto al cliente, algunas modalidades también pueden proporcionar validación o verificación de que los términos de ejecución de las órdenes favorecieron a una parte distinta o además del cliente. Los términos de ejecución que favorecen a una o más de las partes pueden incluir al menos una de las oportunidades para que la respectiva parte reciba un precio mejor que el cotizado actualmente, la rapidez de ejecución y la probabilidad de que se realice la operación.

La Figura 2 muestra aspectos de otro ejemplo de sistema 200 y la gestión del flujo de datos en un conjunto de recursos informáticos en red.

La arquitectura de ejemplo en la Figura 2 puede potencialmente proporcionar un nivel adicional de seguridad que puede ser utilizado por el intermediario para aumentar el anonimato de las solicitudes a nivel de destino. En algunas

modalidades, esto puede tener en cuenta las posibles claves instructoras débiles que son seleccionadas por los sistemas instructores.

Los sistemas intermediarios 104 pueden estar configurados para asignar una clave intermediaria (BK_1) a cada solicitud principal y comunicar esa clave intermediaria a los sistemas instructores 102 (por ejemplo, junto con una comunicación en reconocimiento de una solicitud principal).

Similar a la selección de claves basada en la clave instructora como se describe anteriormente y aquí, los sistemas intermediarios 104 pueden estar configurados para seleccionar una secuencia de claves intermedias basadas en una función de codificación como una función hash.

En algunas modalidades, el sistema intermediario puede seleccionar una clave intermediaria ($BK_1, \dots, BK_N$) para cada solicitud secundaria que genera. Cada clave intermediaria puede ser fusionada con la clave instructora (CK_1) recibida junto con la solicitud principal utilizando una función de fusión. Los resultados de las fusiones se convierten en las claves de destino ($DK_1, \dots, DK_N$) para el enrutamiento con las respectivas solicitudes secundarias. En algunos ejemplos, cualquiera de las funciones de fusión descritas aquí puede ser una función XOR, una concatenación, una función hash o cualquier otra función para codificar dos claves juntas. En algunos ejemplos, las funciones de fusión descritas aquí pueden simplemente agregar o mezclar porciones de las dos claves juntas para formar una única clave fusionada.

Para identificar los datos de solicitud del servidor supervisor que están asociados con una solicitud principal, el dispositivo instructor/solicitante genera una secuencia de claves de destino basada en la clave instructora de la solicitud principal y la clave intermedia recibida del sistema intermediario. Con esta secuencia, el dispositivo instructor/solicitante puede intentar acceder y/o decodificar los datos del servidor supervisor hasta que se hayan identificado las solicitudes secundarias correspondientes a la solicitud principal.

En otras modalidades, las claves instructora de una secuencia de claves instructora pueden fusionarse con claves intermedias de una secuencia de claves intermedias para generar claves de destino. Por el contrario, en algunas modalidades, una única clave intermediaria puede fusionarse con cada una de una secuencia de claves instructoras para generar claves de destino.

En algunos ejemplos, la fusión de dos claves como se ilustra en el ejemplo de la Figura 2 puede disminuir la vulnerabilidad, ya que se deben comprometer múltiples claves y/o sus funciones de generación (por ejemplo, hf_2 y hf_3) para recrear las claves de destino.

Además, la arquitectura de ejemplo de la Figura 2 también puede evitar la exposición de la secuencia de solicitudes secundarias pertenecientes a una única solicitud del instructor, lo que potencialmente reduce la exposición de los algoritmos de intermediación y las técnicas de enrutamiento de órdenes inteligentes (SOR) a los sistemas de destino o supervisión.

La Figura 4 muestra otro ejemplo de sistema 400 en el cual una clave instructora no es generada ni comunicada por el dispositivo instructor al dispositivo intermediario. En cambio, el sistema intermediario 104 puede generar una clave instructora (BK_1) y comunicarla al sistema instructor en un mensaje de confirmación o de otra manera. El proceso/sistema luego funcionará de manera similar al sistema en la Figura 1B, con el sistema instructor configurado para acceder y/o decodificar los datos de solicitud secundaria asociados con la solicitud principal utilizando la clave instructora/destino (BK_1) recibida del sistema intermediario o derivados de la misma (por ejemplo, hashes de la clave original del instructor/destino para obtener claves subsiguientes en la secuencia).

Como el cálculo de las claves secundarias/derivadas puede requerir recursos computacionales significativos, en algunas modalidades, las claves pueden ser precalculadas. Por ejemplo, en algunas modalidades según se describe aquí o de otra manera, se pueden generar y compartir secuencias de claves entre sistemas instructores e intermediario antes de cualquier procesamiento de solicitud principal.

De manera similar, en algunas modalidades, series de claves iniciales de instructor (CK_1) pueden ser comunicadas entre el instructor y los sistemas intermediarios al inicio o al final del día o de otra manera antes de las órdenes reales, con las cuales el sistema intermediario puede ser configurado para precalcular series de CK_{N+1} y almacenarlas para su rápida recuperación.

Como se describe en los ejemplos de la Figura 2, en algunas modalidades, las secuencias de claves instructoras (CK_{N+1}) pueden no ser utilizadas para generar claves de destino. En cambio, una única clave instructora (CK) puede fusionarse con una serie de claves intermedias (BK_N) utilizando una función de fusión como la función hash $hf_1()$ para generar una serie de claves de destino (por ejemplo, $DK_{N+1} = hf_1(CK, BK_N)$). En estas modalidades, dado que las claves intermedias (BK_N) no dependen de la clave instructora del sistema instructor, el sistema intermedio puede configurarse para precalcular secuencias de claves intermedias de antemano.

La Figura 5 muestra otro ejemplo de sistema 500 en el cual una clave instructora no es generada ni comunicada por el dispositivo instructor al dispositivo intermediario. En esta modalidad de ejemplo, similar a los ejemplos de la Figura 4,

el sistema instructor está configurado para enviar una solicitud principal al sistema intermediario sin una clave. El sistema intermediario está configurado para seleccionar tanto una clave instructora (CK) como una secuencia de claves intermediarias (BK_N) con las cuales se puede generar una secuencia de claves de destino mediante una función de fusión. La clave instructora (CK) y al menos una clave intermediaria inicial (BK₁) se comunican de vuelta al sistema instructor en un acuse de recibo u otro mensaje. En algunas modalidades, esto puede aliviar la necesidad de que un sistema instructor sea configurado o actualizado para generar cualquier clave. En algunas modalidades, dado que tanto las claves instructora como las claves intermediarias son generadas por el sistema intermedio, el sistema intermedio puede configurarse para precalcular secuencias de claves de destino, reduciendo así o eliminando cualquier retraso en tiempo de ejecución requerido para generar las claves de destino.

La Figura 6 muestra otro ejemplo de sistema 600 para gestionar procesos de datos en una red de recursos informáticos. En esta modalidad de ejemplo, no todos los flujos de órdenes de solicitud de los intermediarios a los dispositivos de destino pasarán por el sistema supervisor, ya que los intermediarios pueden optar por omitir el enrutamiento del supervisor y enviar solicitudes directamente a las bolsas y/o otros lugares.

Por ejemplo, los sistemas intermediarios pueden cruzar solicitudes internamente y/o dirigirlas a mercados opacos internas. Sin embargo, puede ser ventajoso para los instructores tener acceso a la mayor parte posible de su flujo de solicitudes a través del sistema supervisor.

En algunas modalidades, los sistemas intermediarios están configurados para enviar copias de las solicitudes secundarias que pueden ser enrutadas y/o procesadas internamente (como solicitudes de órdenes cruzadas o mercados opacos internos) al sistema supervisor. En algunas modalidades, los dispositivos de destino, como los lugares de negociación financiera, pueden configurarse opcionalmente para enviar copias de seguridad de las solicitudes secundarias recibidas y/o mensajes de respuesta a las solicitudes secundarias. Estas copias de caída pueden contener las claves de destino enviadas con las solicitudes secundarias, de modo que el mecanismo pueda ser procesado y almacenado como datos de solicitud secundaria recibidos a través de otros mecanismos. Como se discute aquí, los sistemas informáticos supervisores 106 pueden estar configurados para almacenar datos de solicitud secundaria que incluyen un indicador que identifica la fuente de los datos. En algunos casos, estos indicadores pueden permitir a los clientes evaluar la confiabilidad y/o precisión de los datos.

En algunas modalidades, también se puede utilizar el uso de copias de caída cuando los dispositivos de destino (como lugares o intermediarios posteriores en un entorno de múltiples saltos) no están configurados para manejar claves de destino u otros datos de supervisión.

En algunas modalidades, las copias de caída pueden ser el único mecanismo mediante el cual el sistema supervisor 190 puede recibir datos de solicitud, por ejemplo, cuando no hay un proxy o dispositivo de escucha entre el sistema intermediario 104 y el destino 108, como es el caso, por ejemplo, para la solicitud secundaria 1 en la Figura 6.

En algunos ejemplos, los sistemas intermediarios y/o de destino pueden estar configurados para enviar copias de seguridad incluso cuando hay un componente supervisor 106 entre los dos sistemas.

Soporte MultiSalto

En algunas modalidades, los aspectos de las modalidades descritas aquí pueden aplicarse a escenarios en los que puede haber más de un sistema intermediario (por ejemplo, un intermediario) que actúa entre un sistema instructor (por ejemplo, un cliente) y un sistema de destino (por ejemplo, un lugar).

La Figura 7 es un diagrama esquemático en bloque que muestra un ejemplo de sistema 700 que involucra múltiples sistemas intermediarios 106 entre un sistema instructor original y los recursos informáticos de destino final.

En la Figura 7, varias claves pueden comunicarse entre diferentes sistemas en conjunto con o en asociación con diferentes solicitudes. En algunos ejemplos, las claves pueden ser incluidas como etiquetas o campos, incluyendo o transmitiéndose junto con las solicitudes. Para referencia, las etiquetas en la Figura 7 se han designado como aguas abajo (TAGa) y aguas arriba (TAGb); por ejemplo, TAGa incluye CK, DK, AI transmitidos hacia adelante desde un sistema instructor (por ejemplo, desde un sistema cliente o un sistema intermediario anterior en la cadena) hacia un sistema intermediario (por ejemplo, un siguiente intermediario); y TAGb incluye BK transmitidos hacia atrás desde un intermediario (por ejemplo, hacia un sistema instructor 102 o componente, o hacia un intermediario aguas arriba).

Algunos de estos sistemas intermediarios pueden estar configurados para operar con los sistemas informáticos supervisores 106, y por lo tanto, deben ser capaces de proporcionar y/o generar información de identificación de solicitudes de orden (por ejemplo, en forma de claves de identificación codificadas) para ayudar en el seguimiento y/o análisis posterior de las órdenes relacionados con la orden original de un cliente.

"Multisalto" puede ser una capacidad del sistema, en donde el sistema facilita el enrutamiento de una solicitud a través de más de un sistema intermediario.

Las solicitudes de procesamiento de datos derivados pueden estar asociadas entre sí, por ejemplo, una solicitud puede tener una "solicitud secundaria" relacionada, una "solicitud terciaria" relacionada, una "solicitud cuaternaria" relacionada, etc. De manera similar, las solicitudes que se han utilizado para derivar solicitudes secundarias pueden ser referidas como solicitudes principales, solicitudes primordiales, etc.

En algunas modalidades, los sistemas en la ruta de múltiples saltos pueden estar configurados para realizar las funciones de un dispositivo instructor, un dispositivo intermediario y/o un dispositivo de destino. Por ejemplo, el sistema del cliente puede actuar como un sistema instructor y generar solicitudes principales para el sistema intermediario A, que actúa como un sistema intermediario y dirige las solicitudes secundarias resultantes al intermediario B, que actúa como el dispositivo de destino. El sistema intermediario A también actúa como un sistema instructor y genera solicitudes secundarias/instructor para el sistema intermediario B, que actúa como un sistema intermediario y enruta las solicitudes terciaria/secundaria a los lugares que actúan como dispositivos de destino. Como se ilustra en la Figura 7, el sistema supervisor puede obtener datos de solicitud de uno o más dispositivos a través del enrutamiento entre estos saltos en el sistema 700.

Por ejemplo, el intermediario A podría recibir una orden de un cliente y luego dirigir toda la orden o una parte de la orden a través del intermediario B. En teoría, el sistema podría tener en cuenta un escenario de orden arbitrariamente complejo en el que el intermediario A dirige a varios intermediarios y luego uno o más de ellos dirigen a otro intermediario, etc. Las transacciones que involucran al intermediario A y al intermediario B pueden, por ejemplo, ser supervisadas por un servidor supervisor, que puede incluir un sistema informático supervisor 190 y/o componentes supervisores 106 como se describe anteriormente o de otra manera. Aunque la estructura en la Figura 7 se ilustra como una estructura de múltiples saltos lineales para simplificar, en otros ejemplos, la estructura puede ser similar a un árbol, cíclica o cualquier otra disposición de nodos del sistema.

En algunas modalidades, un dispositivo instructor puede estar configurado para enviar una solicitud principal directamente a un recurso informático de destino en el lugar, sin ningún sistema intermediario en el medio. En algunos ejemplos, el sistema supervisor puede adicionalmente recibir estos datos de solicitud para proporcionar una imagen más completa de las actividades y/o rendimiento de solicitud de un sistema instructor. Por ejemplo, esto puede proporcionar una comparación para el tiempo, la efectividad en el cumplimiento de solicitudes, etc.

Los aspectos de salto múltiple pueden ser proporcionados a través de uno o más proxies adaptados para facilitar la generación, asociación y/o seguimiento de varias claves criptográficas que pueden ser propagadas a través del enrutamiento del orden y/o sus partes constituyentes. La propagación de las claves criptográficas puede incluir la derivación de claves criptográficas aguas abajo, en donde en algunas modalidades, la derivación de las claves aguas abajo incluye al menos el procesamiento de una o más claves aguas arriba.

Por ejemplo, desde la perspectiva de un intermediario arbitrario en la cadena de intermediarios, un intermediario aguas arriba puede considerarse un "dispositivo instructor", que luego se asocia con al menos una clave instructora y una solicitud principal de ejecución. La clave instructora y la solicitud principal para su ejecución pueden ser recibidas por el sistema informático intermediario, y luego el sistema informático intermediario puede generar al menos una solicitud secundaria para su ejecución que se proporcionará a un dispositivo de destino (que puede ser un lugar o otro intermediario aguas abajo). Esta solicitud secundaria para su ejecución puede estar asociada con una "clave de destino", generada al menos en base a la "clave instructora".

Como se describe aquí con respecto a otros ejemplos, la solicitud secundaria para su ejecución puede ser dirigida al dispositivo de destino, y la solicitud secundaria para su ejecución puede, en algunas modalidades, ser dirigida de tal manera que la información asociada con la solicitud secundaria pueda ser obtenida por el servidor supervisor, que luego almacena y/o pone a disposición la información de ejecución (por ejemplo, acusos de recibo, órdenes enviadas, confirmaciones, marcas de tiempo, identificador para el mecanismo de recopilación del supervisor, etc.) para análisis futuro.

Por lo tanto, puede haber más de un intermediario en una cadena de procesamiento de órdenes, donde un intermediario A podría dirigir órdenes a través de un segundo intermediario B. Puede haber cualquier número de intermediarios, o "saltos", en dicha cadena. El sistema informático supervisor 106 puede utilizarse, en algunas modalidades, para supervisar estas actividades derivadas del orden inicial del cliente a intermediario A. Si intermediario B no está habilitado para operar con el sistema informático supervisor 106, la arquitectura puede configurarse para funcionar como si intermediario B fuera el lugar, y las actividades de intermediario A pueden ser supervisadas como se describe en otras modalidades.

Sin embargo, si el intermediario B está habilitado para operar con sistemas informáticos supervisores 106, entonces las acciones de llenado de órdenes del intermediario B deben estar relacionadas con las acciones de llenado de órdenes del intermediario A en los sistemas informáticos supervisores 106. Una solución de este tipo debería ser capaz de funcionar dado que cada intermediario no necesariamente sabe dónde se encuentra en la cadena de intermediarios, y la cadena de intermediarios puede ser un árbol de intermediarios, no una cadena lineal. Además, puede haber importancia asociada con mantener la confidencialidad del intermediario (por ejemplo, evitar que un intermediario aguas abajo pueda descifrar el algoritmo de enrutamiento de un intermediario aguas arriba). Configurar

los sistemas informáticos supervisores 106 para poder soportar dicho escenario puede aumentar la complejidad en algunas implementaciones, pero también brinda la oportunidad de desarrollar una solución robusta que proporcione verificación de enrutamiento de órdenes al tiempo que se mantiene la confidencialidad entre los intermediarios y/o el público en general.

Para proporcionar más detalles en algunas modalidades, el cliente y el intermediario A se comunican utilizando una clave cliente (CK). El intermediario A puede enviar órdenes al intermediario B utilizando una clave de destino A (DK_A). El intermediario B puede enviar órdenes al intermediario C utilizando una clave de destino B (DK_B), etc. Se pueden proporcionar proxies de puerta de enlace o dispositivos de escucha para monitorear la comunicación entre cada par de intermediarios, guardando la información en los sistemas informáticos supervisores 106. El proxy puede implementarse en hardware o software (o una combinación de ambos) y puede estar físicamente presente en la salida de un intermediario, o en la entrada de otro intermediario, o en ambos, o puede estar ubicado de forma remota de ambos (por ejemplo, a través de una red). El mismo CK podría ser utilizado entre cada salto, pero esto puede no ser tan efectivo para ocultar las actividades comerciales del cliente.

Cuando el intermediario A y el intermediario B están habilitados para su uso con el sistema informático supervisor 106, cualquier dato específico del sistema informático supervisor 106 puede ser comunicado entre los intermediarios en una etiqueta de metadatos específica para cada orden individual enviada desde el intermediario A al intermediario B.

Haciendo referencia a la Figura 7, el intermediario A puede enviar una orden al intermediario B a través de los sistemas informáticos supervisores 106. El intermediario A copia DK en TAG_A (la misma etiqueta utilizada por los clientes para enviar CK) esto indica a los sistemas informáticos supervisores 106 que este es un mensaje de múltiples saltos y permite que el intermediario B lo trate como si fuera un mensaje de un cliente. El intermediario B puede transmitir un ACK del mensaje con una clave intermedia BK.

En consecuencia, el sistema instructor 102 puede ser capaz de recibir BK_A del intermediario A, calcular Al_A y DK_A, consultar el almacenamiento de datos del supervisor con Al_A, descifrar las órdenes y respuestas entre el intermediario A y B, extraer de los mensajes ACK del intermediario B al intermediario A la clave BK_B y/o calcular Al_B y DK_B.

Cuando un cliente desea identificar órdenes enrutadas basadas en las instrucciones del cliente, los sistemas informáticos clientes 102 pueden utilizar el componente informático del cliente para consultar el almacenamiento de datos asociado con los sistemas informáticos supervisores 106 con Al_B y descifrar las órdenes y respuestas entre el intermediario B y el/los lugar(es) 108a..108n.

En este ejemplo, inicialmente, el intermediario A recibe una orden de un cliente y recibe una etiqueta llamada TAG_A del cliente, que incluye el CK del cliente, el cual puede ser generado por el sistema informático supervisor 106.

El intermediario A realiza una orden al intermediario B para satisfacer la solicitud de orden del cliente. Al hacerlo, el intermediario A envía de vuelta una etiqueta llamada TAG_B al Cliente que contiene una clave intermediaria para el intermediario A (BK_{A1}). El intermediario A también genera DK_A y Al_A (índice anónimo) basado en CK y BK_{A1}, e incluye DK_A y Al_A en su propio nuevo TAG_A.

La TAG_A del intermediario A se envía junto con la orden al intermediario B. El sistema informático supervisor 106 registra la orden y la TAG_A en su base de datos. El intermediario B recibe la orden y repite el proceso, utilizando el DK_A recibido como si fuera el CK.

El intermediario B luego genera DK_B y Al_B basado en DK_A y su propia clave intermediaria BK_{B1}. El intermediario B envía de vuelta el TAG_B que contiene BK_{B1}, el cual se almacena en la base de datos del sistema informático supervisor 106 como una confirmación de que la orden fue recibida o completada, y el proceso continúa hasta que se llega al lugar final.

Como cada DK posterior está relacionado con el DK o CK que lo precedió inmediatamente, el cliente puede consultar la base de datos del sistema informático supervisor 106 para encontrar cada mensaje de orden relacionado.

Si se determina que un BK está asociado con el mensaje Al almacenado en la base de datos, la ordenador del cliente se configuraría para determinar el siguiente DK y consultar la base de datos para obtener el siguiente mensaje de orden utilizando el DK conocido y el BK asociado recuperado de la base de datos.

La clave intermediaria A, recibida en el primer TAG_B del intermediario A, se puede utilizar para consultar la base de datos del sistema informático supervisor 106 en busca de los Al del intermediario A. En respuesta, el cliente puede recibir todos los mensajes y confirmaciones en la base de datos derivados del intermediario A. Ya sea la ordenador del cliente, un sistema informático supervisor 106 proxy con el que se interfaz, o la base de datos del sistema informático supervisor 106 pueden realizar uno o más pasos de procesamiento (por ejemplo, extracción, transformación, carga, cálculo, determinación) para identificar cuáles de todos los mensajes y confirmaciones están asociados con la orden inicial del cliente.

Dado que puede haber múltiples saltos de intermediarios, en una cadena lineal, ciclo o arreglo de árbol ramificado, para cumplir con una sola orden del cliente, el sistema informático supervisor 106 puede estar configurado para seguir cada rama de actividad del intermediario en la base de datos del sistema informático supervisor 106 para recrear todas las actividades del intermediario para una orden específica del cliente.

El sistema puede seguir una cadena de actividad de intermediarios en la base de datos hasta que la cadena termine en un recurso informático de destino, como un lugar (por ejemplo, una instalación de procesamiento de solicitudes de orden, una bolsa de valores, una piscina oscura, un sistema de coincidencia de órdenes). Esto podría ocurrir cuando no hay DK presente con un AI almacenado en la base de datos. Para las actividades de llenado de órdenes entre intermediarios, la respuesta de confirmación de un intermediario que llena una orden puede incluir la clave BK del intermediario.

Los lugares no necesariamente tienen capacidades de verificación de orden y es posible que no respondan al intermediario inmediatamente anterior con ningún acuse de recibo que contenga una clave adicional. En estos escenarios, la base de datos del sistema informático supervisor 106 solo habría almacenado el AI del intermediario inmediatamente anterior al lugar sin ningún AI asociado. Un proxy puede ser configurado para interpretar esa situación como el punto final para ese orden en particular.

Como cada intermediario puede enviar partes de la orden de un cliente a más de un intermediario para su ejecución, pero esto no necesariamente se ha comunicado al cliente, el proxy puede configurarse para rastrear y/o monitorear (por ejemplo, buscar) múltiples órdenes secundarias utilizando el mismo CK y BK inicial y posteriormente el mismo DK y BK. Puede haber múltiples entradas en la base de datos del sistema informático supervisor 106 indexadas por la misma combinación DK/AI. Cada una de estas entradas puede ser recuperada y analizada por el proxy.

En algunos casos, puede haber brechas en los mensajes de orden almacenados en la base de datos del sistema informático supervisor 106. El proxy no necesariamente debe finalizar la búsqueda de mensajes de orden si no se puede encontrar un AI en la base de datos, especialmente en casos donde el AI y/o DK para mensajes de orden posteriores puedan ser conocidos o deducibles por el proxy. Por ejemplo, cada intermediario puede estar configurado para comunicar AI, BK, DK o cualquier combinación de ellos de vuelta al intermediario o cliente anterior en la cadena, posiblemente reenviándolo finalmente hasta el cliente.

El cliente puede entonces consultar la base de datos del sistema informático supervisor 106 para obtener todos los mensajes de orden que deberían haber sido generados y almacenados en la base de datos. Si no se puede encontrar un mensaje de orden en particular, el cliente aún puede consultar todos los demás mensajes de orden esperados.

Ejemplos de posibles casos finales para consultar la base de datos de mensajes de órdenes pueden incluir:

(1) orden completada en su totalidad (se encontraron mensajes de llenado para cada orden)

a. si no se cumple la orden, no se llena completamente (por ejemplo, no se llena al 100%):

i. el intermediario permite al cliente recrear las claves del intermediario con hash

ii. consulta la base de datos hasta que dejes de ver una clave 1. el intermediario puede haber omitido una clave

iii. el intermediario puede enviar al cliente un límite de clave terminal para dejar de buscar.

