

**DE PATENTE DE UTILIDAD
DE LOS ESTADOS UNIDOS**

PARA

**ALERTAS CON BASE EN REGLAS SENSIBLES AL CONTEXTO
PARA la supervisión DEL FRAUDE**

Inventores:

Lyle Hardy

Preparado por:

MURABITO, HAO & BARNES, LLP

Two North Market Street

Third floor

San José, California 95113

(408) 938-9060

ALERTAS CON BASE EN REGLAS SENSIBLES AL CONTEXTO

PARA LA SUPERVISIÓN DEL FRAUDE

ANTECEDENTES

[0001] Muchas empresas y organizaciones ofrecen servicios a consumidores y otros clientes a distancia. Mientras que una parte cada vez mayor de estos servicios se automatiza, a menudo se prefiere la interacción humana (y a veces es necesaria) para casos más difíciles o complejos. Naturalmente, muchas empresas y organizaciones emplean representantes humanos para proporcionar soporte (técnico) y/o información a consumidores interesados y otras partes interesadas con respecto a productos y/o servicios. Para manejar grandes volúmenes de solicitudes, un enfoque típico es usar uno o más centros de contacto atendidos por agentes humanos. Muchos centros de contacto individualizados están centralizados para proporcionar suficiente espacio y recursos para muchos agentes que trabajan simultáneamente. Por ejemplo, un centro de contacto más grande puede admitir cientos o miles de estaciones de trabajo en un solo edificio o campus de edificios. De esa manera, el mantenimiento y la instalación de toda la infraestructura (e.g., computadores, cubículos de estaciones de trabajo, etc.), están centralizados.

[0002] Estos centros de contacto típicamente manejan los grandes volúmenes de solicitudes de servicio o cumplimiento por teléfono (o tecnologías de comunicación que simulan una comunicación telefónica). Normalmente, los agentes responderán a las llamadas en el orden en que se reciben, y cuando se supere el número de agentes disponibles por el número de llamadas pendientes, se formará una cola cronológica a la que los agentes pueden responder cuando estén disponibles (e.g., se completa una llamada