(2) el período de tiempo de orden ha expirado;

(3) la orden ha sido cancelada; y

(4) el cliente pierde la conectividad con el intermediario.

Los mensajes terminales pueden ser almacenados en la base de datos o ser devueltos (por ejemplo, enviados/transmitidos) al cliente. En general, el cliente (o el proxy) puede seguir hasheando las claves de intermediario buscando mensajes de orden en la base de datos utilizando las claves hasheadas hasta que se encuentre un vacío en la base de datos. El cliente/el proxy puede procesar otro número de (por ejemplo, 20-30) claves de intermediario para ver si hay algo más, y luego detenerse si no se encuentra nada más.

Si el intermediario envía todas las claves de intermediario utilizadas al cliente, en lugar de permitir que el cliente las vuelva a crear, entonces el cliente solo verá lo que el intermediario quiere que el cliente vea. Otras actividades realizadas por el intermediario aún pueden estar almacenadas en la base de datos, pero es posible que el cliente no pueda localizarlas. Cuando el cliente está configurado para generar o recrear claves de intermediario, la arquitectura proporciona mayores oportunidades para que el cliente supervise las actividades del intermediario a través del uso de las diversas claves.

Por ejemplo, el intermediario A podría eliminar una ruta de orden de la vista del cliente (por ejemplo, una ruta que proporcionara una ganancia al intermediario A) si el intermediario A solo envía las claves del intermediario y no permite que el cliente regenere todas las claves que se habrían utilizado.

5 Si cada DK no estuviera de alguna manera relacionado con el DK anterior, o con el CK original, entonces el cliente requeriría otra forma de recuperar toda la actividad del intermediario de la base de datos para una orden dado. Eso podría ser posible si solo se utilizara un único CK en lugar de todos los DK, pero entonces múltiples etapas del mismo cumplimiento de orden serían más fácilmente identificables por terceros que revisen la base de datos del sistema informático supervisor 106.

10 En algunas modalidades, cada intermediario podría comunicar su respectivo DK de vuelta al intermediario anterior en la cadena, y finalmente de vuelta al cliente, de modo que cada DK no necesariamente tendría que ser derivable del CK original en este caso. Sin embargo, el sistema informático cliente/supervisor 106 tendría que mantener un registro más grande de DK para cada orden y podría tener mayor dificultad para discernir la orden de los saltos en la cadena de intermediarios sin datos adicionales.

15 Las técnicas de clave y/o codificación/codificación también pueden adaptarse para facilitar el recorrido y la identificación aguas abajo (por ejemplo, por parte del supervisor y/o componente(s) informático(s) del cliente). Por ejemplo, las claves y/o técnicas de codificación/codificación pueden adaptarse de manera que sea más fácil identificar rápidamente la información que puede estar asociada, por ejemplo, a una orden en particular. Un conjunto de técnicas descritas aquí incluyen el uso de técnicas de "índice anónimo", pero también se pueden contemplar otras técnicas.

20 En algunas configuraciones de salto único y salto múltiple, se puede utilizar un índice anónimo (AI) para indexar y localizar mensajes de orden en la base de datos del sistema informático supervisor 106 que pueden estar relacionados con las claves utilizadas. Por ejemplo, un AI puede ser una truncación o un hash de un DK. Otras relaciones entre las claves y un AI.

25 Cuando se combinan DK y AI en una etiqueta, se puede establecer una longitud de etiqueta a una longitud específica para la ofuscación. Por ejemplo, si la clave utilizada es más corta que la longitud del campo, puede ser rellenada en la parte delantera.

30 En algunas modalidades, en la etiqueta resultante, el AI puede ser la parte más a la derecha, y el DK puede ser la parte más a la izquierda. Puede haber superposición entre estas dos partes de la etiqueta. De esta manera, podría ser posible admitir longitudes de bits mayores para las claves al mismo tiempo que se admiten claves heredadas más cortas.

35 En algunos ejemplos, el servidor/sistema supervisor puede codificar los datos de solicitud con una DK y almacenarlos junto con un AI correspondiente.

40 En algunas modalidades, un índice como el AI puede ser utilizado por el cliente para localizar los datos de solicitud almacenados en el servidor supervisor. Por ejemplo, el cliente puede reconstruir el AI para cada orden secundaria relacionada con la orden original del cliente utilizando la(s) clave(s) del instructor y/o del intermediario. El cliente puede entonces consultar el servidor supervisor con cada AI reconstruido para recuperar los datos de la orden secundaria correspondientes a cada AI respectivo.

45 En algunos ejemplos, el uso de indexados para almacenar datos en el sistema supervisor puede reducir el cálculo requerido por un instructor u otro dispositivo solicitante para identificar los datos de solicitud asociados con sus claves. Por ejemplo, para un sistema supervisor que recopila datos de solicitud para numerosos intermediarios, clientes y/o lugares y maneja millones de solicitudes al día, intentar decodificar todos los datos de solicitud para identificar las solicitudes de un instructor es intensivo computacionalmente. Los instructores u otros sistemas solicitantes pueden solicitar solo los datos de solicitud codificados correspondientes a sus AI regenerados, lo que reduce el conjunto de datos que los sistemas deben intentar decodificar. Si bien puede haber colisiones entre diferentes DK, dado que se requiere el DK completo para decodificar los datos, solo un dispositivo instructor que tenga el DK completo tendrá acceso a los datos subyacentes.

50 En algunas modalidades, el dispositivo de proxy/solicitud/instrucción puede estar configurado para solicitar datos correspondientes a sus AI reales, así como AI aleatorios o de distracción. En algunos ejemplos, la adición de AI falsos puede ocultar el verdadero número de AI y/o solicitudes del cliente de terceros que estén escuchando.

55 Si bien el ejemplo anterior se describe con respecto a la relación entre DK y AI, en otros ejemplos, el sistema supervisor puede almacenar datos de solicitud en conjunto con claves instructoras (CK), claves intermedias (BK), claves de destino (DK), un identificador de instructor o cualquier combinación o derivado de los mismos.

60 En algunas implementaciones, cualquier DK individual utilizado por el sistema informático supervisor 106 puede tener una longitud arbitraria y puede ser rellenado para ocultar la verdadera longitud de la clave o para cumplir con una longitud de clave predeterminada. La longitud máxima de la clave puede aumentarse en cualquier momento, y las

claves heredadas anteriores pueden ser rellenadas si es necesario. Las longitudes de clave pueden definirse en función de períodos de día/hora. La base de datos estaría configurada para recordar qué longitud de claves se utilizó en qué momentos. Puede ser ventajoso que la longitud de la etiqueta clave exceda el tamaño del contenido real de DK y AI almacenado en ella para proporcionar una mayor confusión de los mensajes de orden.

En algunas modalidades, un sistema intermediario 104 puede estar configurado para truncar, enmascarar, codificar mediante hash u otra forma de codificación una clave de destino antes de que sea enrutada con una solicitud secundaria. Por ejemplo, un DK_N de 512-bits generado a partir de un XOR de una clave instructora CK y una clave intermedia BK_N puede ser truncado a 256 bits para su uso como clave de destino. Este DK truncado o codificado de otra manera se puede utilizar para codificar y/o almacenar junto con los datos de solicitud secundaria en el sistema supervisor. Al codificar el DK, un supervisor, destino y/o tercera parte que tenga conocimiento de un hash u otra función BK o DK hf no podrá recrear otras claves en la secuencia porque el DK transmitido al supervisor/destino ha sido truncado o codificado de tal manera que aplicar la función hf no proporcionará la siguiente clave en la secuencia. En algunos ejemplos, esto puede proporcionar otro nivel de protección de datos.

Cada usuario del sistema informático supervisor 106 no puede tener acceso a toda la base de datos del sistema informático supervisor 106 para realizar consultas. Por ejemplo, un usuario puede tener que ser provisto para acceder a diferentes tipos de instrumentos, regiones (por códigos de región, por ejemplo, América del Norte, Europa, Asia, etc.). Cada entrada en la base de datos del sistema informático supervisor 106 puede estar asociada con una fecha, código de región, tipo de instrumento y AI. Debido a etiquetas de relleno u otras razones, a veces los AI pueden duplicarse entre órdenes. En ese caso, el sistema del cliente puede intentar decodificar cada mensaje codificado que tenga un AI que el cliente cree que pertenece al cliente. Si el sistema del cliente no puede descifrar el mensaje para una entrada en particular, el sistema del cliente asumirá que ese mensaje no es el mensaje del cliente y pasará al siguiente. El sistema informático supervisor 106 puede replicar datos de centros de datos en todo el mundo para que los usuarios puedan acceder a datos de todo el mundo que se originen en otros centros de datos de forma local, si el usuario tiene los privilegios de acceso para hacerlo.

Si bien se discuten varias claves anteriormente, estas claves se utilizan principalmente para indexar. El sistema informático supervisor 106 puede no requerir que los mensajes de orden en sí mismos estén codificados, y en muchos casos las órdenes no están codificados, lo cual es intencional. Sin embargo, en algunos casos, puede ser necesario o deseable que el contenido de mensajes de orden específicos entre intermediarios, y almacenados en la base de datos del sistema informático supervisor 106, esté codificado. Los medios para descifrar el contenido de dichos mensajes codificados preferiblemente no deben ser conocidos por la base de datos del sistema informático supervisor 106 o por terceros. Cualquier codificación del contenido del mensaje puede ser completamente independiente del sistema CK/BK/DK/AI utilizado por el sistema informático supervisor 106. En este caso, cada intermediario debería ser capaz de cifrar de tal manera que el intermediario posterior y también el cliente puedan descifrar.

Tanto el intermediario A como el intermediario B pueden necesitar almacenar las claves necesarias para descifrar los mensajes de los intermediarios anteriores y cifrar los mensajes posteriores, y el cliente también necesitaría la(s) clave(s) de descodificación. El intermediario B puede comunicar una clave de codificación o descodificación con anticipación desde el primer intermediario en la cadena, o el intermediario anterior. Cualquier comunicación de claves de este tipo puede ser enviada por un intermediario anterior a través de un canal de comunicación separado de aquellos para las comunicaciones supervisadas por el sistema informático supervisor 106, evitando así completamente el sistema informático supervisor 106. Cada intermediario puede utilizar la misma clave para una orden en particular, o cada intermediario puede tener una clave única para cada orden, lo que requiere que el cliente reciba y almacene claves de decodificación (por ejemplo, de descodificación) para cada salto en la cadena.

En algunas modalidades, el mismo intermediario podría aparecer varias veces en la misma cadena. En tal escenario, el mismo intermediario puede utilizar los mismos y/o diferentes DK.

En algunas modalidades, el intermediario puede enviar un DK en una etiqueta al siguiente intermediario y al sistema informático supervisor 106, la existencia del DK en la etiqueta puede ser utilizada como una señal para el cliente de que esta orden se está enviando a otro intermediario en una cadena.

En algunas modalidades, un proxy puede o no estar configurado para procesar cada mensaje de orden recuperado como si se refiriera a un salto posterior en la cadena de procesamiento de órdenes, de modo que la etiqueta del mensaje se pueda utilizar como una señal para el cliente de que se debe aplicar el algoritmo de encadenamiento de recuperación de mensajes.

En algunas modalidades, el mensaje de acuse de recibo (ACK) de un intermediario aguas abajo a un intermediario aguas arriba puede incluir su BK, almacenado por la base de datos del sistema informático supervisor 106 para que se pueda seguir la cadena. El ACK puede, por ejemplo, devolver una clave utilizada en un esquema de múltiples saltos (por ejemplo, el intermediario B devuelve su BK hacia el intermediario A en un ACK, filtrado por el proxy para que el BK se almacene en la base de datos del sistema informático supervisor 106, pero no regresa al intermediario A.

Por ejemplo, el sistema informático supervisor 106 puede consultar a BK_{A1} CK para obtener: $DK_A A_{1A}$, y buscar A_{1A} para obtener BK_{B1} .

Como otro ejemplo, el sistema informático supervisor 106 puede consultar a BK_{B1} DK_1 para obtener $DK_B A_{1B}$.

En algunas modalidades, el sistema informático supervisor 106 puede estar configurado para almacenar los acuses de recibo en la base de datos del sistema informático supervisor 106, además de los mensajes de solicitud de llenado de órdenes de los intermediarios. Por ejemplo, los sistemas informáticos intermediarios 104 podrían enviar un mensaje al sistema informático supervisor 106 y proporcionar una copia directamente al lugar (por ejemplo, a través de una copia de seguridad).

Soporte de Múltiples Patas dentro de un Sistema

En algunos casos, un intermediario puede tener múltiples sistemas internos a través de los cuales se procesan las órdenes. Similar a los ejemplos en los que un sistema supervisor y la comunicación de claves entre sistemas permiten la gestión y monitorización de recursos informáticos en red, estos aspectos pueden aplicarse de manera similar para monitorizar el manejo de solicitudes secundarias dentro de un sistema como un único sistema intermediario/intermediario.

La Figura 8 es un diagrama esquemático en bloque que ilustra una implementación de ejemplo donde un único sistema, como un dispositivo intermediario, tiene múltiples sistemas internos 810, 820, 830 en los cuales se pueden procesar solicitudes, según algunas modalidades.

Cuando un intermediario tiene una estructura de cadena interna, donde cada ordenador envía datos directamente a la siguiente ordenador para finalmente completar las órdenes, la situación puede ser más simple y no requerir pasos específicos que se deban tomar.

En una implementación base, BK_0 sería generado por la entidad de negociación electrónica del intermediario 810 que genera una orden secundaria (por ejemplo, el enrutador de órdenes inteligente) y luego se comunica de vuelta al cliente en el ACK de la orden del cliente. Entonces, la secuencia de BK generada por la entidad del intermediario sería una simple lista única que también podría ser reproducida por un sistema supervisor. Sin embargo, las diferentes estructuras de sistemas intermediarios pueden complicar este proceso.

En algunos ejemplos, los componentes de procesamiento 820 que generan las solicitudes secundarias pueden no ser el componente de procesamiento que envía el ACK para la solicitud principal. El envío del ACK puede realizarse aguas arriba en una pasarela orientada al cliente, y en consecuencia, esto podría requerir que exista alguna forma de sincronización de selección de BK entre el sistema aguas arriba y el componente de procesamiento aguas abajo que genera solicitudes secundarias.

Los componentes de procesamiento 810, 820, 830 pueden incluir enrutadores inteligentes u otros dispositivos computacionales y/o de redes para procesar y/o generar solicitudes secundarias para enrutamiento. En ejemplos donde hay más de un componente de procesamiento/dispositivo informático que genera órdenes secundarias potencialmente de forma concurrente, se implementan mecanismos para evitar colisiones entre los dispositivos de procesamiento 810, 820, 830.

En algunos ejemplos, puede haber múltiples componentes de procesamiento 820 que generan órdenes secundarias que se ejecutan de forma independiente. Por ejemplo, una orden de cliente de 10K acciones puede dividirse de manera que un componente de procesamiento que ejecuta el algoritmo A negocie 3K acciones y las 7K acciones restantes sean negociadas por otro componente de procesamiento que ejecuta el algoritmo B. Otro enfoque de implementación puede ser gestionar la selección de BK y la inserción de DK/AI en las pasarelas. Dado que puede haber muchas pasarelas, la coordinación de los BK puede resultar poco práctica.

El sistema "Multi-etapa" 800 proporciona la capacidad de manejar una orden principal única que es manejada o procesada por múltiples componentes de procesamiento generando o manejando solicitudes secundarias dentro de un sistema. Este es un problema para la arquitectura porque idealmente, cada entidad debería poder asignar el siguiente BK_N en secuencia comenzando desde el BK_0 inicial. Sin embargo, si las entidades están solo ligeramente acopladas, como en el caso de dos o más enrutadores algorítmicos o enrutadores de órdenes inteligentes, o dos o más pasarelas, etc., la coordinación puede ser un desafío y puede generar una latencia adicional no deseada.

Grandes cadenas de BK pueden ser generadas simplemente ejecutando algoritmos de codificación o hash (por ejemplo, SHA512) en un bucle tantas veces como sea necesario. Sin embargo, esto puede ser computacionalmente costoso y no es escalable si hay muchos componentes de procesamiento "multi-etapa".

De acuerdo con algunas modalidades, un enfoque para reducir el costo computacional de generar BK al mismo tiempo que se reduce el tiempo computacional a una constante pequeña para generar un BK arbitrario (en lugar de requerir generar una cadena de BK) es generar una matriz multidimensional de BK donde cada entrada es un XOR de los BK

a lo largo del eje de la matriz multidimensional. En algunas modalidades, seleccionar el número divisor y el tamaño de la dimensión del bloque BK como primos relativos puede mejorar la probabilidad de que los BK generados no se superpongan hasta que se hayan utilizado todos los BK en el conjunto. Incluso cuando se produce una superposición, en algunas modalidades, enfoques adicionales, como rotar los BK a lo largo de una de las dimensiones del bloque en 1 byte cada vez que el bloque se envuelve, pueden ayudar a generar más de 1 millón de matrices únicas a partir del mismo conjunto de BK precalculados. Dado que calcular una entrada BK requiere un tiempo de cálculo constante independientemente del índice BK, el divisor para el esquema puede ser arbitrariamente grande (mayor que el número máximo de indexados que puedan ser requeridos en algún momento).

En algunas modalidades, el sistema puede estar configurado para admitir el enfoque de múltiples etapas asignando un BK₀ inicial a una orden principal, y luego permitiendo que todas las entidades que generan órdenes secundarias lo hagan de forma independiente asignándoles un índice de módulo único "i" y un divisor "m" donde "m" es igual o mayor que el mayor "i" en el conjunto de entidades. Otras metodologías de numeración también son posibles. Una entidad genera solicitudes secundarias y les asigna BK comenzando con BK indexado por "i" y luego incrementando por "m". Entonces, el primer BK enviado sería "i", el segundo "i+m", el tercero "i+2m", y así sucesivamente.

Por ejemplo, un componente de procesamiento indexado como "3" en un conjunto de entidades con divisor "7" enviaría la siguiente secuencia de BK: 13, 10, 17, 24, 31.

En este ejemplo, un sistema informático de proxy/supervisor puede recibir el índice BK 0 y luego ser capaz de calcular todos los BK subsiguientes en la serie reproduciendo los mismos BK que serían utilizados por las entidades de intermediarios.

Por lo tanto, es posible que el sistema no pueda determinar el índice de las entidades que generaron órdenes secundarios y tendría que utilizar un algoritmo heurístico para encontrarlas.

En algunas modalidades, si el intermediario elige no implementar una estrategia de múltiples etapas, entonces puede utilizar un ID de entidad/modulo índice predeterminado (por ejemplo, 1) para todas las órdenes secundarias.

Cuando un intermediario tiene múltiples componentes/ordenadores de llenado de órdenes (enrutadores de órdenes) que cada uno puede llenar parte de la solicitud de un cliente instructor, entonces puede haber un desafío mayor para el sistema informático supervisor 106 para rastrear las actividades del intermediario. El instructor puede desear rastrear todas las órdenes ejecutadas por diferentes partes del intermediario, manteniendo un buen nivel de anonimato y tiempos de ejecución razonables.

Por ejemplo, el cliente se conecta a un intermediario, a través de un proxy del sistema informático supervisor 106, el intermediario envía órdenes a uno o más enrutadores algorítmicos para llenar las órdenes. Un servidor proxy podría residir entre cada enrutador y la ruta fuera de la red interna del intermediario. Puede surgir un desafío en cuanto a cómo generar y asignar claves de intermediario a cada acción de llenado de órdenes por cada enrutador.

El sistema informático supervisor 106 podría revelar cuánto tiempo tarda en procesarse la orden de un cliente a través del intermediario. El mismo orden podría ser gestionado por uno o más enrutadores, o podría ser gestionado por diferentes enrutadores en diferentes momentos, a lo largo de un día u otro período de tiempo. Uno o más de los enrutadores del intermediario que utilizan las mismas claves pueden ser suficientes para garantizar que la arquitectura funcione, pero para ocultar mejor las actividades entre los intermediarios, puede ser una mejora que cada llenado de cada enrutador esté configurado para utilizar un BK diferente, que también debe ser verificable por el cliente (por ejemplo, para que el cliente pueda, mediante el procesamiento de los registros, determinar, mediante el uso de los BK, qué órdenes y/o solicitudes de procesamiento estaban relacionadas con las órdenes del cliente, de modo que el cliente pueda validar y/o analizar el rendimiento del intermediario).

En una modalidad, un primer ejemplo de método para rastrear a un intermediario que utiliza múltiples enrutadores internos de órdenes puede ser que cada enrutador (o hoja en el árbol) utilice la misma clave intermediaria (BK) para la orden de un cliente en particular. En ese caso, el BK debería ser comunicado a cada hoja. Esto se puede lograr enviando los BK reales a cada enrutador, o enviando un índice a una base de datos interna de BK, para que cada enrutador busque el BK que se utilizará para cada orden.

Llenar órdenes de esta manera puede resultar en múltiples entradas en la base de datos del sistema informático supervisor 106 que tienen el mismo índice, lo que requiere un método descrito anteriormente para que un proxy recupere todos los mensajes de orden que están indexados por el mismo AI (por ejemplo, el cliente no debe dejar de identificar posibles coincidencias tan pronto como se encuentre un mensaje con ese índice).

Mientras que en algunas modalidades, el sistema permite consultar múltiples mensajes de orden con el mismo AI, este método puede revelar que el intermediario está dividiendo una orden en X número de partes. Un tercero podría contar cuántos AI duplicados existen y extrapolar información sobre las actividades de llenado de órdenes basándose en esa información.

En consecuencia, en otra modalidad, se aplica un método alternativo. En esta modalidad, cada enrutador de órdenes podría generar o ser asignado su propio BK. Este BK sería comunicado de vuelta al cliente. El sistema informático intermediario 104 estaría configurado de manera adecuada para enviar todas las claves de hojas de vuelta al cliente. Los BK podrían ser transmitidos al cliente uno a la vez o en lotes a medida que se va completando la orden. Los BK podrían ser comunicados únicamente cuando comienza a procesarse la orden, o cuando la orden está completamente lleno.

En tal modalidad, un desafío a superar puede incluir la gestión del rendimiento informático en relación con la generación de los BK. La generación puede volverse computacionalmente compleja, lo cual puede llevar a problemas de rendimiento posteriores y/o generales. En consecuencia, en algunas modalidades, con el fin de mejorar el rendimiento de la generación de BK y permitir al cliente recrear los BK, en lugar de tener que recibirlos individualmente, los BK pueden asignarse a cada enrutador interno de órdenes si se conoce el número de enrutadores de órdenes.

Si bien se pueden utilizar diversas metodologías, una de ellas es asignar BK utilizando la división módulo. Por ejemplo, suponiendo que el intermediario utiliza 25 órdenes internas de orden, los BK pueden asignarse comenzando desde el número 1, mediante la división módulo 25, lo que significa que los siguientes BK se asignarían al primer enrutador de órdenes: 1, 26, 51, 76, etc., y los siguientes BK al enrutador de segundo orden: 2, 27, 52, 77, etc., y así sucesivamente.

Por ejemplo, la división módulo 10 asignaría en su lugar 1, 11, 21, 31, 41, etc. al enrutador de primer orden. En este caso, cada enrutador podría enviar de vuelta el número de indexado para el último BK utilizado para completar la orden de ese cliente.

Los índices podrían ser comunicados al cliente para recrear los BK, lo cual puede ser más eficiente que comunicar la totalidad de cada BK utilizado al cliente. Cada rama en el árbol de enrutadores de orden podría comunicar continuamente su valor de indexado BK terminal de vuelta al cliente, pero puede ser preferible recopilar los valores terminales de todos los enrutadores y enviarlos de vuelta como una única confirmación al cliente.

El cliente deberá consultar la base de datos para obtener todos los AI utilizando todos los BK. Cuando el cliente examina la base de datos para AI, la falta de un AI en este caso no necesariamente significa que haya una anomalía de la que preocuparse. Por ejemplo, los BK 1, 11, 21 y 31 pueden ser utilizados por el enrutador de primer orden, mientras que solo los BK 2 y 12 pueden ser utilizados por el segundo enrutador, dejando posiblemente muchos BK entre 1 y 31 sin usar.

Sin embargo, la división módulo puede ser ineficiente si uno o más enrutadores no utilizan muchas de sus claves. En el método de módulo, cada enrutador (o sistema informático supervisor 106 conectado a cada enrutador) puede tener un ID único.

Los BK pueden ser precalculados en un grupo al que cada proxy/enrutador puede acceder o las claves podrían ser pasadas internamente. Donde hay un gran número de enrutadores, esto puede volverse ineficiente. Una posible solución sería no generar los BK hasta que sean necesarios. Después de una ronda de generación de BK, un enrutador/proxy puede consultar al sistema informático supervisor 106 para ver qué BK se utilizaron, luego generar la siguiente clave para aquellos BK utilizados (por ejemplo, si se utilizó BK01, generar BK11, pero si no se utilizó BK01, no generar BK11).

Idealmente, uno puede desear infinitos BK, seleccionados arbitrariamente. Si los BK se generan mediante la operación XOR de un conjunto de BK con otro, entonces se necesita precalcular un menor número de BK. Por ejemplo, precalcule BK01 a 20 y haga una operación XOR con BK21 a n según sea necesario. Cada fila de la matriz resultante es determinable por cualquiera de los enrutadores/proxies. Además, se puede desplazar cualquiera de los ejes de la matriz o se pueden desplazar los BK y recalcular una vez que la matriz se haya agotado.

Cada enrutador inteligente puede ser configurado para realizar generación de claves matriciales según este algoritmo. Un proxy (por ejemplo, el cliente) también podría reproducir la clave conociendo los parámetros de la matriz. En algunas modalidades, el divisor (por ejemplo, para operaciones de módulo) número (número de enrutadores) debe ser un número primo relativo a la matriz. Por ejemplo, en una matriz de 5x5, un divisor de 3 y un divisor de 7 pueden dar lugar a resultados superpuestos.

Se podría diseñar un proxy en cada enrutador de órdenes inteligente en lugar de ser un dispositivo separado.

En algunas modalidades, se utiliza un enfoque alternativo en lugar del enfoque de módulo para generar secuencias de BK. Se genera un BK específico de la entidad.

Por ejemplo, bajo este enfoque, cada entidad comienza con BK_0 y luego genera un BK_{E0} específico de la entidad = $fSHA512(BK_0, Entity_ID)$. El ID de la entidad puede necesitar ser anticipado por los clientes y intermediarios aguas arriba (por ejemplo, en algunas modalidades, se establece como un número entero simple que comienza con 1). La secuencia de BK específicos de la entidad se puede generar utilizando codificación en cascada, por ejemplo: $BK_{En+1} = fSHA512(BK_{En})$.

Una ventaja de este enfoque es que garantiza que la superposición de DK y AI entre diferentes entidades es poco probable. El enfoque también utiliza cadenas secuenciales de BK con un bloque único de BK para cada entidad, en lugar de un esquema de módulo en el que todos los BK comparten el mismo bloque de BK. El enfoque no requiere que las entidades compartan bloques BK precalculados. Cada entidad genera y mantiene su propio bloque BK que puede precalcular más bloques BK; sin embargo, puede ser necesario compartir una lista de BK₀ para facilitar el precálculo.

La entidad que asigna BK₀ a un CK puede necesitar poder comunicar esa selección a las partes involucradas. Por ejemplo, un BK₀ puede necesitar ser devuelto al cliente en el mensaje ACK; un BK₀ puede necesitar ser comunicado hacia adelante a todas las entidades que están generando órdenes secundarios esto puede ser comunicado como el índice del BK₀ en la lista compartida de BK₀ o puede ser comunicado como el propio BK₀.

Cuando una entidad aguas abajo recibe un BK₀, puede generar un bloque BK directamente a partir de él en tiempo real (el bloque puede generarse de forma incremental o en su totalidad) o puede buscar el BK₀ en sus bloques precalculados de BK₀ basados en una lista compartida previa de BK₀.

Monitoreo interno por parte del intermediario de los propios sistemas del intermediario utilizando un sistema supervisor interno.

en lugar de que el cliente utilice el sistema informático supervisor 106 para monitorear y verificar las actividades del intermediario, que aún pueden ocurrir independientemente de eso, el intermediario puede estar monitoreando sus propios enrutadores internos utilizando una base de datos interna y una aplicación similar a un proxy. El intermediario puede entonces ser capaz de monitorear la actividad del enrutador de órdenes inteligentes y posiblemente detectar anomalías, como un enrutador llenando órdenes de manera inesperada o no intencionada.

Por ejemplo, una solución de este tipo puede ser proporcionada en forma de un kit de implementación de intermediario que incluye gestión de entidades y configuración.

La Figura 9 es un diagrama esquemático en bloque que ilustra aspectos de una implementación de ejemplo del sistema 900, donde un único intermediario tiene múltiples sistemas internos en los que se pueden procesar órdenes, y el intermediario utiliza una aplicación/componente interna de supervisión en el lado del intermediario para monitorear el rendimiento del intermediario, según algunas modalidades.

El sistema de monitoreo interno puede, por ejemplo, realizar diversos análisis en relación con el rendimiento y/o uso, como latencias asociadas con técnicas de nivelación de latencia, gestión de opciones, etc. La solución puede ayudar, por ejemplo, a aislar la capacidad de verificación de riesgos y utilizar estrategias clave (por ejemplo, la estrategia CK/BK) para correlacionar las órdenes de clientes entrantes con las órdenes secundarias salientes.

Puede haber un dispositivo o aplicación de supervisión interna 112 que se puede utilizar para diversos fines, como verificar si las cantidades salientes superan las cantidades entrantes, verificar si los parámetros de las órdenes salientes (precio, lado, cantidad, TIF,...) no son consistentes con las órdenes entrantes o con los parámetros o opciones configurados, verificar la falta de actividad saliente, verificar la actividad saliente ineficaz: grandes cantidades de órdenes secundarias que no generan llenados, generar alertas electrónicas en tiempo real, proporcionar una capacidad de interruptor de apagado manual o automatizado, generar alertas electrónicas con múltiples niveles de activación y/o proporcionar una pantalla de GUI de las anomalías detectadas.

El dispositivo o aplicación de supervisión interna 112 puede estar configurado para coordinar con un sistema informático supervisor 106, y el sistema informático supervisor 106 puede estar ubicado en la entrada del sistema intermediario y en las salidas de los enrutadores de órdenes inteligentes del sistema intermediario.

Cada proxy puede comunicarse con un servidor interno de manera similar a cómo el sistema informático supervisor 106 recibe datos de intermediarios y lugares intermedios. El servidor del sistema informático supervisor interno puede ser privado, o también puede enrutar hacia un servidor del sistema informático supervisor externo 106 el enrutamiento externo puede ser útil cuando el intermediario es cliente de otro intermediario.

En algunas modalidades, dado que este sistema es interno, la codificación puede no ser tan importante y no ser utilizada. Solo se almacenan y se pueden acceder los datos internos del intermediario.

Un problema a resolver es que a veces un enrutador de órdenes inteligente no funciona correctamente, o está programado de una manera que resulta en un comportamiento inesperado. El enrutador podría realizar órdenes que no estaban destinados. Una implementación interna puede ayudar a detectar dichas actividades, por ejemplo, determinando el número total de órdenes secundarias que ingresan al sistema y el número total de órdenes que salen. Si hay una discrepancia, la implementación interna del intermediario puede configurarse para indicar que hay un problema. Factores que pueden ser examinados pueden ser la cantidad total de órdenes, el tamaño de las órdenes y los símbolos. Las órdenes pueden ser emparejadas mediante la comparación/vinculación de los BK salientes con los CK entrantes.

La implementación interna del supervisor puede configurarse para enviar alertas al detectar una anomalía. Las alertas también pueden ser ejecutables. Por ejemplo, el supervisor interno puede ser capaz de bloquear que se envíen más órdenes desde un enrutador en particular hacia el exterior del intermediario, o el supervisor interno puede tener la capacidad de enviar un mensaje de control al enrutador de órdenes para detener el llenado de órdenes o apagarlo por completo.

A veces, el enrutador preciso con el problema puede no ser fácilmente identificable, o puede haber habido un problema con la forma en que se segmentó la orden a través de los enrutadores. En esos casos, el supervisor interno puede evitar que se procesen cualquier orden derivada del CK o DK coincidente. Se puede enviar un mensaje de control a todos los enrutadores salientes para que dejen de procesar órdenes de ese CK o DK, o los proxies orientados hacia el exterior pueden bloquear las solicitudes de llenado de órdenes que coincidan con ese CK o DK.

Las acciones de las alertas pueden ocurrir en tiempo real, pero también puede haber un peligro al reaccionar exageradamente a problemas percibidos que en realidad están funcionando según lo previsto. Actuar en falsos positivos puede ser tan problemático como pasar por alto problemas.

En algunas modalidades, un supervisor interno puede estar configurado con un umbral de manera que solo cuando las actividades de llenado de órdenes superen la orden total del cliente más el umbral, se tomará acción. Para ayudar a determinar un umbral adecuado, el supervisor interno podría configurarse inicialmente para operar en modo de alerta solamente antes de habilitar acciones basadas en las alertas.

Puede haber otra información o parámetros que se deben monitorear en lugar de o además de las órdenes de entrada/salida. El supervisor interno podría monitorear la frecuencia de llenado de órdenes para identificar fallas en el algoritmo del enrutador de órdenes o un rendimiento subóptimo. Cada vez que llega o sale un orden, el supervisor interno puede correlacionar y verificar con cualquier regla programada en el sistema.

En algunas modalidades, la gestión/monitorización interna de los procesos de datos dentro de un sistema puede proporcionar ventajas sobre las técnicas de monitorización tradicionales. Por ejemplo, cuando los componentes de procesamiento individuales monitorean y reportan su propio comportamiento, si un componente falla o deja de funcionar, su capacidad de reporte puede fallar o cesar, lo que provoca una falta de información en un momento crítico. Además, cualquier cambio en las topologías de enrutadores o la adición/sustracción de componentes puede requerir cambios en el sistema de monitoreo.

Sin embargo, en las modalidades del sistema supervisor descritas aquí, el monitoreo/gestión puede ser tecnológicamente agnóstico y recibir continuamente datos de solicitudes secundarias, independientemente de si un nodo se cae o presenta fallas. El sistema también puede proporcionar marcas de tiempo precisas a medida que las órdenes ingresan o salen del sistema, y a través de la gestión de claves puede rastrear las órdenes secundarias hasta sus dispositivos generadores.

Tanto el Cliente como el intermediario Conociendo las Claves Completas, Algoritmo de Hashing.

En algunas modalidades, el servidor supervisor puede estar configurado para mantener una base de datos pública de órdenes codificadas (secundarias), las cuales pueden ser indexadas (por ejemplo, utilizando un Índice Anónimo (AI)). Las órdenes codificadas pueden ser listadas y recuperadas por cualquier persona, pero requieren una copia de la clave X, o la clave de decodificación correspondiente, para descodificar. Opcionalmente, se puede proporcionar un proceso de inicio de sesión seguro para permitir únicamente a los usuarios registrados del servidor supervisor consultar y recuperar cualquiera de las órdenes.

Para permitir que el cliente verifique/rastree las actividades del intermediario, este puede compartir sus claves de codificación completas y cualquier información segura relacionada con el cliente. En algunas modalidades, especialmente cuando solo se comparte una clave entre el intermediario y el cliente, el cliente, utilizando la información proporcionada por el intermediario, puede regenerar una secuencia de claves secundarias hash utilizadas por el intermediario para determinar qué órdenes secundarias se realizaron a partir de la orden principal original. El cliente puede regenerar las claves secundarias utilizando el mismo proceso utilizado por el intermediario para generar las claves secundarias, donde el cliente conoce la clave intermediaria, o la clave cliente en el caso de que la clave cliente se haya compartido originalmente con el intermediario, y el algoritmo de hash utilizado por el intermediario. El cliente también puede ser capaz de determinar qué órdenes secundarias estaban relacionadas con otras órdenes secundarias utilizando este proceso.

En algunas modalidades, el intermediario puede precalcular una o más claves de intermediario o claves secundarias antes de recibir una orden de un cliente. Por ejemplo, puede ser ventajoso para el intermediario realizar cualquier cálculo requerido para generar claves secundarias para un intermediario o clave cliente en particular de antemano, para reducir la latencia o la sobrecarga de procesamiento en el momento en que se solicita la orden del cliente, especialmente cuando se reciben muchas órdenes en el intermediario simultáneamente o razonablemente contemporáneas.

En algunas modalidades, en lugar de que el intermediario genere claves secundarias a partir de una clave intermediaria o cliente, el intermediario puede generar una o más claves aleatorias de forma anticipada o en el momento del orden, que sean independientes entre sí, y asociar cada orden secundario requerido con una de las claves generadas aleatoriamente. En esta implementación, el intermediario puede compartir cada una de las claves asociadas a las órdenes secundarias de la orden del cliente para que el cliente pueda verificar la información de transacción de la orden con el servidor supervisor utilizando las claves secundarias recibidas. Si las claves secundarias no fueron generadas a partir de una clave intermediaria o cliente principal, entonces puede que no haya una relación discernible entre las claves secundarias de tal manera que el cliente no pueda derivar todas las claves secundarias de una colección completa para una orden de cliente en particular. El cliente puede requerir recibir la lista completa de claves secundarias del intermediario en este caso.

En algunas modalidades, el intermediario puede generar cualquier clave secundaria necesaria para una orden del cliente en tiempo real o al recibir una solicitud de orden de un cliente. Opcionalmente, el intermediario puede depender de hardware o software especializado o personalizado, aprovechando opcionalmente una o más unidades de procesamiento central ("CPU"), unidades de procesamiento acelerado ("APU") y/o unidades de procesamiento gráfico ("GPU"), para acelerar el cálculo en tiempo real de las claves.

Opcionalmente, se puede proporcionar información de relación en forma de los parámetros de una función de hash, una tabla de hash, claves de hash, información de cadena de hash, etc.

A partir de ahí, el cliente puede solicitar las órdenes secundarias específicas mediante el código AI al servidor supervisor, opcionalmente a través de un canal de comunicación codificado.

Como finalmente podría ser posible descifrar la clave X y, por lo tanto, descodificar la información del orden, solo el cliente o el intermediario pueden conocer la clave completa Y, lo que permite al cliente o al intermediario determinar qué órdenes secundarias recuperables públicamente fueron realizadas por el cliente/intermediario como parte del mismo orden principal. Opcionalmente, la comunicación de claves entre el intermediario y el cliente puede ser a través de un canal codificado. En algunas modalidades, el servidor supervisor no puede determinar las interrelaciones entre órdenes, incluso cuando ha recibido órdenes secundarias sin codificar del intermediario. Por lo tanto, cuando el supervisor almacena los datos del orden en su base de datos codificada con la clave X recibida del intermediario, no se pueden almacenar ni discernir información de relación entre las órdenes secundarios desde el servidor supervisor.

La codificación y hashing con una clave más grande que la compartida para descodificación.

El intermediario puede cifrar y resumir las órdenes con una clave grande Y, pero solo puede transmitir una clave truncada X al supervisor/lugar. Una parte de la clave puede ser utilizada en el codificación, mientras que otra parte puede ser utilizada para el hashing.

La clave Y puede incluir: la clave de codificación X que se utiliza para cifrar la orden, un código de indexado Anónimo (AI) para identificar la orden y bits adicionales para el hash de la serie de claves de cliente para cada orden principal.

Al no transmitir la clave completa Y, el supervisor/local puede descifrar y procesar cada orden secundaria, pero no podrá determinar cómo se hashearón las claves de las órdenes secundarias y, por lo tanto, no podrá determinar qué órdenes están relacionadas entre sí. Esto puede proporcionar seguridad adicional en comparación con el simple uso de un algoritmo de hash confidencial, ya que podría ser posible ingeniar en reversa el algoritmo de hash. En algunas modalidades, se pueden utilizar algoritmos de hash convencionales (por ejemplo, MD5, SHA-1, SHA-2, SHA-3 o varios algoritmos del Instituto Nacional de Estándares y Tecnología) y asociarlos con los bits adicionales.

Incluso si el algoritmo de hash fuera ingeniería inversa, podría ser mucho más difícil descifrar la relación de hash cuando solo se comparte la clave truncada. Por ejemplo, la única forma de determinar prácticamente cómo se han ordenado las órdenes secundarias es con la clave completa Y, que solo está disponible para el intermediario y el cliente.

Por ejemplo, la clave Y puede tener una longitud de 384 bits, siendo la clave de codificación X de 256 bits y el código AI de 32 bits. Los 96 bits restantes se mantendrían privados (por ejemplo, no se transmitirían a un lugar o supervisor), lo que aumentaría la dificultad para que un lugar o supervisor regenere la secuencia de claves secundarias a partir de la primera.

En algunas modalidades, la clave raíz de 384 bits puede ser transmitida en su totalidad de regreso al cliente en el mensaje de ACK. Esta clave puede facilitar la regeneración de la secuencia de claves hash que el intermediario utilizó para procesar la orden. Por ejemplo, un cliente o varios sistemas informáticos utilizados por el cliente pueden ser utilizados para regenerar esta secuencia (por ejemplo, una secuencia de hashes repetidos, donde un hash anterior es la entrada en una función hash posterior) y, por lo tanto, determinar la relación entre varios órdenes secundarios y/o órdenes del cliente.

La regeneración de la secuencia puede, por ejemplo, permitir que un cliente o una parte asociada con el cliente identifique todas las órdenes secundarias que se generaron a partir de una orden del cliente, por ejemplo, para que el cliente pueda evaluar el rendimiento del intermediario. Por ejemplo, se puede evaluar el desempeño del intermediario en función de las mejores prácticas de ejecución, las cuales pueden evaluar las órdenes recibidas por un intermediario y evaluar periódicamente si el intermediario utilizó mercados competidores, creadores de mercado o redes de comunicación electrónica.

(ECNs) que ofrecieron las condiciones más favorables de ejecución en el momento de la ejecución. Algunos de los factores relacionados con la mejor ejecución pueden incluir: la oportunidad de obtener un precio mejor que el actualmente cotizado, la rapidez de ejecución y la probabilidad de que se realice la operación.

Un desafío potencial podría ser que terceros puedan monitorear varios elementos de información para correlacionar estadísticamente a los clientes con las operaciones, por ejemplo, a través de la asociación temporal. Se pueden utilizar diversas estrategias para ayudar en la obfuscación del cliente.

En algunas modalidades, la longitud exacta en bits de la clave Y también puede no ser revelada públicamente por el intermediario, para mayor seguridad.

La longitud del bit de la clave Y también puede variar de orden a orden, para mayor seguridad adicional. En algunas modalidades, se puede utilizar relleno, acolchado o bits desechables, por ejemplo, para hacer que la longitud de bits de la clave Y parezca uniforme. La longitud de la clave Y puede ser configurable y reconfigurable según sea necesario, incluyendo aumentar la longitud de la clave según lo requieran o recomienden ciertos estándares de codificación.

Este método también puede ocultar el número de órdenes secundarias en una orden principal, de esta manera ocultando a los respectivos lugares si recibieron la orden principal completa o no.

En el contexto de la Figura 2, en este ejemplo, las claves de destino (DK_N) pueden ser solo porciones de una clave completa, las claves de destino permiten el descodificación de la orden secundaria, pero no permiten a los sistemas informáticos supervisores 106 determinar la relación entre varias órdenes secundarias recibidas de un intermediario (por ejemplo, la clave completa puede ser requerida para esto). La clave completa puede ser proporcionada a los sistemas informáticos clientes 102, los cuales pueden utilizar la clave completa para descifrar y asociar la información de procesamiento de órdenes secundarias que puede ser recuperada de los sistemas informáticos supervisores 106. En algunas modalidades, la información de procesamiento de órdenes secundarias puede ser publicada como un informe de acceso público, que incluye información de procesamiento asociada con varios órdenes. En algunas modalidades, la información de procesamiento está codificada.

Herramienta informática

En algunas modalidades, se puede proporcionar una herramienta informática, la cual está configurada para la correlación de claves con órdenes de clientes. La herramienta informática puede ser configurada para el análisis y reporte relacionado con el enrutamiento de órdenes a lugares.

Por ejemplo, la herramienta informática puede estar configurada para realizar análisis, como verificar que las órdenes fueron efectivamente enrutadas de acuerdo con las instrucciones, que las órdenes fueron enrutadas de acuerdo con la "mejor ejecución"; determinar las diferencias entre la "mejor ejecución" y el procesamiento de órdenes enrutados; determinar el tiempo promedio requerido para cumplir un orden; comparar precios y/o cantidades de órdenes procesados en comparación con las órdenes deseados, etc.

Esta información puede ser útil, por ejemplo, para proporcionar una visión sobre la ruta y eficiencia de su procesamiento de órdenes. En algunas modalidades, la herramienta informática compara los registros de mensajes de órdenes de clientes con los registros de mensajes codificados de servicios para el cliente y genera un informe de discrepancias.

La herramienta informática puede ser implementada como software, hardware, un servicio web, de forma individual o en varias combinaciones.

La herramienta informática puede configurarse para, por ejemplo, recibir y/o acceder automáticamente a información codificada (información de transacciones, datos de mercado, etc., recibidos de los sistemas informáticos supervisores o del sistema informático de un lugar); basándose en una copia de las órdenes del cliente (incluyendo las claves de codificación/decodificación y/o información del registro de transacciones), acceder a los datos codificados, decodificar y comparar la información con la información del cliente; y/o producir uno o más informes.

En algunas modalidades, la herramienta informática puede estar configurada para generar y/o proporcionar claves codificadas seguras para que el cliente y/o los sistemas informáticos clientes 102 las utilicen al enviar órdenes a los intermediarios y/o sistemas informáticos intermediarios 104. Por ejemplo, la herramienta informática puede incluir un generador de números aleatorios que puede generar una serie de claves para cada cliente. Estos pueden, por ejemplo,

basarse en la fecha/hora y/o un parámetro clave único definido por el personal del cliente. La herramienta informática puede incluir funciones de gestión de claves: construcción de claves, actualización de claves, alertas para crear nuevas claves, y así sucesivamente.

- 5 La generación y/o provisión de claves de codificación/codificación puede llevarse a cabo en un servicio de solicitud de clave individual y/o como un servicio en bloque.

10 Los posibles beneficios de proporcionar una herramienta informática pueden ser la reducción de los requisitos de desarrollo y/o soporte técnico, la facilidad de adopción del sistema y la facilidad de actualización y/o modificación del sistema.

15 En algunas modalidades, la herramienta informática puede estar configurada para proporcionar soporte analítico, como el desarrollo de puntos de referencia, informes, análisis estadísticos, análisis heurísticos, comparaciones con datos de condiciones del mercado, etc. La funcionalidad de soporte analítico puede respaldar varios análisis basados en información de enrutamiento histórico, métricas de enrutamiento estándar de la industria, indicadores clave de rendimiento, etc. Por ejemplo, la herramienta informática puede estar configurada para realizar análisis de causa raíz, análisis de regresión, modelado, predicción y/o pronóstico.

20 En algunas modalidades, la herramienta informática puede estar configurada para emitir automáticamente notificaciones basadas, por ejemplo, en tendencias identificadas basadas en prácticas de enrutamiento de intermediarios. Por ejemplo, la herramienta informática puede estar configurada para enviar una notificación cuando la herramienta informática identifica que un intermediario ha enrutado una orden en violación de las instrucciones de un cliente, o ha enrutado una orden en violación de las mejores prácticas.

25 Recuperación de Orden de Enmascaramiento

30 La actividad del cliente al recuperar órdenes también debe estar enmascarada. Para ocultar aún más las órdenes reales, el cliente también puede solicitar al servidor supervisor un número aleatorio de órdenes adicionales, o puede solicitar periódicamente, continuamente o aleatoriamente órdenes al servidor supervisor para ocultar cuándo el cliente está solicitando órdenes reales al servidor supervisor. Por ejemplo, la ordenador cliente puede estar configurada para solicitar datos del repositorio todos los días a una hora o horas específicas, independientemente de la actividad real de negociación del cliente.

35 Rellenando el Repositorio de Orden Público con Entradas Codificadas

40 En algunas modalidades, un repositorio que contiene información de órdenes (que puede estar codificada) puede ser expuesto al público. En consecuencia, diversas características, como el número de órdenes, la fecha en que se agregan, la longitud de los datos correspondientes a las órdenes, etc., pueden ser utilizadas por un tercero para determinar aspectos de las órdenes.

45 El sistema puede configurarse para rellenar la base de datos/repositorio público con entradas codificadas formateadas de manera que sean indistinguibles de otras entradas de órdenes codificados reales, de modo que sea más difícil determinar la fuente o las interrelaciones entre las órdenes en función del volumen o el momento del orden. El servidor supervisor puede no ser capaz de distinguir las entradas de órdenes codificadas reales de las entradas codificadas acolchadas.

50 Esto se puede lograr mediante el servidor supervisor creando y almacenando un número suficiente de entradas codificadas para enmascarar ya sea el número total de órdenes reales en el sistema, o para enmascarar el número de órdenes reales creadas dentro de un período de tiempo específico.

El número de entradas codificadas creadas y el momento de creación de las entradas codificadas pueden variar.

55 El servidor supervisor puede configurarse para generar un número fijo o aleatorio de entradas codificadas cuando se alcanza un número umbral de órdenes reales, en intervalos de tiempo aleatorios o en números umbral de órdenes reales aleatorios.

En algunas modalidades, el supervisor está configurado para no registrar qué órdenes son reales y cuáles no lo son.

60 También puede haber otras formas de generar las entradas codificadas para su registro en la base de datos, aparte de la generación realizada por el propio servidor supervisor.

65 Como el intermediario proporciona información de descodificación y de relación, tal como se describe aquí, al cliente, el intermediario y el cliente aún pueden determinar qué registros son reales y distinguir esos registros de otros registros codificados.

Búsqueda Heurística de Múltiples Etapas

En algunas modalidades, el sistema informático supervisor 106 o el componente informático del cliente pueden estar configurados para varios tipos de consultas de datos. Los enfoques heurísticos pueden proporcionar varios beneficios técnicos, especialmente cuando hay un gran volumen de datos que procesar y los recursos informáticos y/o de tiempo disponibles pueden estar limitados.

Por ejemplo, un componente informático de cliente puede consultar datos comerciales del sistema informático supervisor 106 solicitando bloques de AI. Los AI se calculan junto con los DK a partir de una combinación de los CK de los clientes asignados al orden del cliente y la secuencia de BK asignados a las órdenes secundarias.

En un caso de ejemplo de una entidad de intermediario único que reconoce las órdenes de los clientes y genera órdenes secundarias, el componente informático del cliente simplemente generaría BK_0 a través de BK_N y consultaría las operaciones correspondientes utilizando AI_0 a través de AI_N hasta que se contabilice la totalidad de la orden.

En un escenario de Multietapa, solo se puede utilizar un subconjunto de los posibles BK, dependiendo de qué entidades de intermediarios estén gestionando la orden.

La Figura 10 es una tabla 1000 que ilustra un posible escenario donde se utiliza un esquema de módulo 7 (por ejemplo, donde se utiliza un divisor de 7 para operaciones de módulo) y 4 de las entidades estuvieron involucradas en el manejo del orden, según algunas modalidades. Otros esquemas y/o valores de módulo pueden ser posibles, y la Figura 10 se proporciona con fines de ejemplo.

Las casillas con líneas cruzadas representan los índices BK utilizados para órdenes que no tuvieron ningún llenado asociado, y las casillas con líneas longitudinales representan órdenes que sí resultaron en llenado.

Los siguientes ejemplos demuestran una heurística posible que podría ser utilizada para buscar órdenes. La heurística puede utilizar varios parámetros configurables:

SWEEP = el número de columnas de BK que se barrerán exhaustivamente o buscarán (en este ejemplo se establece en 2).

BURST = el número de BK que se buscarán en una fila para ver si hay algún orden adicional para una entidad dada una vez que se haya encontrado al menos una orden (en este ejemplo se establece en 5).

MAX_SWEEPS es número máximo de veces que se repetirá el barrido para encontrar la cantidad de llenado faltante (en este ejemplo, establecido en 3).

Buscar BK 1 a 14 ($SWEEP \times modulo = 2 \times 7 = 14$) Se encontraron órdenes 2, 9 para la entidad 2 y 5, 12 para la entidad 5.

Repetir BURST a lo largo de la fila para la entidad 2 hasta que la lista completa de ráfagas de BK no contenga órdenes. Buscar 16, 23, 30, 27, 44 (órdenes encontradas), buscar 51, 58, 65, 72, 79 (órdenes encontradas), buscar 86, 93, 100, 107, 114 (órdenes encontradas), buscar 121, 128, 135, 142, 149 (órdenes encontradas), buscar 156, 163, 170, 177, 184 (órdenes no encontradas, detener búsqueda). Se encontraron rellenos pero todavía queda una cantidad mayor a 0.

Repetir BURST a lo largo de la fila para la entidad 5: Buscar 5, 12, 19, 26, 33 (órdenes encontradas), buscar 40, 47, 54, 61, 68 (órdenes encontradas), buscar 75, 82, 89, 96, 103 (órdenes no encontradas, detener la búsqueda). Cantidad encontrada, pero aún queda una cantidad restante.

Repetir los barridos hasta MAX_SWEEPS veces para intentar encontrar la cantidad de llenado faltante comenzando con los BK que aún no se han buscado: Buscar 15, 17, 18, 20, 21, 22, 24, 25, 27, 28 (no se encontró nada después del primer barrido), buscar 29, 31, 32, 34, 35, 36, 38, 39, 41, 42 (no se encontró nada después del segundo barrido), tercer y último barrido buscar 43, 45, 46, 48, 49, 50, 52, 53, 55, 56 (se encontró la orden en 55 así que hacer Burst en la Entidad 6).

Repetir BURST a lo largo de la fila para la entidad 6: Buscar 62m 69, 76, 83, 90 (encontrado en orden), buscar 97, 104, 111, 118, 125 (encontrado en orden), buscar 132, 139, 146, 153, 160 (no se encontró orden, detener búsqueda). Cantidad de llenado restante = 0, Heurística completa.

En el ejemplo anterior no se encontró la orden con índice BK 178. Si el parámetro SWEEP fuera más grande, como por ejemplo 15, se habrían encontrado 178.

Los parámetros se pueden mantener pequeños para minimizar la cantidad de datos a consultar y el tiempo de cálculo. Sin embargo, cuanto más pequeños sean, mayor será la probabilidad de encontrar una orden con grandes brechas de órdenes faltantes.

Tenga en cuenta que incluso con parámetros muy pequeños, las entidades bien comportadas (aquellas sin lagunas) se encontrarán por completo con una cantidad mínima de cálculos y consultas.

La heurística puede no encontrar todas las cantidades de llenado si existen grandes brechas en los flujos de orden, pero eso se detectará si la cantidad de llenado restante es > 0 , pero se han agotado los MAX_SWEEPS y no se han encontrado los llenados.

La heurística no detectará en absoluto órdenes no completados después de grandes brechas si las órdenes encontrados representaron el 100 % de la cantidad a completar.

En algunas modalidades, el dispositivo instructor/solicitante puede estar configurado para intentar decodificar porciones del conjunto de datos recibido de un servidor supervisor utilizando claves de al menos un conjunto de claves indexadas por módulo. Cada conjunto que contiene M claves consecutivas. Donde M representa el divisor o el número máximo de entidades de cómputo en el sistema. En el ejemplo de la Figura 10, M es 7, y cada columna representa un conjunto.

Mientras que los procesadores pueden intentar decodificar uno o más conjuntos (es decir, columnas en la Figura 10), en el ejemplo anterior, los procesadores recorren dos conjuntos (SWEEP = 2).

Basándose en si las claves en el barrido correspondiente a un solo módulo índice decodifican exitosamente porciones, los procesadores pueden intentar primero decodificar utilizando solo las claves exitosas. Por ejemplo, en la Figura 10, los módulos 2 y 5 tuvieron éxito en el barrido inicial, por lo que los intentos iniciales de decodificación de ráfagas utilizan las claves en las filas correspondientes a las entidades 2 y 5 en la Figura 10.

Técnicas, Variaciones y/o Algoritmos de Ejemplo

Varios algoritmos y/o técnicas de codificación pueden ser utilizados en cualquiera de las modalidades descritas aquí, por ejemplo:

- Un algoritmo para generar claves aleatorias de una longitud especificada (por ejemplo, un generador de números aleatorios que se puede ejecutar en modo de consulta/respuesta o llamada/retorno para generar claves individuales, y/o se puede ejecutar para generar un bloque de claves). En algunas modalidades, el algoritmo para generar claves aleatorias puede estar configurado para ser sembrado con el fin de evitar duplicaciones entre diferentes clientes (por ejemplo, se pueden generar claves pseudo únicas utilizando información de la hora del día y la fecha, dirección IP del servidor, dirección MAC, nombre del servidor), a cada cliente se le puede asociar un código de semilla "secreto" que tiene la longitud de la clave, números pseudo aleatorios, no predecibles y no reproducibles pueden ser utilizados para aleatorizar aún más la semilla, incluyendo el tamaño de los archivos temporales del sistema operativo, espacio de intercambio, recuentos de bytes de I/O en interfaces de red y uso actual de memoria y recursos en el sistema, entre otros.

- Un algoritmo de codificación/descodificación que utiliza claves de -256 bits o más grandes: dado que el tamaño del registro puede ser relativamente pequeño (~1K bytes) o solo alrededor de veinte veces más grande que la clave, el codificación y descodificación pueden llevarse a cabo mediante la generación de una cadena aleatoria de 1 kilobyte o más grande a partir de la clave y luego realizando una operación de exclusión OR (XOR) con una copia enmascarada del registro para el codificación y la operación complementaria para el descodificación. Una ventaja potencial de dicho esquema es la posible reducción de la complejidad computacional de las funciones de codificación/descodificación. En algunas modalidades, también se pueden utilizar claves de menos de 256 bits.

- Un algoritmo de hash para generar una serie de claves a partir de una única clave principal. El algoritmo de hash se puede utilizar para generar series de órdenes secundarias, cada una con una clave única.

- Almacenar datos codificados/codificados/descodificados como caracteres imprimibles/mostrables, lo cual puede reducir la complejidad asociada con la descarga de archivos binarios. Por ejemplo, se puede utilizar un esquema de codificación de 6 bits/carácter, lo cual solo resultaría en un aumento del 33 % en el tamaño del archivo/datos. En algunas modalidades, los datos codificados/codificados/descodificados almacenados como caracteres imprimibles/mostrables pueden ser utilizados para representar claves en los campos de etiquetas de mensajes FIX.

- Una función puede ser utilizada para combinar múltiples claves en una sola clave (por ejemplo, se utiliza para permitir que un intermediario genere una clave de procesamiento y luego genere una clave de destino a partir de la combinación de la clave cliente y la clave de procesamiento).

- Se puede proporcionar un esquema de codificación que permita configurar el tamaño de la clave, lo que potencialmente permitiría una expansión futura del tamaño de la clave.

Como ejemplo adicional, se pueden utilizar las siguientes técnicas para la generación de claves secundarias, codificación y decodificación de órdenes secundarias y/o otras entradas codificadas:

Un generador de claves aleatorias (por ejemplo, asumiendo una clave de 256 bits) puede ser utilizado para generar un bloque de claves utilizando un generador de números pseudoaleatorios a partir de una semilla no reproducible.

Se puede proporcionar una función de fusión de claves para fusionar 2 claves en una sola clave: Generar $K_C = f_{\text{Fusión}}(K_A, K_B)$. La función de fusión de claves debe ser una función computacionalmente ligera y debe estar configurada de tal manera que sea difícil extraer las claves originales de la clave fusionada.

El sistema puede necesitar tener funcionalidad para convertir una primera clave en una segunda clave para potencialmente generar una lista arbitraria de claves que se pueden generar a partir de una clave inicial, generando $K_{N+1} = f_{\text{Hash}}(K_N)$. El hashing debe realizarse de tal manera que sea difícil determinar la clave K_N a partir de la clave K_{N+1} o determinar que un conjunto de mensajes forma parte de una única cadena de claves.

El sistema también puede incluir funcionalidad para codificar un registro utilizando una clave, (por ejemplo, Generar $\langle \text{Registro codificado} \rangle = f_{\text{Cifrado}}(K, \langle \text{Registro No codificado} \rangle)$). Tal función también puede adaptarse para rellenar el registro y así oscurecer información relacionada en detalle.

El sistema puede incluir funcionalidad para extraer un Índice Anónimo de una clave (por ejemplo, Generar $AI = f_{AI}(K)$), y llevar a cabo diversas actividades relacionadas con registros AI, como encontrar todos los registros que coincidan con un AI, ordenar un conjunto de registros basados en un AI, descodificar un registro (por ejemplo, Generar $\langle \text{Registro No codificado} \rangle = f_{\text{Descifrado}}(K, \langle \text{Registro codificado} \rangle)$), rellenar un registro, generar una entrada codificada y generar solicitudes de AI.

Complejidad Computacional

Se pueden utilizar diversas técnicas de codificación. Una ventaja potencial de usar claves aleatorias puede ser la relativa facilidad de generar grandes números aleatorios a partir de una semilla temporal no predecible.

Por ejemplo, la entidad generadora (por ejemplo, los sistemas informáticos clientes o los sistemas informáticos intermediarios) puede generar grandes bloques de números aleatorios de antemano (por ejemplo, al inicio o como un proceso por lotes) de manera que no haya una complejidad computacional adicional durante el procesamiento de órdenes.

Los sistemas informáticos intermediarios pueden beneficiarse de una computación más rápida, ya que pueden estar generando claves para órdenes secundarias al recibir las claves de las órdenes principales.

La verificación de la información de enrutamiento puede realizarse después del horario de negociación para reducir el impacto de las actividades computacionales durante las horas pico.

En algunas modalidades, el cliente puede desear verificar la ruta de la orden en tiempo real, inmediatamente o poco después de que la orden del cliente sea procesada. Si bien esto también es posible, la anonimidad del cliente puede verse comprometida si el cliente consulta al servidor supervisor para verificar la orden inmediatamente después de realizarlo. Los observadores cercanos del servidor supervisor pueden inferir razonablemente que las órdenes realizados inmediatamente antes de las consultas de verificación de órdenes pueden estar asociados con el cliente que realiza la consulta. En consecuencia, cuando se requiere una verificación en tiempo real del enrutamiento de órdenes, la ordenador o servidor del cliente puede estar configurado para consultar constantemente el servidor supervisor. El ordenador del cliente podría entonces descartar o ignorar cualquier orden no asociada con el cliente, mientras descifra el resto. En algunas modalidades, el servidor supervisor, o un servidor separado conectado al servidor supervisor, puede estar configurado para transmitir todos los datos desde el servidor supervisor a medida que se registran allí. Cualquier ordenador cliente podría suscribirse a los datos transmitidos y extraer solo las órdenes asociadas con el cliente respectivo, por ejemplo, mediante índices anónimos conocidos por el cliente.

Enmascaramiento de órdenes

Las propias claves de codificación/codificación también pueden inadvertidamente proporcionar información a un tercero (por ejemplo, el tercero puede ser capaz de obtener información de las longitudes de las claves, patrones, etc.). Lo mismo puede ocurrir debido a las longitudes y patrones de los mensajes codificados/codificados.

En consecuencia, en algunas modalidades, las claves pueden ser de 256 bits o más largas, ya sea como la clave cliente por sí sola o como una clave híbrida proporcionada por los sistemas informáticos intermediarios.

En algunas modalidades, se utiliza un esquema de codificación de caracteres imprimibles con mensajes FIX, donde una clave de 256 bits podría representarse como una cadena de 43 caracteres.

En algunas modalidades, los mensajes de orden pueden utilizar técnicas de relleno para que haya una longitud estándar en el mensaje, lo cual puede ayudar a ocultar información que se puede obtener de las longitudes de los mensajes.

- 5 En algunas modalidades, el número total de mensajes de orden puede ser enmascarado mediante la adición de un número aleatorio de entradas codificadas.

Verificación de escala

- 10 Al realizar la verificación de la información cifrada/texto codificación, puede haber grandes volúmenes de datos involucrados. En consecuencia, la verificación puede ser intensiva en términos de cómputo y se pueden aplicar diversas técnicas para reducir los requisitos computacionales.

- 15 Por ejemplo, si un cliente envía 1 millón de órdenes, es posible que el cliente necesite intentar descifrar 1 millón de órdenes utilizando 1 millón de claves de un conjunto de 200 millones de órdenes, y dicha actividad puede ser computacionalmente desafiante. Un algoritmo de ejemplo puede requerir varios microsegundos de tiempo de CPU por intento de clave/mensaje, e incluso en un servidor de ejemplo con 16 núcleos, solo se pueden procesar 10 millones de intentos de clave/mensaje por segundo. En este ejemplo, encontrar los 1 millón de órdenes en un conjunto de 200 millones requeriría 200 billones de cálculos o alrededor de 20 millones de segundos de tiempo de CPU (aproximadamente 8 meses).

Posibles soluciones a estos problemas pueden surgir a través de la creación de un índice.

- 25 En algunas modalidades, una porción de la clave puede ser utilizada para establecer un índice (por ejemplo, de una clave de 48 caracteres, se extraería un índice de 5 caracteres, lo que resultaría en un índice de 30 bits con aproximadamente 1 mil millones de valores posibles).

- 30 El índice podría ser expuesto y asignado a cada uno de los 200 millones de registros de mensajes y preordenado según los índices.

- 35 En este ejemplo, la clave real puede ser de 48 caracteres completos (288 bits), y la clave expuesta puede ser de 5 caracteres que pueden ser expuestos. La clave sigue estando segura ya que los 43 caracteres restantes (258 bits) están ocultos.

- 40 Dado que el cliente conoce el índice de todas las 1 millón de órdenes, un primer paso puede ser encontrar los registros coincidentes para cada una de las 1 millón de órdenes basándose en el índice. La mayoría de los índices solo obtendrían una coincidencia, y un pequeño porcentaje obtendría 2 o más coincidencias, por lo que el número total de descodificaciones probablemente sería menor. Por lo tanto, la verificación puede realizarse de manera factible ya que se puede reducir el cálculo en comparación con una implementación sin el uso del índice como se describe anteriormente.

- 45 En algunas modalidades, la herramienta computacional puede estar configurada para proporcionar un servicio de consulta donde solo se descargan los índices coincidentes a solicitud del cliente. El cliente puede consultar cualquier número de indexados para descargar la información de orden asociada respectiva para ocultar las órdenes específicos y el número de órdenes que coinciden con el cliente (enmascaramiento de sobresuscripción).

El servicio puede publicar una lista de indexados existentes (no vacíos) junto con cada conjunto de datos para facilitar el enmascaramiento de esta sobresuscripción.

- 50 Formato de registro

La Figura 3 muestra un ejemplo de formato de registro, según algunas modalidades.

- 55 En algunas modalidades, los datos del mensaje codificado pueden ser almacenados en un formato que permita delimitar registros individuales, exponga la cadena de indexado para cada registro y/o permita un número de secuencia y una suma de verificación (para asegurar que todos los registros hayan sido descargados y que ninguno de ellos haya sido corrompido o truncado).

- 60 El sistema supervisor también puede almacenar los registros en un almacenamiento de datos, como una base de datos. En consecuencia, el almacenamiento de datos puede estar configurado para devolver varios valores, como 1 o 0 "registros" por consulta basada en AI. Cada "registro" puede contener cualquier número de "mensajes" concatenados, y cada mensaje puede estar codificado con su propia clave DK. Se puede realizar una "consulta", en donde se realiza una solicitud de 1 o más "registros" del almacenamiento de datos.

Dado que el tiempo de ida y vuelta de la consulta puede ser de decenas de milisegundos o más, incluso para un solo registro, los proxies, herramientas informáticas y/o otras aplicaciones que acceden a los sistemas informáticos supervisores 106 pueden mejorar la eficiencia al solicitar grandes bloques de registros (incluso miles a la vez).

5 Los datos que se almacenan en el sistema informático supervisor 106 son una serie de registros de mensajes almacenados en función del código de AI. Los datos pueden ser indexados/consultados por los siguientes campos: Fecha; AI; Código de región; y/o Tipo de instrumento/Tipo de datos.

10 El registro que se devuelve puede tener la siguiente información "encabezado" para todo el registro: Longitud del registro en bytes; y/o una suma de verificación aritmética del registro (por ejemplo, suma de verificación de 32 bits).

15 Los datos pueden ser una serie concatenada de registros, cada uno con una porción decodificada y una porción codificada. La porción decodificada, por ejemplo, puede tener un esquema de delimitación de registros, longitud del registro, un número de mensajes y una suma de verificación del registro (utilizada para validar la transmisión y el almacenamiento en búfer del registro, por ejemplo, la suma aritmética de 32 bits de todos los bytes en el registro). La porción codificada, por ejemplo, puede incluir un mensaje de datos que tenga una copia sin procesar del mensaje en su protocolo nativo (por ejemplo, FIX u otros protocolos como OUCH o SAIL); una marca de tiempo del mensaje de datos (marca de tiempo con resolución de nanosegundos); un tipo de protocolo de mensaje; y una suma de verificación del mensaje (por ejemplo, una suma de verificación que sea independiente del protocolo, como una suma aritmética de 32 bits de todos los bytes en el mensaje que se puede utilizar para validar la descodificación).

20 El mensaje de orden/transacción actual puede estar incrustado en una trama que también está codificado. Parte de la trama puede ser un código de inicio que se puede utilizar para indicar si el marco es una posible coincidencia para la clave de descodificación.

25 En otras palabras, la única forma automatizada de verificar la correcta descodificación del mensaje es comprobando el mensaje en su formato nativo (por ejemplo, FIX tiene un campo de suma de verificación estándar y comienza con una cadena estándar como "8=FIX"). Sin embargo, requiere suponer el protocolo y formato del mensaje.

30 En algunas modalidades, la complejidad puede reducirse mediante el uso de un formato de trama que encapsula el mensaje objetivo de manera que pueda utilizarse de forma independiente para verificar la validez del mensaje, independientemente del formato.

35 Por ejemplo, una trama puede comenzar con la cadena "XX" y terminar con una suma de verificación de 4 caracteres. En este ejemplo, todos los caracteres intermedios serían el mensaje original codificado. Puede haber beneficios potenciales, ya que dicha implementación puede permitir el manejo de mensajes que no están formateados como mensajes FIX, como formatos de mensajes binarios que pueden ser utilizados por algunos intercambios.

40 Los registros también pueden incluir, por ejemplo:

Una CryptoKey: Esta etiqueta contiene las claves CK o DK/AI. Esta clave es utilizada por el servicio Supervisor para codificar e indexar el mensaje en el almacén de datos del Supervisor.

45 Un BrokerKey proporcionado por los intermediarios aguas arriba en las órdenes de llenado/ACK para indicar la primera clave de una secuencia de claves asignadas a las órdenes secundarias. Esta etiqueta es requerida si un intermediario está manejando una orden que tenía CryptoKey establecido por el cliente y el intermediario ha generado una o más claves de intermediario para las órdenes secundarias salientes. Este campo puede ser, por ejemplo, una cadena que representa una clave BR de 512 bits codificada en BASE64. Se puede utilizar en el mensaje ACK enviado por un intermediario a un cliente/intermediario al recibir una nueva orden con un CK. Esta etiqueta también se puede utilizar internamente dentro de una pila de intermediarios para comunicar claves BK entre entidades dentro de la pila.

50 BrokerMode esta etiqueta indica cómo el intermediario está manejando las órdenes del supervisor. Esta etiqueta es un carácter y puede tener uno de los siguientes valores: 'A' – se utiliza el esquema de codificación de clave CK.BK completo; 'C' - la clave está completamente controlada por el cliente; 'B' - la clave está completamente controlada por el intermediario; 'P' - el cliente no está provisto para el almacenamiento de órdenes de supervisor; y 'X' - el cliente ha elegido no almacenar esta orden en un sistema informático supervisor.

60 Convenciones

La metodología del supervisor puede requerir que las claves criptográficas sean pasadas entre los clientes, los intermediarios y el supervisor. Para simplificar esta metodología lo máximo posible y permitir su implementación a través de una metodología simple de paso de etiquetas, se pueden seguir las siguientes convenciones:

65 Si una entidad recibe una clave que es más corta de lo esperado, por ejemplo, si un intermediario espera una clave CK de 256 bits, pero solo recibe una clave de 128 bits, el campo puede ser rellenado al frente con ceros para crear la

longitud de clave esperada. Por ejemplo, si se espera una clave de 8 dígitos y se recibe 12345, se puede rellenar con ceros para obtener 00012345. Si una clave tiene dos partes, como en el caso de una DK y AI, entonces la clave de codificación/codificación, en este caso DK, es el lado izquierdo de la clave, y AI es el lado derecho de la clave.

5 A continuación se presentan algunos ejemplos donde se espera un DK de 8 dígitos y se espera un AI de 2 dígitos: Si se recibe una clave de 10 dígitos, los 8 dígitos de la izquierda son el DK y los 2 dígitos de la derecha son el AI. Por ejemplo, si se recibe 1234567890, entonces DK es 12345678 y AI es 90.

10 Si se recibe una clave más larga con 14 dígitos, entonces nuevamente DK son los 8 dígitos más a la izquierda, y AI son los 2 dígitos más a la derecha. Por ejemplo, si se recibe 12345678909876, el DK es 12345678 y el AI es 76. El 9098 del medio es descartado.

15 Si se recibe una clave acortada con 8 o 9 dígitos, entonces se aplica la misma regla. Por ejemplo, si se recibe 87654321, entonces se utiliza la clave completa para DK, 87654321, y los dos dígitos más a la derecha, 21, son el AI.

Si se recibe una clave aún más corta, por ejemplo, con solo 5 dígitos, entonces la clave se completa y luego se aplican las reglas anteriores para DK y AI. Por ejemplo, si se recibe 54321, se rellena con ceros a la izquierda hasta obtener 00054321, y eso se convierte en el DK, mientras que los dos dígitos más a la derecha, 21, se convierten en el AI.

20 Esta metodología potencialmente ayuda a solucionar problemas con los números 0 acolchados delanteros que se manejan incorrectamente. Básicamente, numéricamente 0123 es el mismo número aritmético que 123, pero criptográficamente son diferentes, por lo que al agregar ceros a la izquierda, este problema puede resolverse.

25 El objetivo es hacer que el sistema informático supervisor funcione si el intermediario pasa la clave CK del cliente al sistema informático supervisor sin asignar nunca las claves BK, y luego generar las claves DK y AI. Utilizando la convención anterior, la metodología puede funcionar incluso si CK es más pequeño o más grande que el DK y AI requeridos.

30 Esta metodología puede facilitar la compatibilidad hacia atrás y hacia adelante si las funciones de codificación y hash se cambian o mejoran en el futuro. La implementación de nuevas tecnologías puede ser incremental al mismo tiempo que se mantiene la compatibilidad hacia atrás y hacia adelante. Este protocolo de paso de clave se utiliza para CK, BK, DK y AI, y cualquier nueva clave en el futuro.

35 Intermediario como Cliente

En algunos casos, el intermediario puede recibir órdenes de un segundo cliente que a su vez es un intermediario para un primer cliente. Puede ser deseable que el segundo cliente pueda verificar las acciones del intermediario. También puede ser deseable que el primer cliente pueda verificar las acciones del intermediario del primer cliente, así como del intermediario del segundo cliente. En algunas modalidades, el servidor supervisor de la presente invención puede ser utilizado como supervisor entre los intermediarios, además de ser utilizado como supervisor entre el intermediario final que realiza órdenes y los lugares. Opcionalmente, el intermediario del primer cliente puede compartir la clave intermediaria del primer cliente con el primer cliente, y también puede transmitir esa clave al intermediario del segundo cliente para que el intermediario del segundo cliente pueda generar órdenes secundarias utilizando la clave compartida entre ambos clientes. De esta manera, tanto el intermediario del primer cliente como el primer cliente podrían recuperar y descifrar la información de la orden del servidor supervisor. Alternativamente, el segundo cliente y el intermediario pueden utilizar una segunda clave que no se comparte con el primer cliente. Opcionalmente, la segunda clave puede estar basada en o derivada de una primera clave compartida entre el primer cliente y el intermediario del primer cliente.

50 Ejemplos de Modalidades

La siguiente sección describe algunas modalidades. Se pueden contemplar otros modos de realización y estos modos de realización se proporcionan como ejemplos. Además, los mismos, diferentes, menos y/o elementos alternativos pueden incluirse en varias otras modalidades.

55 En algunas modalidades, puede haber una ventaja potencial al implementar el servidor supervisor como un servidor separado del intermediario o del lugar, ya que el supervisor puede estar mejor equipado para consolidar todas las órdenes en una base de datos, logrando posiblemente una máscara más sólida de las órdenes de los clientes que si cada intermediario o lugar mantuviera su propio servidor supervisor operando en hardware o software.

60 Ejemplo 1

En algunas modalidades, un cliente puede transmitir una orden sin cifrar junto con una clave cliente proporcionada por el cliente a través de un canal seguro a un intermediario.

65 El canal seguro en sí mismo puede estar codificado, etc., pero la orden no está codificada con la clave cliente. La clave cliente puede estar incrustada como una etiqueta o campo en la orden. El cliente mantiene un registro de claves y

órdenes de clientes, por ejemplo, en una base de datos 110 mantenida por el cliente. La base de datos 110 puede ser implementada utilizando diversas tecnologías de bases de datos, como bases de datos relacionales (por ejemplo, bases de datos SQL), bases de datos planas, hojas de cálculo de Excel, valores separados por comas, etc. Si la base de datos 110 se implementa utilizando tecnología de base de datos relacional, la base de datos de almacenamiento 110 puede estar configurada para almacenar además las relaciones entre varios registros de datos. La base de datos de almacenamiento 110 puede implementarse utilizando diversas tecnologías de hardware o software, como unidades de estado sólido o discos duros, matrices redundantes de discos independientes, almacenamiento en la nube, dispositivos de almacenamiento virtuales, etc.

El intermediario puede generar órdenes secundarias basadas en la orden del cliente y enviar cada orden al supervisor con un hash de la clave cliente para que cada orden pueda ser vinculada a la orden original del cliente. El hash puede ser específico del cliente, específico del intermediario, específico de la relación cliente intermediario, etc.

El supervisor puede mantener un registro sobre las órdenes enviados a uno o más lugares y su clave secundaria asociada, y enviar las órdenes a los lugares, las órdenes siendo despojados de cualquier información clave.

El supervisor puede entonces publicar públicamente todas las transacciones (órdenes, cancelaciones, reemplazos, llenados, etc.), codificadas con la clave secundaria correspondiente.

Un cliente puede acceder/recuperar información de transacciones y verificar transacciones reales con órdenes enviadas al intermediario utilizando el registro mantenido por el cliente. En algunas modalidades, se puede utilizar una herramienta informática para la verificación y/o análisis de las órdenes.

Ejemplo 2

En algunas modalidades, en lugar de que un cliente proporcione una clave cliente, un intermediario, al recibir una orden de un cliente, genera una clave cliente y la comunica de vuelta al cliente. Por ejemplo, el intermediario puede comunicar la clave cliente utilizando en el transcurso de un mensaje de confirmación.

Ejemplo 3

En algunas modalidades, puede no haber un supervisor y los lugares pueden recibir las órdenes secundarias y las claves. Los lugares pueden además codificar la información de transacción utilizando las claves y los clientes pueden recuperar y acceder a esta información, decodificarla y utilizarla para verificar las características asociadas con el enrutamiento de sus órdenes. Por ejemplo, el cliente puede comunicarse directamente con el lugar correspondiente para obtener la información de enrutamiento del orden. Por ejemplo, uno o más lugares pueden informar información de enrutamiento de órdenes a un servidor supervisor después de haber recibido órdenes de intermediarios. El cliente puede luego recuperar la información de enrutamiento del orden de uno o más lugares desde el servidor supervisor único.

Ejemplo 4

En algunas modalidades, se pueden utilizar claves asimétricas. Por ejemplo, un cliente puede exponer una clave pública que puede ser utilizada para cifrar la información de orden relacionada con las órdenes del cliente. El cliente puede mantener una copia de la clave privada asociada para su uso en la decodificación.

Ejemplo 5

En algunas modalidades, un intermediario puede agregar un número de secuencia al final de la clave cliente y luego hacer un hash para crear las claves secundarias. Una implementación de este tipo puede ser útil para que un cliente determine cuántas órdenes secundarias pueden estar asociadas con su orden principal.

Ejemplo 6

En algunas modalidades, el intermediario asigna una clave de procesamiento a cada orden del cliente, comunica la clave de procesamiento al cliente y luego genera una clave de destino para cada orden secundaria hacia el mercado basada en una combinación de la clave cliente y la clave de procesamiento.

Ejemplo 7

En algunas modalidades, se asocia un índice a la información de la transacción para ayudar en la identificación de qué órdenes pertenecen a un cliente. Por ejemplo, el índice puede establecerse mediante la exposición de una porción de la clave, o utilizando diferentes hashes de la clave para actuar como índice.

Un cliente puede descargar y/o procesar únicamente la información que tenga los índices adecuados, lo que potencialmente reduce el tiempo computacional total requerido para la verificación.

Ejemplo 8

En algunas modalidades, el supervisor o el lugar pueden almacenar en búfer los mensajes y/o rellenar los mensajes de manera que tengan un tamaño uniforme. En algunas modalidades, el supervisor o el lugar pueden almacenar en búfer los mensajes y/o rellenar los mensajes de manera que tengan un tamaño aleatorio.

Ejemplo 9

En algunas modalidades, los clientes pueden estar configurados para descargar índices adicionales o todos los índices para enmascarar órdenes.

Ejemplo 10

En algunas modalidades, el supervisor o el lugar pueden agregar entradas codificadas al azar a la información proporcionada.

Ejemplo 11

En algunas modalidades, el supervisor puede estar configurado para recopilar datos de solicitud para rutas en las que no hay sistemas intermediarios (es decir, 0 saltos). En tales situaciones, el supervisor puede recibir datos de solicitud que se enrutan directamente desde un dispositivo instructor a un dispositivo de destino sin intermediarios. Si bien no necesariamente proporciona información desconocida sobre los detalles de la solicitud, los datos de la solicitud pueden incluir marcas de tiempo, tasas de llenado y otra información para comparar con el rendimiento del intermediario y/o simplemente proporcionar una imagen más completa de las actividades de un sistema instructor.

Parámetros de computación

La selección de parámetros informáticos puede ser relevante para algunas modalidades en vista de la capacidad y/o necesidad de escalar para manejar un gran número de órdenes y/o órdenes enrutados. La complejidad y/o el volumen de la codificación provoca que las restricciones en los recursos disponibles (por ejemplo, procesadores, memoria, tiempo) se conviertan en un problema no trivial de resolver. Además, una mayor complejidad computacional en relación con las claves de codificación puede ser preferible para mejorar la capacidad de ocultar y/o mantener la confidencialidad, pero puede haber efectos correspondientes aguas abajo cuando sea necesario descifrar las claves para la verificación de órdenes.

En algunas modalidades, los sistemas informáticos intermediarios 104 o los sistemas informáticos supervisores 106 pueden llevar a cabo la generación de diversas claves criptográficas. Estas claves criptográficas pueden, como se describe en algunas de las modalidades anteriores, configurarse de tal manera que exista una relación persistente a lo largo de generaciones de claves, la cual, si se conoce de antemano, puede utilizarse para "reconstruir" claves si se conoce una "clave semilla".

En algunas modalidades, varias claves de codificación pueden ser precalculadas por las diferentes entidades y/o sistemas informáticos asociados. Por ejemplo, se pueden generar bloques de CK utilizando números aleatorios/pseudoaleatoria independientes que pueden generarse automáticamente en un sistema informático supervisor 106 o un proxy, para su uso con clientes y/o intermediarios.

Se pueden establecer y/o precalcular varios números de claves, que pueden corresponder al número de claves requeridas para un día, o en algunas modalidades, un número adicional de claves. Las claves no utilizadas pueden ser utilizadas en días posteriores (los números aleatorios no caducan), y además, las claves BK pueden generarse en bloques de claves. Si bien la clave inicial en cada bloque puede ser un número aleatorio independiente, cada bloque puede necesitar ser un bloque de BK de tamaño prácticamente infinito.

En lugar de calcular grandes cantidades de BK ejecutando repetidamente SHA512, se pueden generar un número finito de BK que luego se pueden organizar en una matriz multidimensional para facilitar su manejo. Por ejemplo, un hipercubo de cuatro dimensiones de 29x29x29x29 requeriría la generación de 116 BK utilizando SHA512, y luego podría generar 707,281 BK mediante la operación X-OR de cuatro BK para cada campo en el hipercubo. Otros tipos de matrices, que tienen un número n de dimensiones, pueden ser utilizados, y un hipercubo de 4 dimensiones se proporciona únicamente como ilustración. En consecuencia, se pueden proporcionar una gran cantidad de BK disponibles para que, en el improbable caso de que se utilicen todos los BK, un algoritmo simplemente pueda volver a empezar y seguir utilizando la matriz con un efecto limitado y/o nulo en la seguridad de los datos o en el procesamiento. Usar un número primo como 31 para las dimensiones puede ayudar a mejorar el uso de los BK disponibles.

Usando el ejemplo anterior, un sistema podría precalcular 100K bloques BK (cada uno con 117 entradas BK0 + BK1 hasta BK116). Esto requeriría un poco más de 1 GB de almacenamiento (en RAM) y proporcionaría bloques BK para 100K órdenes principales.

El número de bits utilizados para el codificación también puede ser un factor y/o parámetro importante para la selección. Por ejemplo, se pueden seleccionar varios tipos de parámetros de codificación, como los siguientes: CK - 128 bits, DK - 128 bits, BK - 256 bits, AI - 32 bits, SHA256 puede ser utilizado para generar bloques de BK, AES128 puede ser utilizado para codificar los mensajes utilizando DK.

Como otro ejemplo, el aumento de la potencia de cálculo disponible en procesadores superiores a 32 bits (por ejemplo, procesadores de 64 bits y/o ordenadores cuánticos), y por lo tanto se pueden seleccionar parámetros que aprovechen este aumento de capacidad de procesamiento para mejorar la seguridad (por ejemplo, con mayor potencia de cálculo, las partes malintencionadas también pueden aplicar la mayor potencia de cálculo para descifrar claves criptográficas [por ejemplo, ataques de fuerza bruta, ataques de cumpleaños]).

Por ejemplo, el tiempo de cálculo para AES256 frente a AES128 en un procesador de 64 bits es solo un 30 % mayor y puede ofrecer un enfoque viable. Asimismo, calcular SHA512 frente a SHA256 en un procesador de 64 bits puede requerir menos del 25 % de tiempo de cálculo adicional.

En consecuencia, en algunas modalidades, una implementación puede utilizar los siguientes parámetros de codificación: CK - 256 bits, DK - 256 bits, BK - 512 bits, AI - 40 bits, SHA512 para generar bloques de BK, y AES256 para codificar los mensajes usando DK.

Una motivación para este cambio puede ser mejorar la seguridad de codificación al utilizar AES256, lo cual puede proporcionar un estándar más fuerte para la codificación de clave simétrica. El esquema de AI puede mejorarse para que los intermediarios puedan utilizar un subconjunto de dígitos significativos en cualquier día dado para almacenar en una base de datos e indexar mensajes utilizando AI. Tal implementación puede ayudar en la escalabilidad del esquema de búsqueda de AI y la base de datos sin necesidad de cambiar el protocolo o la función de las herramientas de intermediación o el proxy.

Con referencia a la implementación de ejemplo en la Figura 9, un dispositivo/sistema informático de cliente puede estar asociado con un cliente que desea proporcionar instrucciones relacionadas con un resultado específico (por ejemplo, un deseo de comprar, vender un activo subyacente en particular). Puede haber otras instrucciones asociadas, como parámetros sobre cómo debería llevarse a cabo dicha transacción, o restricciones relacionadas con la misma. Por ejemplo, el cliente puede desear el mejor precio posible, la mejor ejecución posible, el uso solo de ciertos tipos de enrutamiento y/o intermediarios, el uso solo de ciertos lugares, la ejecución que se realice de forma escalonada y/o basada en una secuencia de tiempo (por ejemplo, para garantizar una llegada/ejecución sincronizada, ejecución retrasada), etc.

El cliente, a través de los sistemas informáticos clientes 102, puede emitir una solicitud a una institución financiera, que, por ejemplo, puede actuar como intermediario o en conjunto con varios intermediarios para llevar a cabo las instrucciones del cliente. Es importante destacar que la institución financiera y/o los intermediarios pueden tener una considerable discreción en cuanto a cómo debe llevarse a cabo la transacción, y en algunas circunstancias, la institución financiera y/o los intermediarios pueden estar obligados a elegir entre diferentes opciones y/o posibilidades al realizar las transacciones y/o pasos de la transacción. En algunos enfoques convencionales, ha sido difícil para un cliente determinar si las instrucciones del cliente fueron llevadas a cabo de manera alineada con los intereses del cliente.

En consecuencia, se han planteado algunas preocupaciones sobre la corrección de las acciones de los intermediarios y/o subordinados. Además, algunos intermediarios están siendo sometidos a escrutinio regulatorio en relación con la ejecución de órdenes de clientes recibidas por el intermediario y pueden desear reducir y/o simplificar la carga de informes regulatorios utilizando dicho sistema. El sistema de verificación de enrutamiento también puede ser utilizado en otros contextos, por ejemplo, para identificar dónde los dispositivos y/o procesos están incumpliendo los estándares de transacción (por ejemplo, no transmitir operaciones a tiempo, lo que lleva a órdenes no ejecutadas o precios desfavorables), para identificar dónde los dispositivos están fallando, para identificar diferencias en el rendimiento entre intermediarios/mercados/ruteadores de intermediarios, entre otros.

En este ejemplo, los sistemas de instituciones financieras pueden incluir una variedad de componentes diferentes, que pueden incluir, por ejemplo, sistemas de pre o postprocesamiento, un sistema de enrutamiento inteligente (por ejemplo, una plataforma que se puede utilizar para la normalización de latencia), dispositivos/proxies de red y similares. El cliente puede transmitir instrucciones a los sistemas de la institución financiera a través de un sistema informático instructor vinculado a un sistema supervisor, estando configurado el sistema informático supervisor para facilitar la verificación de órdenes de enrutamiento basadas en información proporcionada por el sistema informático intermediario.

En algunas modalidades, el sistema informático del instructor puede incluir una capa de aplicación lógica, como una interfaz que puede configurarse para interoperar como una extensión del sistema informático intermediario.

En algunas modalidades, el sistema informático intermediario está conectado a los sistemas informáticos intermediarios (en este ejemplo, el centro de datos de la institución financiera) y está configurado para obtener

información relacionada con las órdenes realizadas por los sistemas informáticos intermediarios y enviadas a los sistemas informáticos del lugar. El sistema informático intermediario puede recibir la información del orden y luego transmitir la orden al lugar, o en algunas modalidades, el sistema informático intermediario puede simplemente "interceptar" las comunicaciones para recuperar la información que se está comunicando (por ejemplo, los sistemas informáticos intermediarios interactúan directamente con los sistemas informáticos del lugar), y por lo tanto, el sistema informático intermediario puede recibir información de operaciones con varias etiquetas que encapsulan varias claves de codificación que representan etiquetas utilizadas para identificar a qué cliente/instrucción del intermediario pertenece cada orden, etc. En algunas modalidades, también se pueden capturar los acuses de recibo de las órdenes y extraer información, como etiquetas, de las señales de acuse de recibo.

Las claves/etiquetas criptográficas pueden generarse en varias etapas de la transacción y por varias partes, por ejemplo, por el cliente, por un proxy asociado con un cliente, un sistema informático intermediario, un sistema informático de lugar, etc. Estas etiquetas pueden ser utilizadas según se describe en toda esta especificación, y por ejemplo, puede haber una clave criptográfica del cliente que sería recibida de un cliente y luego pasada a través de una pila electrónica (por ejemplo, intermediarios, lugares, varios sistemas informáticos).

Dependiendo del modo de operación, la etiqueta se pasaría en todas las órdenes de clientes o se utilizaría por entidades generadoras de órdenes secundarias para generar claves DK, AI.

Una clave intermediaria puede ser una etiqueta que se comunica de vuelta al cliente para indicar la clave BK que fue asignada a la orden del cliente por el intermediario. Esta etiqueta puede ser transmitida hacia adelante a través de la pila para indicar a todas las entidades que generan órdenes secundarias que se seleccionó BK0 para esta orden del cliente.

Puede haber una etiqueta "brokermode" que también se puede transmitir, indicando cómo se procesará una orden por el intermediario. La etiqueta "brokermode", por ejemplo, puede ser un carácter que tenga varios valores que pueden indicar diferentes modos de operación.

Ejemplos de modos de operación pueden incluir: 'A' - se utiliza el esquema de codificación de clave CK.BK completo; 'C' - la clave está completamente controlada por el cliente; 'B' - la clave está completamente controlada por el intermediario; 'P' - el cliente no está provisto para el almacenamiento de órdenes intermediarias; y 'X' - el cliente ha elegido no almacenar esta orden en el intermediario.

Por ejemplo, si un intermediario recibe una orden que no tiene una etiqueta de clave cliente, entonces hay tres opciones:

El cliente no puede ser provisto para enviar órdenes habilitadas por intermediarios en esta sesión, por lo que no se deben proporcionar las etiquetas de clave intermediaria o modo de intermediario en el mensaje ACK o en cualquier mensaje de retorno posterior.

El cliente está configurado para enviar órdenes habilitadas por intermediarios en esta sesión con los CK proporcionados por el cliente. Por lo tanto, el cliente ha decidido no enviar estos órdenes a través del intermediario al omitir la etiqueta clave cliente. El intermediario no devolverá la etiqueta de clave intermediaria en el ACK. El intermediario enviará de vuelta la etiqueta de modo de intermediario con un valor (por ejemplo, un valor de 'X'), confirmando que la orden no se almacenará en el sistema informático intermediario.

El cliente está configurado para enviar todas las órdenes a través del sistema informático intermediario, pero el cliente simplemente quiere que el intermediario asigne las claves. El intermediario debe devolver el BK0 asignado a la orden en la etiqueta de clave cliente, y un valor (por ejemplo, una 'B') en la etiqueta de modo de intermediario indicando que la asignación de clave está controlada por el intermediario.

Si el intermediario recibe una orden que tiene una etiqueta de clave cliente, entonces hay tres opciones:

Si el cliente no está configurado para enviar órdenes habilitadas para intermediarios en esta sesión, entonces no se debe devolver la etiqueta de clave intermediaria y la etiqueta de modo del intermediario debe establecerse en un valor (por ejemplo, 'P') que indique que el cliente no está configurado para órdenes habilitadas para intermediarios.

Si el cliente está configurado para enviar órdenes habilitadas para intermediarios en esta sesión, el intermediario puede querer pasar únicamente la etiqueta del cliente al servicio intermediario. En este caso, la etiqueta clave intermediaria no sería devuelta al cliente, y la etiqueta de modo intermediario se establecería en un valor (por ejemplo, 'C') que indica que la clave asignada está completamente controlada por el cliente.

Alternativamente, el intermediario puede implementar la estrategia de clave intermediaria. La etiqueta clave intermediaria se establecería en la clave BK0 que el intermediario asignó a esta orden del cliente. La etiqueta brokermode se establecería en un valor (por ejemplo, 'A') que indica que se está utilizando el esquema criptográfico completo CK, BK.

Los datos pueden ser almacenados en los sistemas informáticos intermediarios en diversas formas, como en un almacenamiento de base de datos y/o almacenamiento de datos, con varios registros. Por ejemplo, los registros pueden estar configurados para llevar a cabo diversas consultas asociadas con diversas solicitudes.

En algunas modalidades, el sistema informático intermediario también puede recibir información proporcionada por los sistemas informáticos del lugar, como datos de mercado, información de confirmación de operaciones, etc. Esta información puede ser utilizada por el sistema informático intermediario para determinar si la operación fue debidamente ejecutada por el lugar, o si otros factores interfirieron con la operación (causando que la operación se perdiera, que se perdiera el precio deseado, etc.). Por ejemplo, un intermediario puede en secreto dirigir una operación a un lugar particularmente lento que ofrece un incentivo financiero significativo para el intermediario. El comercio puede ser ejecutado de manera deficiente y dicha información puede ser transmitida en la correspondiente salida de datos por los sistemas informáticos del lugar.

Flujos de trabajo de ejemplo

La siguiente sección describe algunos flujos de trabajo de ejemplo 1300, 1400 y 1500 que pueden ser realizados por varios sistemas, dispositivos, módulos y/o componentes, según algunas modalidades. Más, menos, diferentes y/o pasos alternativos pueden ser posibles, en diferentes órdenes, permutaciones y/o combinaciones.

La Figura 12 es un ejemplo de flujo de trabajo que proporciona los pasos de un método de ejemplo desde la perspectiva de un intermediario, según algunas modalidades. El flujo de trabajo 1200 puede llevarse a cabo, por ejemplo, en un sistema para gestionar procesos de datos en una red de recursos informáticos (por ejemplo, un dispositivo informático de intermediario), el sistema que comprende al menos un procesador configurado para ejecutar instrucciones interpretables por máquina.

En 1202, un dispositivo informático de intermediario puede recibir, desde un dispositivo instructor, una solicitud principal para ejecutar un proceso de datos principal ejecutable por recursos informáticos. En algunas modalidades, el dispositivo instructor también puede proporcionar al menos una clave instructora. En algunas modalidades, el dispositivo informático del intermediario puede estar configurado para generar al menos una clave instructora y generar señales para comunicar al menos una clave instructora al dispositivo instructor.

En 1204, el dispositivo informático del intermediario puede generar solicitudes secundarias para enrutamiento hacia al menos un dispositivo de destino correspondiente cada dato secundario, cada una de las solicitudes secundarias para ejecutar al menos una parte de la solicitud principal e incluir una clave de destino derivada de al menos una clave instructora. En algunas modalidades, generar al menos una solicitud secundaria implica generar una pluralidad de solicitudes secundarias.

En 1206, el dispositivo informático del intermediario puede seleccionar una secuencia de claves de destino, cada clave de destino en la secuencia para incluirse en una solicitud secundaria correspondiente de la pluralidad de solicitudes secundarias. Seleccionar una secuencia de claves de destino, por ejemplo, puede implicar aplicar una función hash a al menos una clave instructora para generar una primera clave de destino en la secuencia y generar una clave de destino posterior en la secuencia aplicando una función hash a una clave de destino previa en la secuencia.

En algunas modalidades, al menos uno de (i) un algoritmo de hash para seleccionar la secuencia de claves, (ii) y una secuencia predeterminada de claves de la cual se seleccionan las claves de destino de la secuencia, se comparten entre el sistema y el dispositivo instructor.

En algunas modalidades, el dispositivo informático del intermediario puede estar configurado para realizar un hash de al menos una clave instructora con una clave intermedia para generar al menos una clave de destino y transmitir al dispositivo instructor un mensaje que incluya la clave intermedia.

El dispositivo informático del intermediario también puede estar configurado para codificar una secuencia de claves intermedias con al menos una clave instructora o derivados de al menos una clave instructora para generar al menos una clave de destino.

En 1208, el dispositivo informático del intermediario puede enrutar cada una de las solicitudes secundarias a al menos un dispositivo de destino correspondiente.

La Figura 13 es un ejemplo de flujo de trabajo que proporciona los pasos de un método de ejemplo desde la perspectiva de un supervisor, según algunas modalidades. El flujo de trabajo 1300 puede llevarse a cabo, por ejemplo, en un sistema para gestionar procesos de datos en una red de recursos informáticos (por ejemplo, un dispositivo informático supervisor), el sistema que comprende al menos un procesador configurado para ejecutar instrucciones interpretables por máquina.

En 1302, un dispositivo informático supervisor puede recibir al menos una solicitud secundaria que se está enrutando desde un dispositivo intermediario hacia al menos un dispositivo de destino correspondiente, la al menos una solicitud

secundaria solicita la ejecución de al menos un proceso de datos secundario correspondiente, cada uno de los al menos un proceso de datos secundario para ejecutar al menos una parte del al menos un proceso de datos principal desde un dispositivo instructor, y cada una de las al menos una solicitud secundaria incluye una clave de destino derivada al menos en parte de la al menos una clave instructora.

5 En algunas modalidades, el dispositivo informático supervisor recibe de un dispositivo solicitante al menos uno de: una clave instructora, una clave intermedia y una clave de indexado, y genera señales para comunicar solicitudes secundarias asociadas con al menos uno de ellos: (i) la clave instructora, (ii) la clave intermedia y (iii) la clave de indexado para el dispositivo solicitante.

10 La al menos una solicitud secundaria puede ser recibida, por ejemplo, desde uno o más dispositivos de toma en una o más rutas entre el dispositivo intermediario y el al menos un dispositivo de destino correspondiente.

15 En 1304, el dispositivo informático supervisor puede almacenar la al menos una solicitud secundaria en al menos un dispositivo de almacenamiento 110. En algunas modalidades, el dispositivo informático supervisor puede estar configurado para almacenar la al menos una solicitud secundaria en asociación con un identificador que identifica un mecanismo mediante el cual la al menos una solicitud secundaria fue obtenida por el sistema.

20 En 1306, el dispositivo informático supervisor puede generar señales para comunicar las solicitudes secundarias a uno o más dispositivos solicitantes. En algunas modalidades, el dispositivo informático supervisor puede estar configurado para cifrar cada una de las al menos una solicitud secundaria con su correspondiente clave de destino antes de generar las señales para comunicar las solicitudes secundarias.

25 En algunas modalidades, en el paso 1308, la clave de destino y/o la clave de indexado pueden ser eliminadas de al menos una solicitud secundaria antes de transmitir la al menos una solicitud secundaria a al menos un dispositivo de destino correspondiente en el paso 1310.

30 En algunas modalidades, el al menos un dispositivo de destino puede ser otro dispositivo intermediario, y el dispositivo informático supervisor puede estar configurado para recibir al menos una clave intermediaria del otro dispositivo intermediario, y almacenar la al menos una clave intermediaria asociada a la al menos una solicitud secundaria asociada.

35 En algunas modalidades, un dispositivo solicitante particular que tiene al menos una clave instructora particular puede decodificar la solicitud secundaria cifrada correspondiente para identificar al menos un proceso de datos secundario enrutado para ejecutar al menos un proceso de datos principal particular asociado con la clave de destino particular.

40 La Figura 14 es un ejemplo de flujo de trabajo que muestra los pasos de un método de ejemplo desde la perspectiva de un cliente, según algunas modalidades. El flujo de trabajo 1400 se puede realizar, por ejemplo, en un sistema para gestionar procesos de datos en una red de recursos informáticos (por ejemplo, un dispositivo informático cliente), el sistema comprende al menos un procesador configurado para ejecutar instrucciones interpretables por máquina.

45 En 1402, el dispositivo informático del cliente puede transmitir, desde un dispositivo instructor a un dispositivo intermediario, al menos una clave instructora y una solicitud principal para la ejecución de al menos un proceso de datos principal ejecutable por una pluralidad de recursos informáticos, la solicitud principal para enrutamiento como al menos una solicitud secundaria por el dispositivo intermediario para su ejecución por al menos un destino. En algunas modalidades, en lugar de transmitir la al menos una clave instructora, el dispositivo informático del cliente recibe al menos una clave intermedia del dispositivo intermediario.

50 En 1404, el dispositivo informático del cliente puede recibir, desde un servidor supervisor, un conjunto de datos que incluye datos asociados con una pluralidad de solicitudes.

55 En 1406, el dispositivo informático del cliente puede identificar porciones del conjunto de datos asociadas con al menos una solicitud secundaria utilizando al menos una clave de instrucción o derivados de al menos una clave de instrucción. En algunas modalidades, la identificación de las porciones del conjunto de datos asociadas con al menos una solicitud secundaria se basa al menos en parte en al menos una clave intermediaria.

60 En 1408, el dispositivo informático del cliente puede intentar decodificar porciones del conjunto de datos utilizando la al menos una clave de instrucción o derivados de la al menos una clave de instrucción e identificar las porciones del conjunto de datos decodificadas exitosamente.

En 1410, el dispositivo informático del cliente puede asociar una porción identificada del conjunto de datos con al menos una solicitud principal.

65 En algunas modalidades, el dispositivo informático del cliente puede estar configurado para generar al menos uno de: al menos una clave de indexado y al menos una clave de destino basada en al menos una clave instructora y al menos

una clave intermedia; e identificar las porciones del conjunto de datos asociadas con al menos una solicitud secundaria se basa al menos en parte en al menos una de las claves de indexado y las claves de destino.

5 En algunas modalidades, el dispositivo informático del cliente puede estar configurado para generar al menos uno de (i) al menos una clave de indexado y (ii) al menos una clave de destino basada en al menos uno de (i) al menos una clave instructora y (ii) al menos una clave intermedia; y enviar al servidor supervisor una solicitud de un conjunto de datos correspondiente a al menos una de las siguientes opciones: la al menos una clave instructora y la al menos una clave intermedia.

10 En algunas modalidades, cuando las porciones identificadas del conjunto de datos incluyen datos asociados con una solicitud secundaria para un segundo dispositivo intermediario, el dispositivo informático del cliente puede estar configurado para identificar o solicitar porciones adicionales del conjunto de datos que están asociadas con solicitudes terciaria enviadas por el segundo dispositivo intermediario.

15 En algunas modalidades, el dispositivo informático del cliente puede estar configurado para generar o seleccionar derivados de al menos uno de: el al menos una clave instructora, al menos una clave intermedia y al menos una clave de indexado para identificar las porciones del conjunto de datos asociadas con el al menos una solicitud secundaria.

General

20 Aunque varias modalidades descritas aquí se refieren específicamente a la verificación de la ruta de orden entre clientes y intermediarios, la presente invención puede aplicarse a varias partes para proporcionar la verificación de transacciones en otros tipos de partes en una cadena de relaciones. Por ejemplo, la verificación de una variedad de órdenes o adquisiciones de materiales, bienes o servicios en nombre de un cliente puede ser posible de acuerdo con la presente invención.

25 Las modalidades de los dispositivos, sistemas y métodos descritos aquí pueden ser implementados en una combinación de hardware y software. Estas modalidades pueden ser implementadas en ordenadores programables, cada ordenador incluyendo al menos un procesador, un sistema de almacenamiento de datos (que incluye memoria volátil o memoria no volátil u otros elementos de almacenamiento de datos o una combinación de los mismos), y al menos una interfaz de comunicación.

30 El código del programa puede aplicarse a los datos de entrada para realizar las funciones descritas aquí y generar información de salida. La información de salida se aplica a uno o más dispositivos de salida. En algunas modalidades, la interfaz de comunicación puede ser una interfaz de comunicación de red. En modalidades en las que los elementos pueden combinarse, la interfaz de comunicación puede ser una interfaz de comunicación de software, como las utilizadas para la comunicación entre procesos. En otras modalidades, puede haber una combinación de interfaces de comunicación implementadas como hardware, software y combinación de ambos.

40 A lo largo de la siguiente discusión anterior, se harán numerosas referencias a servidores, servicios, interfaces, portales, plataformas u otros sistemas formados por dispositivos informáticos. Debe apreciarse que el uso de dichos términos se considera representar uno o más dispositivos informáticos que tienen al menos un procesador configurado para ejecutar instrucciones de software almacenadas en un medio tangible y no transitorio legible por ordenador. Por ejemplo, un servidor puede incluir uno o más ordenadores que funcionen como servidor web, servidor de base de datos u otro tipo de servidor informático de manera que cumpla con los roles, responsabilidades o funciones descritas.

Se debe apreciar que los sistemas y métodos descritos en este documento pueden permitir un cálculo más eficiente, una menor probabilidad de compromiso, etc.

50 La siguiente discusión proporciona muchos ejemplos de modalidades. Aunque cada modalidad representa una única combinación de elementos inventivos, otros ejemplos pueden incluir todas las posibles combinaciones de los elementos descritos. Así, si una modalidad comprende los elementos A, B y C, y una segunda modalidad comprende los elementos B y D, también se pueden utilizar otras combinaciones restantes de A, B, C o D.

55 El término "conectado" o "acoplado a" puede incluir tanto el acoplamiento directo (en el que dos elementos acoplados entre sí se contactan) como el acoplamiento indirecto (en el que al menos un elemento adicional se encuentra entre los dos elementos).

60 La solución técnica de las modalidades puede adoptar la forma de un producto de software. El producto de software puede ser almacenado en un medio de almacenamiento no volátil o no transitorio, que puede ser un disco compacto de memoria de solo lectura (CD-ROM), una memoria flash USB o un disco duro extraíble. El producto de software incluye una serie de instrucciones que permiten que un dispositivo informático (ordenador personal, servidor o dispositivo de red) ejecute los métodos proporcionados por las modalidades.

65 Las modalidades descritas en este documento se implementan mediante hardware informático físico, que incluye dispositivos de computación, servidores, receptores, transmisores, procesadores, memoria, pantallas y redes. Las

modalidades descritas en este documento proporcionan máquinas físicas útiles y arreglos de hardware informático especialmente configurados. Las modalidades descritas en este documento se refieren a máquinas electrónicas y métodos implementados por máquinas electrónicas adaptadas para procesar y transformar señales electromagnéticas que representan diversos tipos de información. Las modalidades descritas en este documento se relacionan de manera

5 pervasiva e integral con máquinas y sus usos; y las modalidades descritas en este documento no tienen ningún significado o aplicabilidad práctica fuera de su uso con hardware de ordenador, máquinas y varios componentes de hardware. Sustituir el hardware físico especialmente configurado para llevar a cabo diversas acciones por hardware no físico, utilizando pasos mentales, por ejemplo, puede afectar sustancialmente la forma en que funcionan las

10 modalidades. Tales limitaciones de hardware informático son elementos esenciales de las modalidades descritas en este documento, y no pueden ser omitidas o sustituidas por medios mentales sin tener un efecto material en el funcionamiento y estructura de las modalidades descritas en este documento. El hardware de la ordenador es esencial para implementar las diversas modalidades descritas aquí y no se utiliza únicamente para realizar pasos de manera expedita y eficiente.

15 Los sistemas informáticos supervisores 106 puede ser implementado utilizando varios dispositivos informáticos. Los sistemas informáticos supervisores 106 puede incluir al menos un procesador, un dispositivo de almacenamiento de datos 110 (que incluye memoria volátil o memoria no volátil u otros elementos de almacenamiento de datos o una combinación de los mismos) y al menos una interfaz de comunicación. Los componentes del dispositivo informático pueden estar conectados de diversas formas, incluyendo conexión directa, conexión indirecta a través de una red y

20 distribución en una amplia área geográfica y conexión a través de una red (que puede denominarse "computación en la nube").

Por ejemplo, y sin limitación, los sistemas informáticos supervisores puede ser un servidor, un dispositivo de red, una

25 ordenador personal, una ordenador portátil, un asistente personal de datos, un teléfono celular, un dispositivo de teléfono inteligente, una terminal de visualización de video, una consola de juegos, un dispositivo de lectura electrónica y un dispositivo de hipermedia inalámbrico o cualquier otro dispositivo informático capaz de ser configurado para llevar a cabo los métodos descritos aquí.

La Figura 11 es un diagrama esquemático 1100 de un ejemplo de sistemas/dispositivos informáticos de supervisor, instructor, intermediario y/o destino 106, ejemplar de una modalidad. Como se muestra, los sistemas informáticos

30 supervisores 106 incluyen al menos un procesador 1102, memoria 1104, al menos una interfaz de E/S 1106 y al menos una interfaz de red 1108.

Cada procesador 1102 puede ser, por ejemplo, cualquier tipo de microprocesador o microcontrolador de propósito general, un procesador de procesamiento de señales digitales (DSP), un circuito integrado, una matriz de compuertas programable en campo (FPGA), un procesador reconfigurable, una memoria de solo lectura programable (PROM) o cualquier combinación de los mismos.

35

La memoria 1104 puede incluir una combinación adecuada de cualquier tipo de memoria de ordenador que se encuentre ubicada interna o externamente, como por ejemplo, memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), memoria de solo lectura de disco compacto (CDROM), memoria electroóptica, memoria magnetoóptica, memoria programable de solo lectura borrrable (EPROM) y memoria programable de solo lectura borrrable eléctricamente (EEPROM), memoria RAM ferroeléctrica (FRAM) o similar.

40

Cada interfaz de I/O 1106 permite a los sistemas informáticos supervisores de dispositivos informáticos 106 interconectarse con uno o más dispositivos de entrada, como un teclado, un ratón, una cámara, una pantalla táctil y un micrófono, o con uno o más dispositivos de salida, como una pantalla y un altavoz.

45

Cada interfaz de red 1108 permite a los sistemas informáticos supervisores del dispositivo de computación 106 comunicarse con otros componentes, intercambiar datos con otros componentes, acceder y conectarse a recursos de red, servir aplicaciones y realizar otras aplicaciones informáticas mediante la conexión a una red (o múltiples redes) capaz de transportar datos, incluyendo Internet, Ethernet, línea de servicio telefónico básico (POTS), red telefónica conmutada pública (PSTN), red digital de servicios integrados (ISDN), línea de abonado digital (DSL), cable coaxial, fibra óptica, satélite, móvil, inalámbrica (por ejemplo, Wi-Fi, WiMAX), red de señalización SS12, línea fija, red de área

50 local, red de área amplia y otras, incluyendo cualquier combinación de estas.

55

REIVINDICACIONES

1. Un método de monitoreo de procesos de datos electrónicos para gestionar procesos de datos secundarios que representan una o más solicitudes secundarias de transacciones en intereses financieros generados a partir de al menos un proceso de datos principal enrutado electrónicamente a al menos un dispositivo de destino, el método comprende:

recibir al menos una solicitud secundaria de las una o más solicitudes secundarias que se enrutan desde un dispositivo intermediario hacia al menos un dispositivo de destino correspondiente, la al menos una solicitud secundaria que solicita la ejecución de al menos un proceso de datos secundario correspondiente de los procesos de datos secundarios, cada uno de los al menos un proceso de datos secundario para ejecutar al menos una parte del al menos un proceso de datos principal desde un dispositivo instructor, y cada una de las al menos una solicitud secundaria codificada que utiliza una clave de codificación de destino que se deriva utilizando codificación en cascada al menos en parte a partir de al menos una clave de codificación del instructor; almacenar la al menos una solicitud secundaria en al menos un dispositivo de almacenamiento de datos; generar señales para comunicar una o más solicitudes secundarias al dispositivo instructor o a un dispositivo solicitante asociado a un regulador; y utilizar, mediante el dispositivo instructor o un dispositivo solicitante asociado al regulador, un dispositivo de acceso que tiene al menos una de la clave de codificación de destino o al menos una clave de codificación del instructor, para acceder a la al menos una solicitud secundaria registrada en el al menos un almacenamiento de datos para identificar una o más características de ejecución de enrutamiento de la al menos una solicitud secundaria y verificar automáticamente las una o más características de ejecución de enrutamiento de la al menos una solicitud secundaria.

2. El método de la reivindicación 1, el método que comprende codificar cada una de al menos una solicitud secundaria con su correspondiente clave de codificación de destino antes de generar las señales para comunicar las solicitudes secundarias.

3. El método de la reivindicación 2, en donde un dispositivo solicitante particular que tiene al menos una clave de codificación de destino particular puede decodificar la solicitud secundaria codificada correspondiente para identificar al menos un proceso de datos secundario enrutado para ejecutar al menos un proceso de datos principal particular asociado con la clave de codificación de destino particular.

4. El método de cualquier reivindicación anterior, el método que comprende la transmisión de al menos una solicitud secundaria a al menos un dispositivo de destino correspondiente, y opcionalmente: el método que comprende eliminar la clave de codificación de destino de al menos una solicitud secundaria antes de transmitir la al menos una solicitud secundaria a al menos un dispositivo de destino correspondiente.

5. El método de cualquier reivindicación anterior, el método que comprende: recibir al menos un mensaje de respuesta asociado con al menos una solicitud secundaria; y generar señales para comunicar datos desde al menos un mensaje de respuesta con las solicitudes secundarias correspondientes.

6. El método de cualquier reivindicación anterior, en donde la al menos una solicitud secundaria es recibida de uno o más dispositivos de escucha en una o más rutas entre el dispositivo intermediario y el al menos un dispositivo de destino correspondiente.

7. El método de cualquier reivindicación anterior, el método que comprende recibir al menos una clave de indexado asociada con al menos una solicitud secundaria; y almacenar la al menos una solicitud secundaria en asociación con la al menos una clave de indexado.

8. El método de cualquier reivindicación anterior, el método que comprende almacenar al menos una solicitud secundaria asociada con un identificador que identifica un mecanismo mediante el cual se recibió al menos una solicitud secundaria.

9. El método de cualquier reivindicación anterior, el método que comprende recibir del dispositivo instructor o del dispositivo solicitante asociado al regulador al menos uno de: la clave de codificación del instructor, la clave de codificación intermediaria, la clave de codificación de destino y una clave de indexado; y generar señales para comunicar solicitudes secundarias asociadas a al menos uno de: la clave de codificación del instructor, la clave de codificación intermediaria, la clave de codificación de destino y la clave de indexado al dispositivo solicitante.

10. El método de cualquier reivindicación anterior, en donde cuando al menos uno de los al menos un dispositivo de destino es otro dispositivo intermediario, el método comprende: recibir al menos una clave intermediaria del dispositivo intermediario adicional, y almacenar la al menos una clave intermediaria asociada a la al menos una solicitud secundaria asociada.

11. El método de cualquier reivindicación anterior, el método que comprende:

recibir al menos una segunda solicitud principal que se enruta desde el dispositivo instructor hacia al menos un dispositivo de destino, cada una de las al menos una segunda solicitud principal para ejecutar al menos un segundo proceso de datos principal;
 almacenar la al menos una segunda solicitud principal en el al menos un dispositivo de almacenamiento; y

- 5 generar señales para comunicar la segunda solicitud principal al uno o más dispositivos solicitantes.
-
12. El método de cualquier reivindicación anterior, en donde almacenar la al menos una solicitud secundaria incluye almacenar metadatos de la solicitud secundaria en asociación con la al menos una solicitud secundaria; en donde
10 los metadatos de la solicitud secundaria incluyen al menos uno de: información de marca de tiempo y un identificador que identifica un método mediante el cual se obtuvo la solicitud secundaria del enrutamiento.
 13. El método de cualquier reivindicación anterior, en donde el al menos un proceso de datos principal representa al
15 menos una solicitud de una transacción en un interés financiero.
 14. Un sistema para gestionar procesos de datos en una red de recursos informáticos, el sistema comprende al menos un procesador configurado para ejecutar instrucciones interpretables por máquina que hacen que el sistema lleve a cabo el método de cualquiera de las reivindicaciones 1 a 13.
 - 20 15. Un medio no transitorio legible por ordenador para gestionar procesos de datos en una red de recursos informáticos, el medio no transitorio legible por ordenador que comprende instrucciones interpretables por máquina que, cuando se ejecutan, hacen que al menos un procesador lleve a cabo el método de cualquiera de las reivindicaciones 1 a 13.

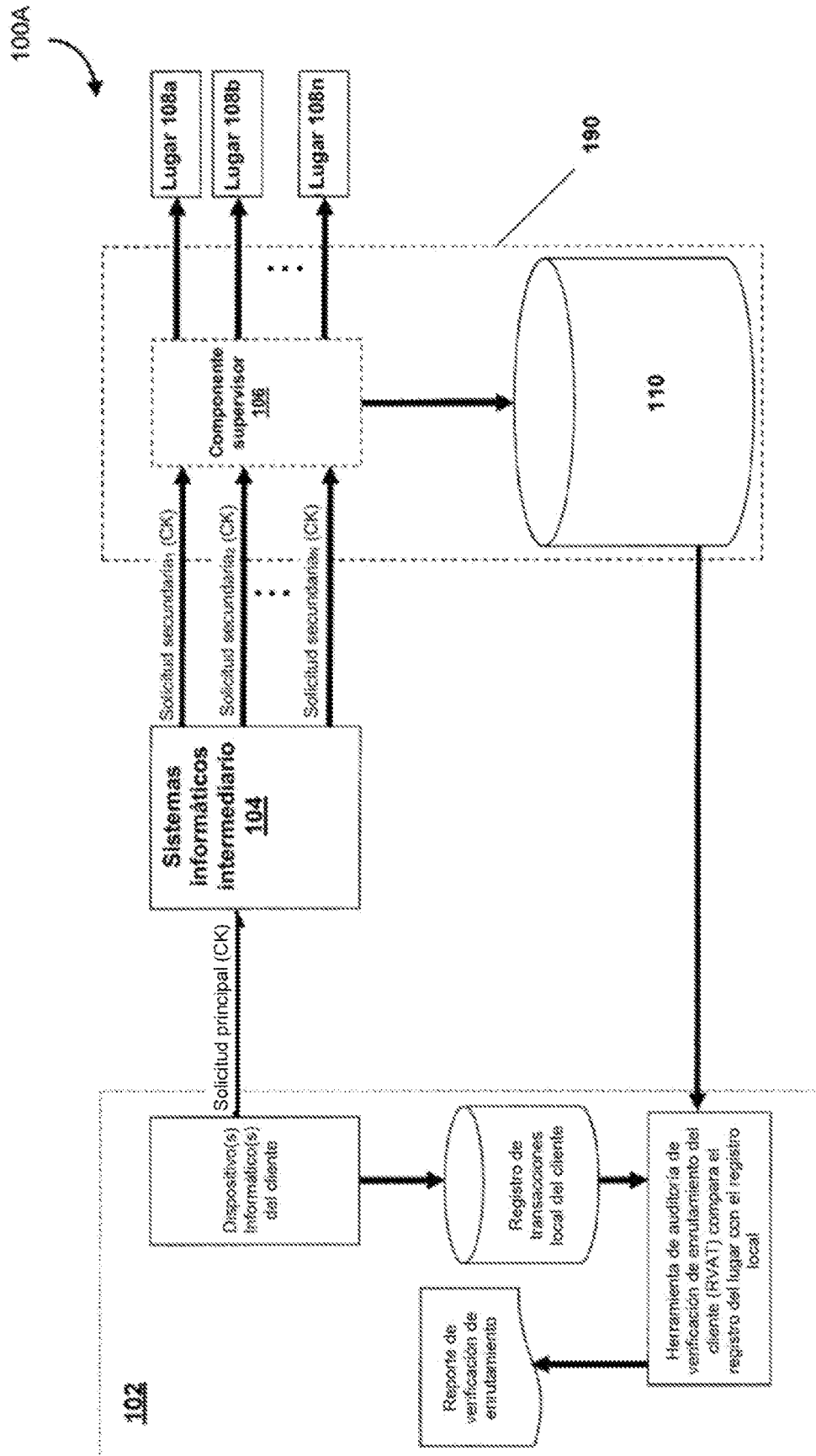


FIGURA 1A

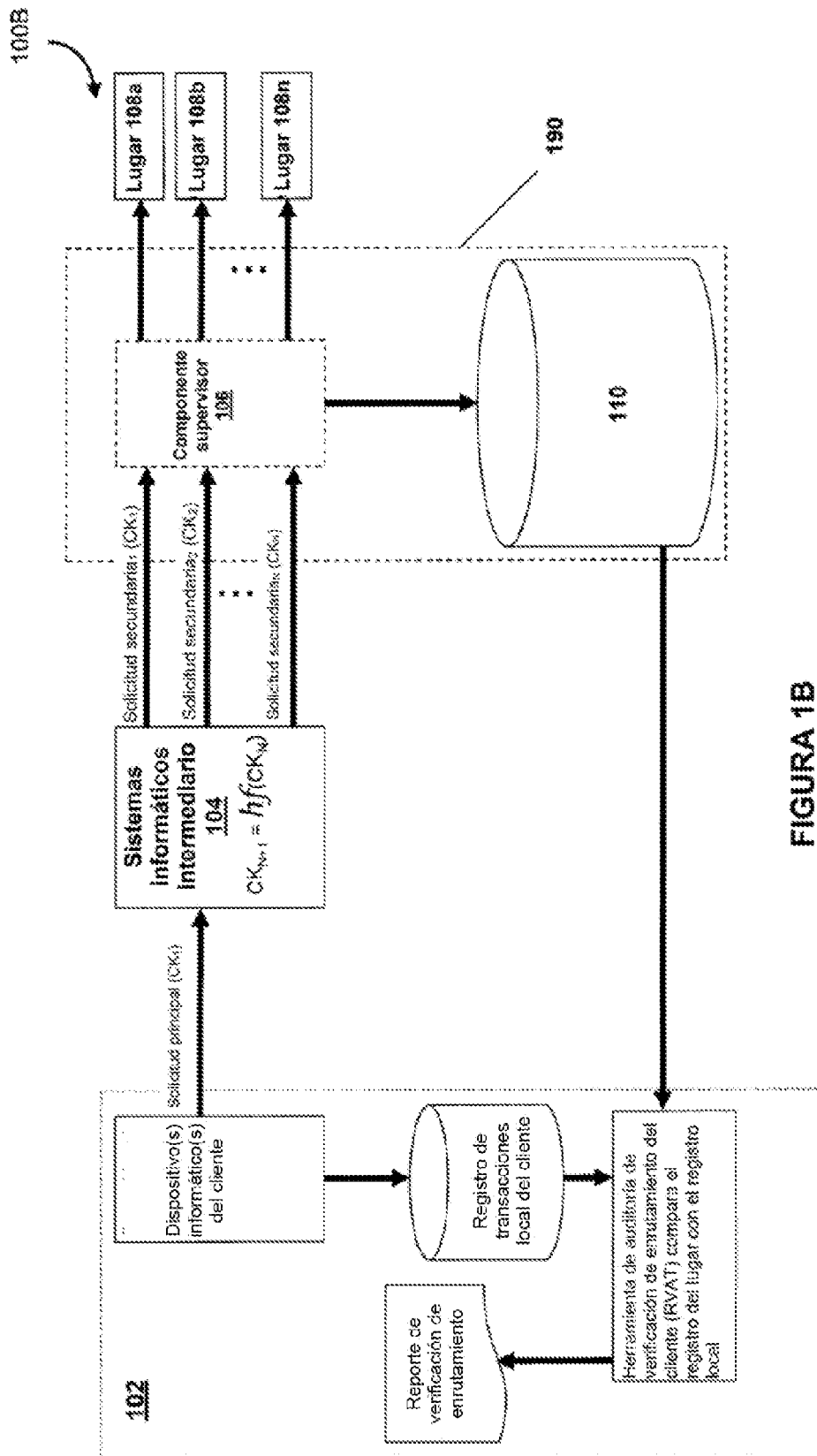
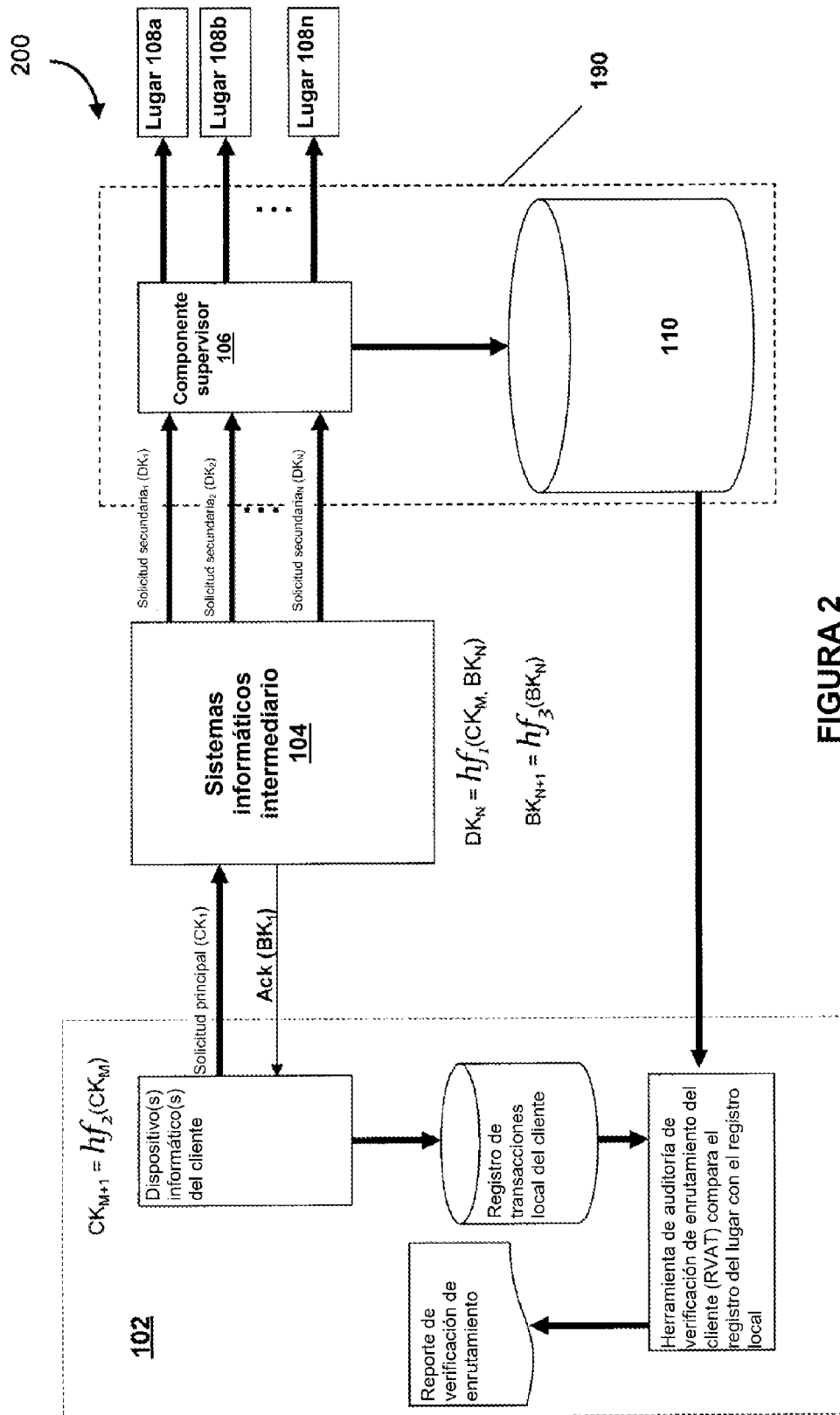


FIGURA 1B



300

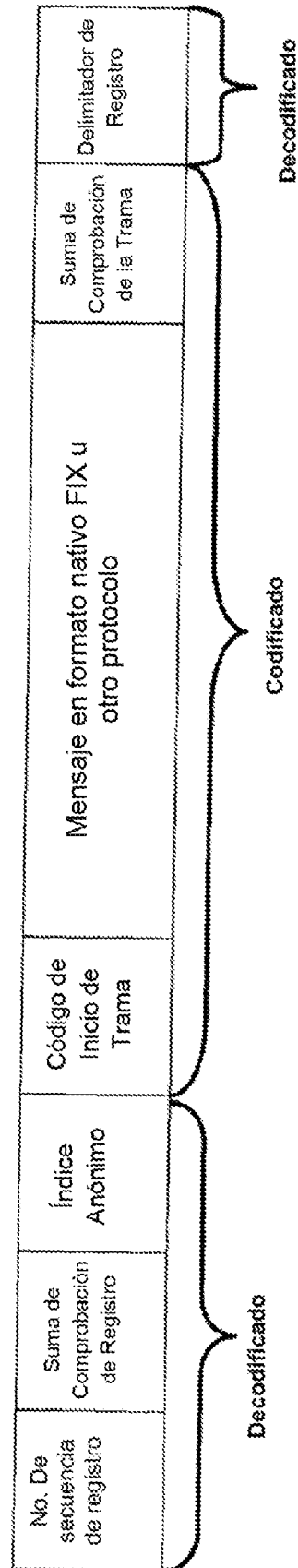


FIGURA 3

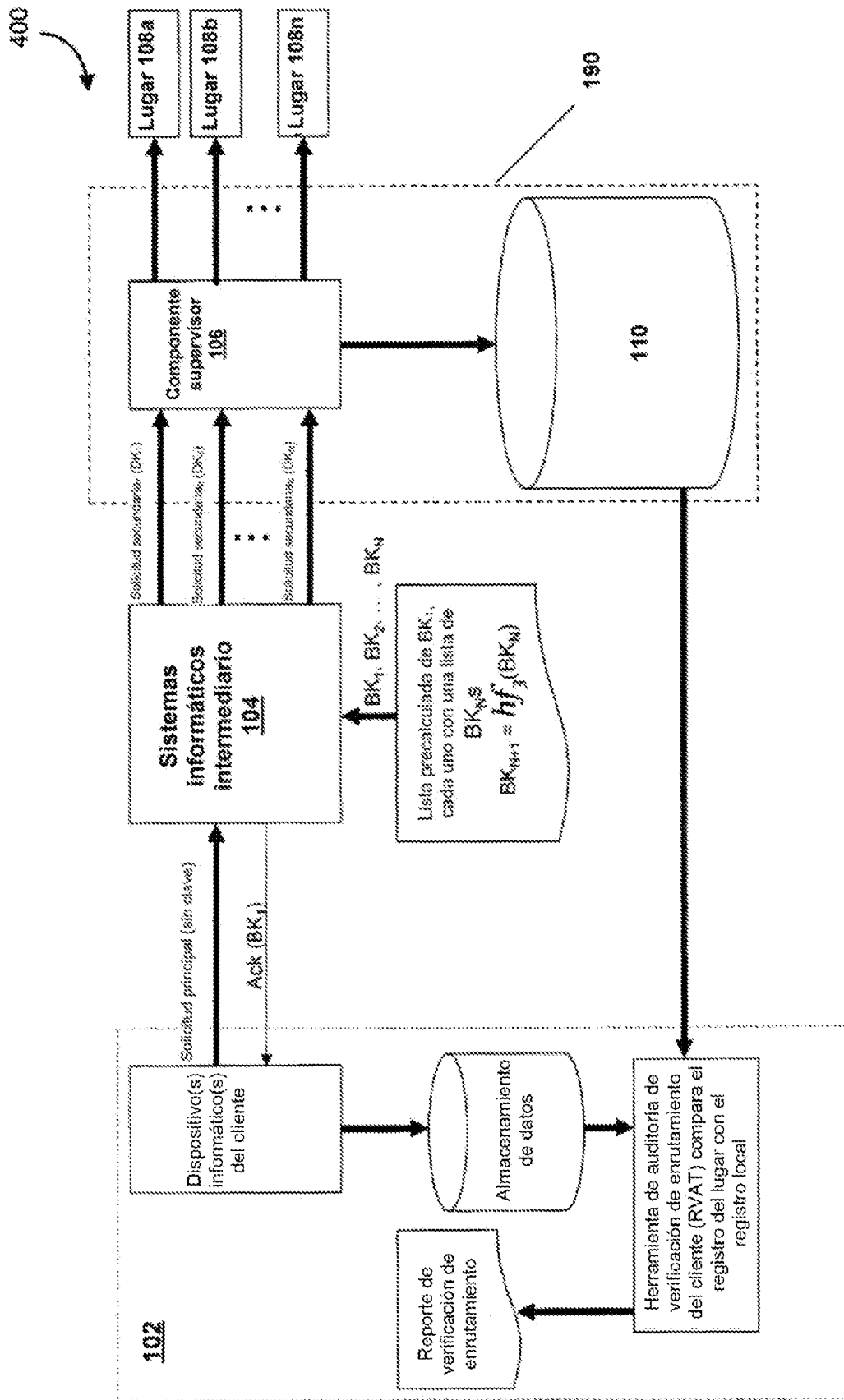


FIGURA 4

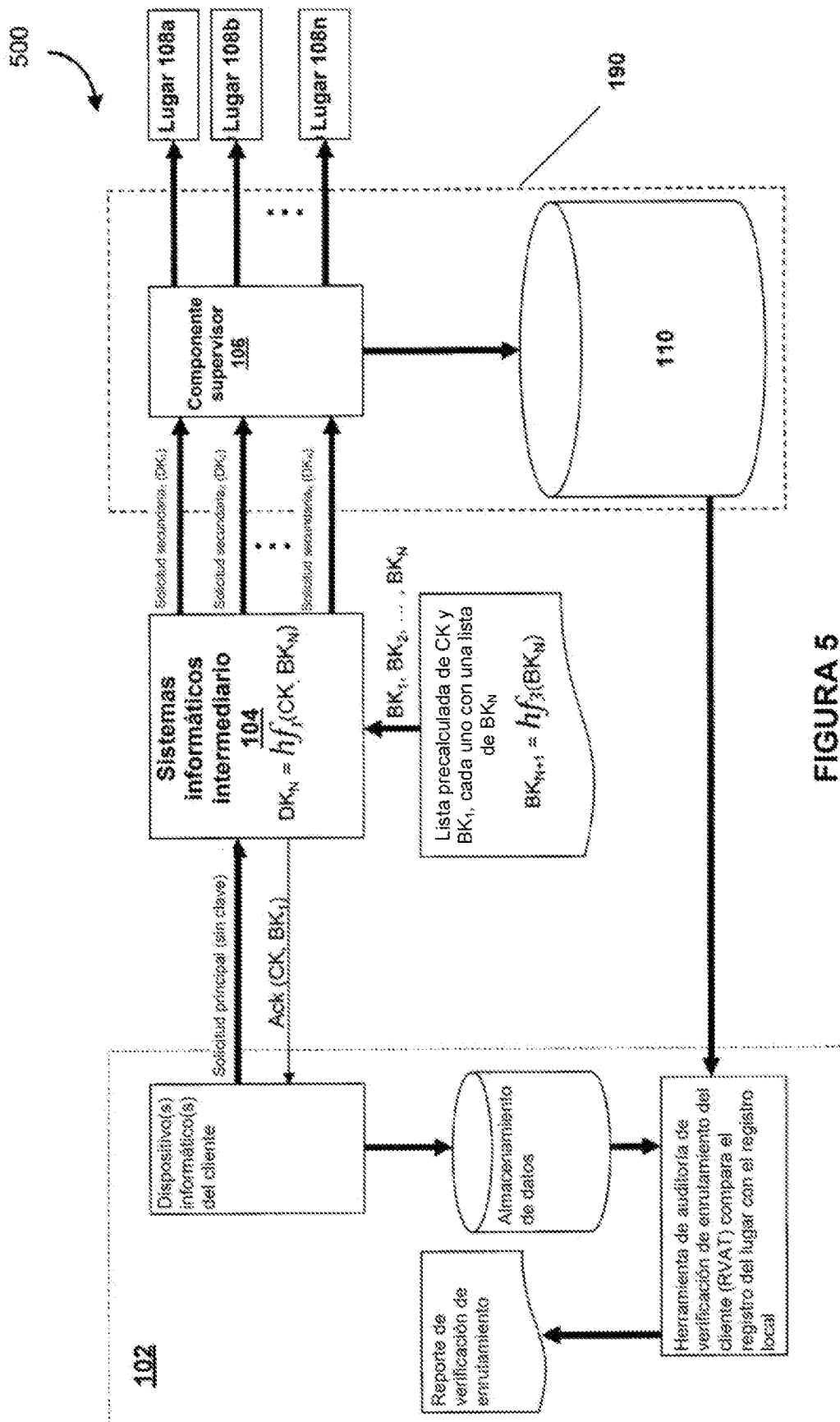


FIGURA 5

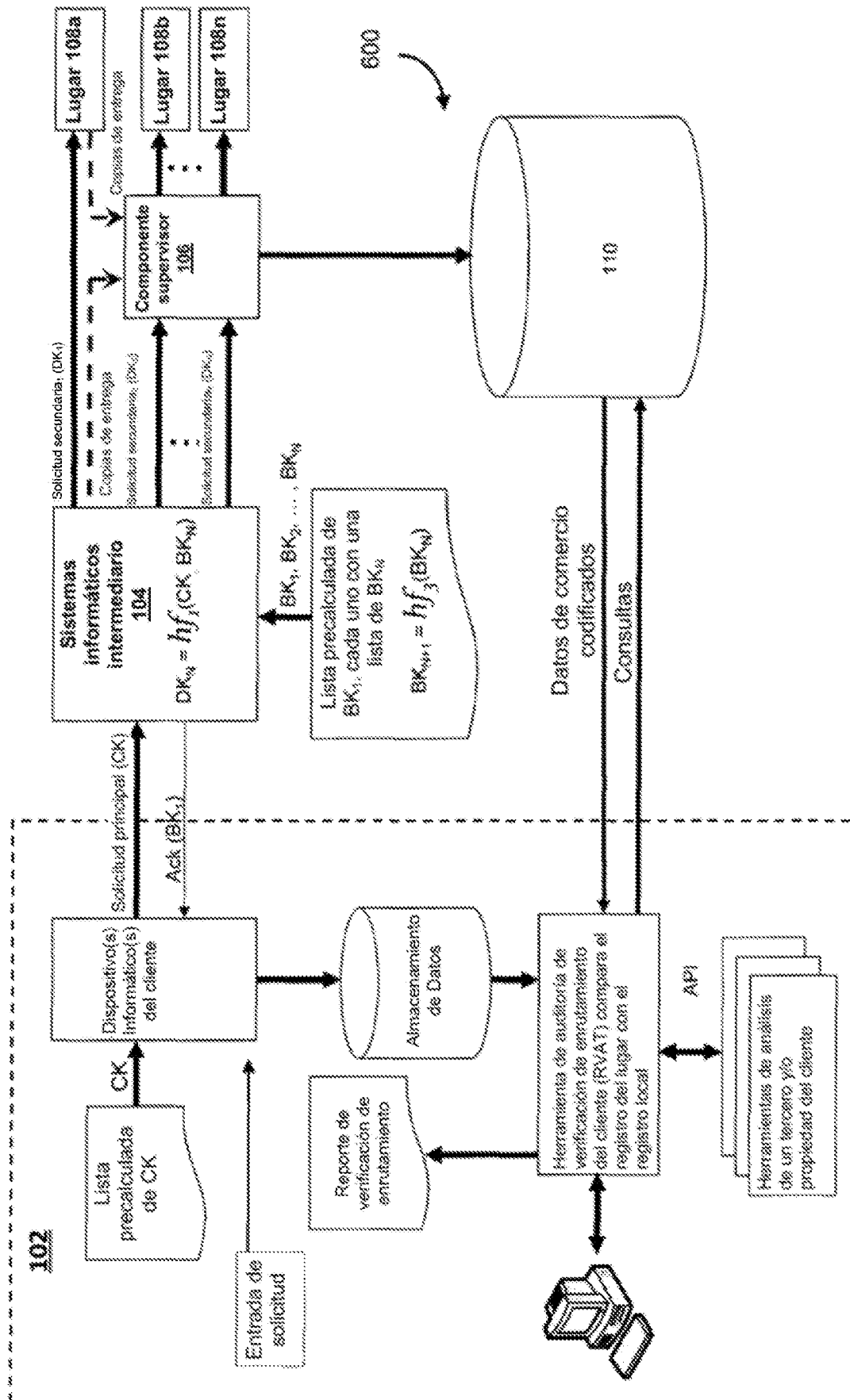


FIGURA 6

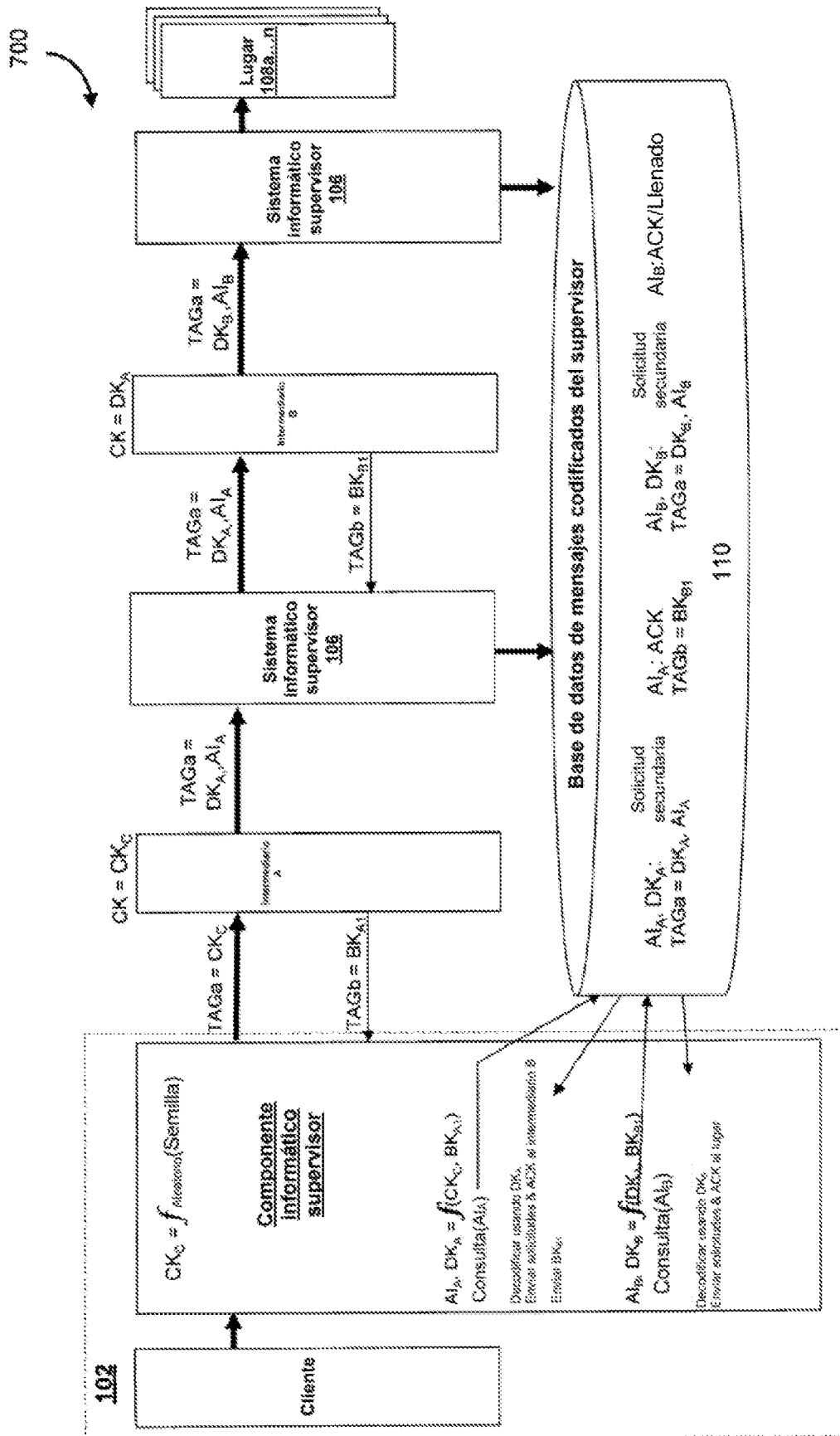


FIGURA 7

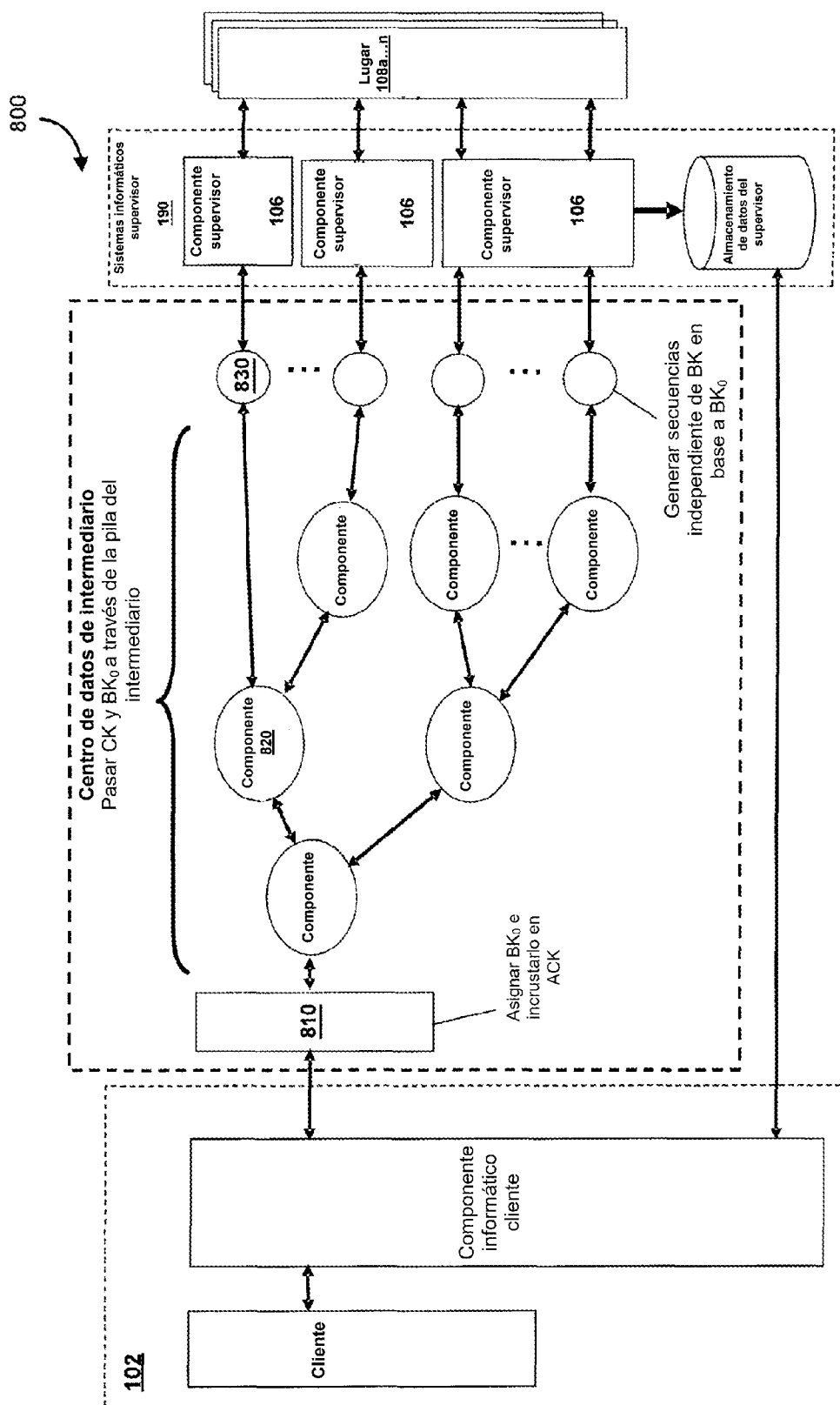


FIGURA 8

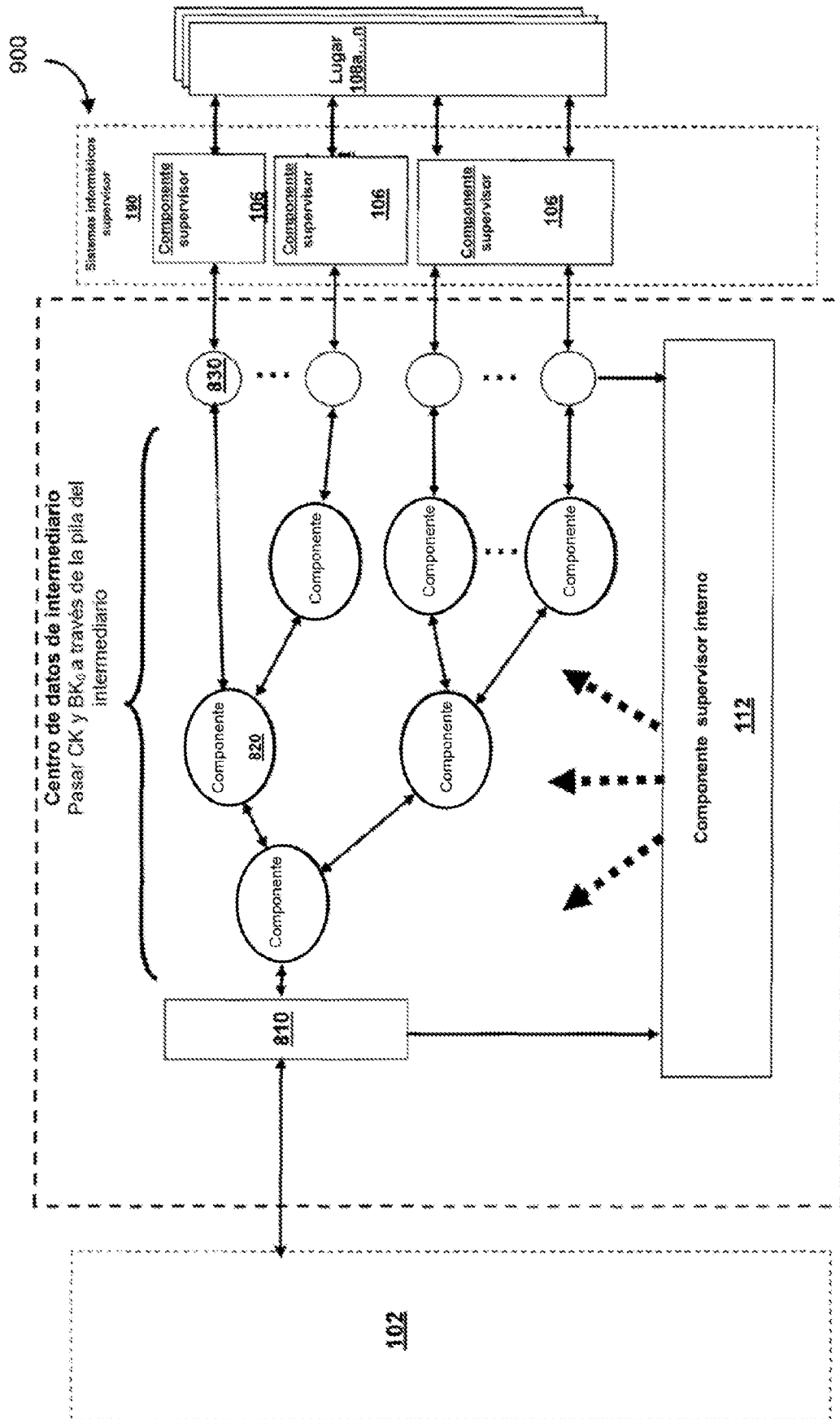


FIGURA 9

1000



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Entidad 1 ==>	1	8	15	22	29	36	43	50	57	64	71	78	85	92	99	106	113	120	127	134	141	148	155	162	169	176	183	190
Entidad 2 ==>	2	9	16	23	30	37	44	51	58	65	72	79	86	93	100	107	114	121	128	135	142	149	156	163	170	177	184	191
Entidad 3 ==>	3	10	17	24	31	38	45	52	59	66	73	80	87	94	101	108	115	122	129	136	143	150	157	164	171	178	185	192
Entidad 4 ==>	4	11	18	25	32	39	46	53	60	67	74	81	88	95	102	109	116	123	130	137	144	151	158	165	172	179	186	193
Entidad 5 ==>	5	12	19	26	33	40	47	54	61	68	75	82	89	96	103	110	117	124	131	138	145	152	159	166	173	180	187	194
Entidad 6 ==>	6	13	20	27	34	41	48	55	62	69	76	83	90	97	104	111	118	125	132	139	146	153	160	167	174	181	188	195
Entidad 7 ==>	7	14	21	28	35	42	49	56	63	70	77	84	91	98	105	112	119	126	133	140	147	154	161	168	175	182	189	196

FIGURA 10

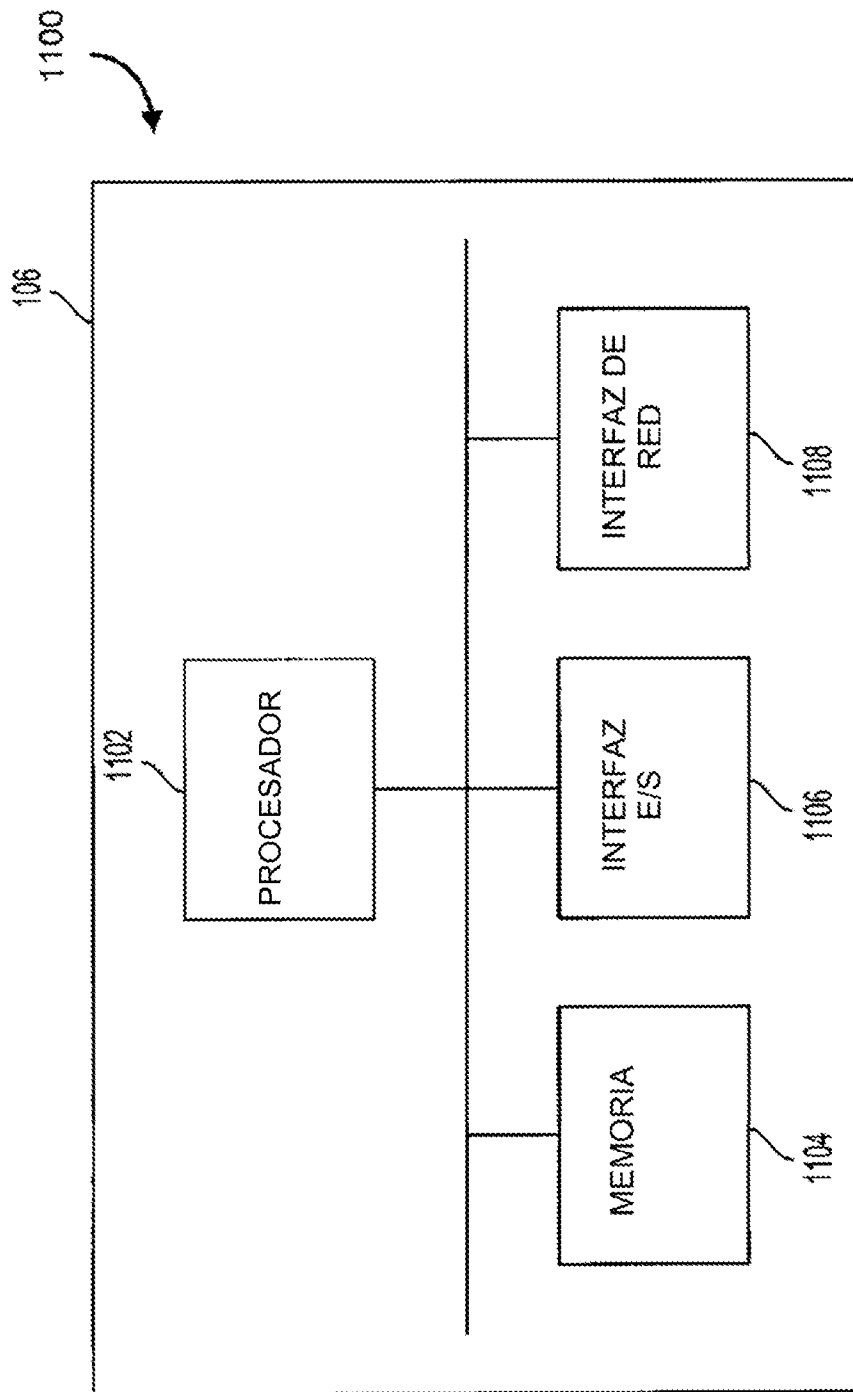


FIGURA 11

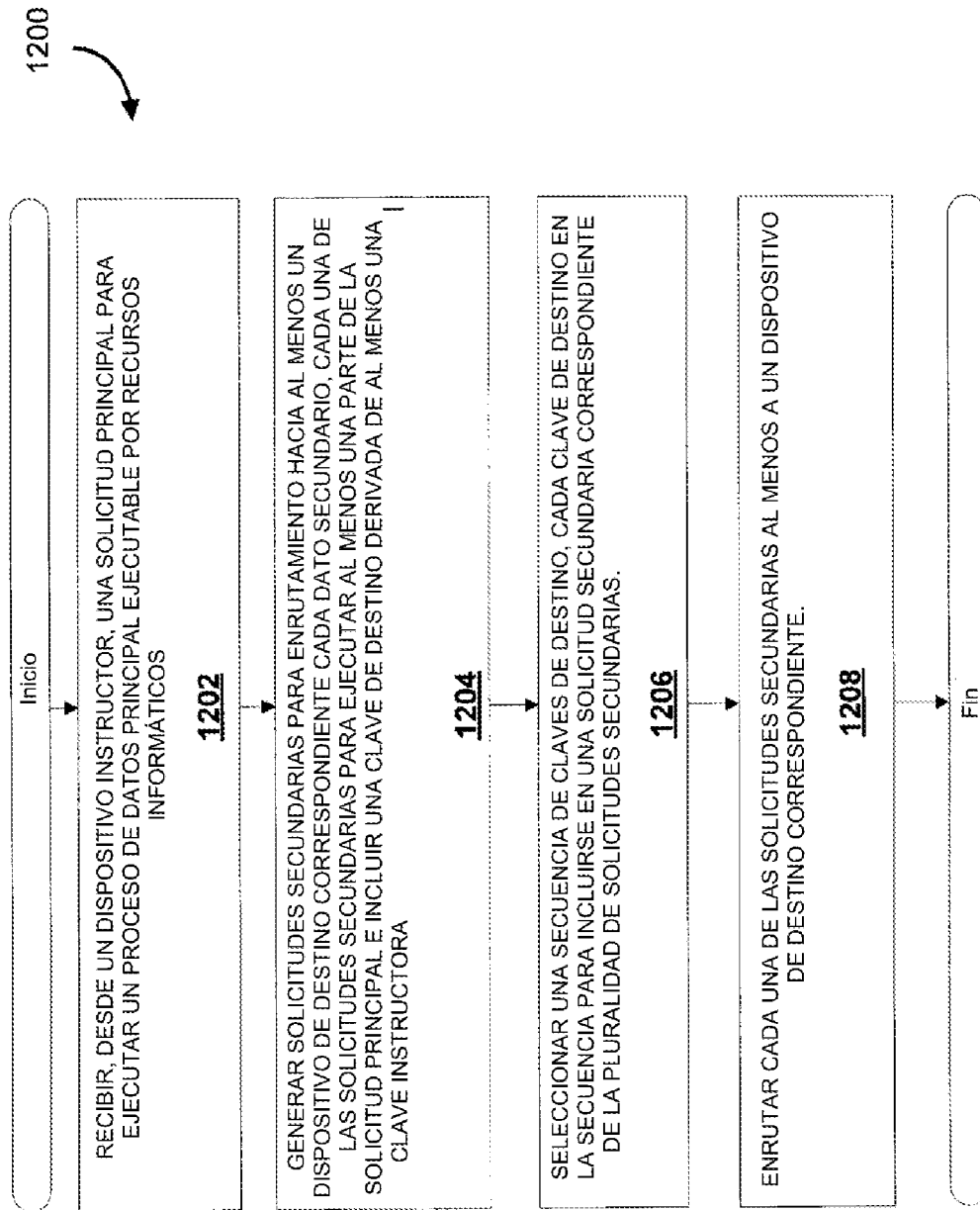


FIGURA 12

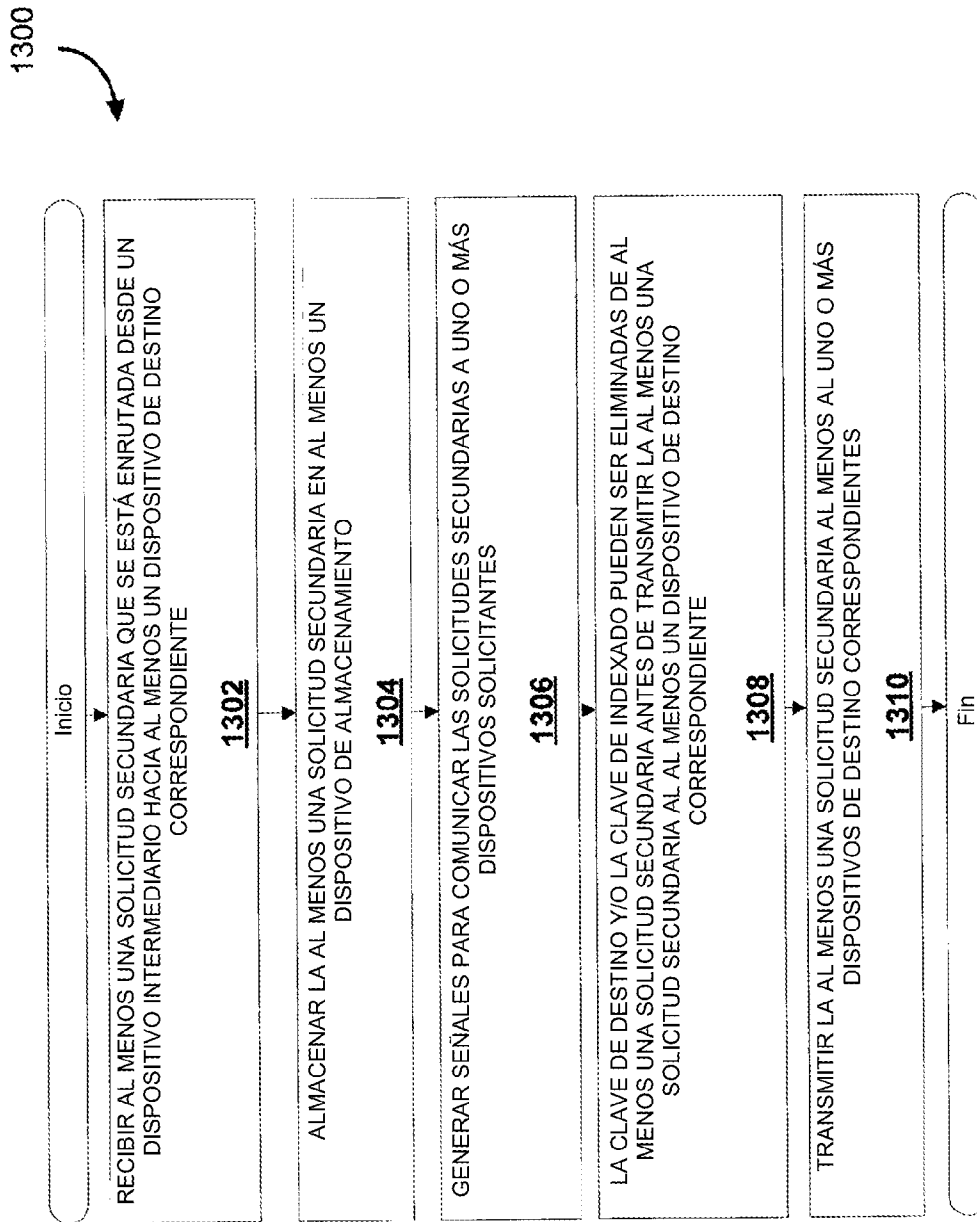


FIGURA 13

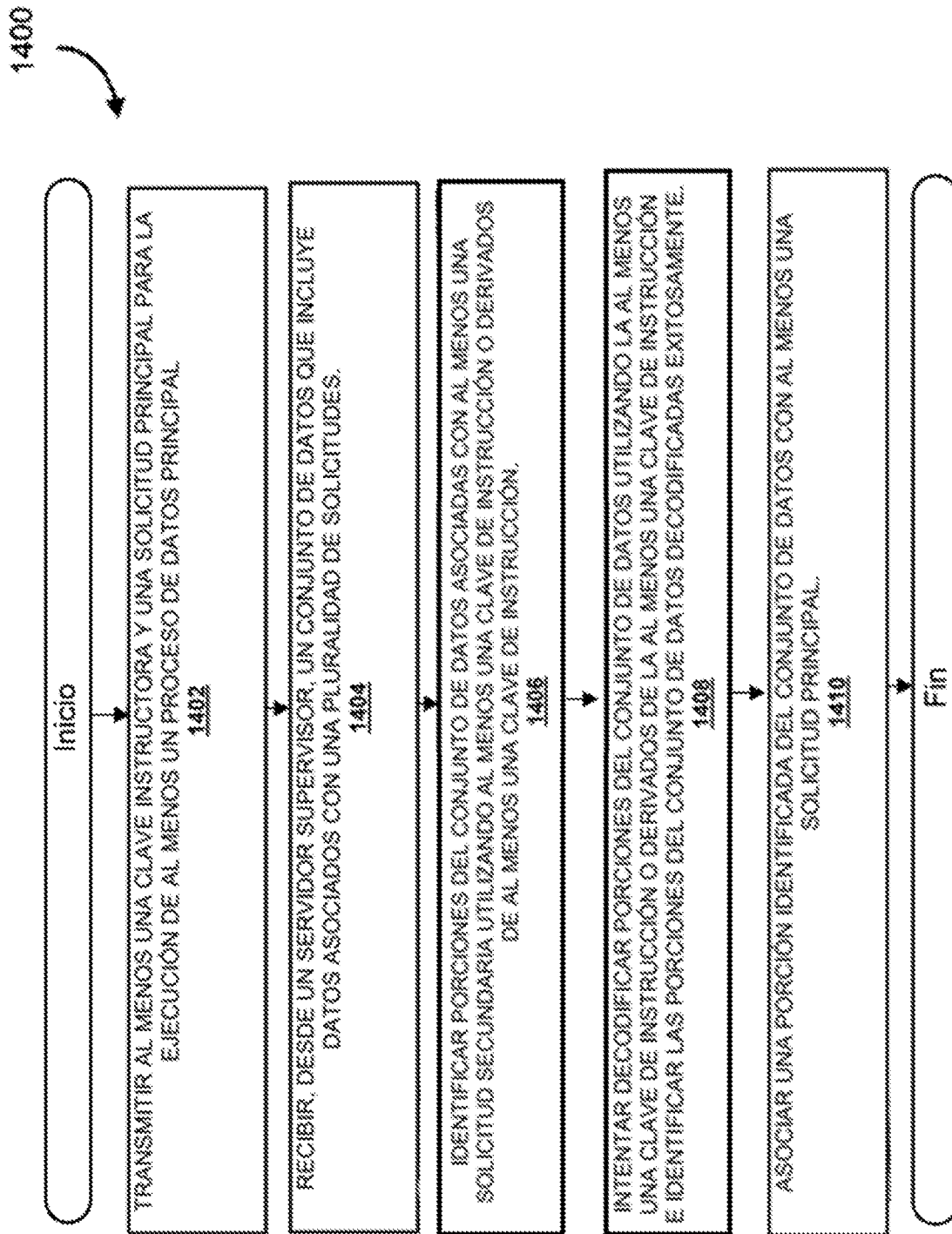


FIGURA 14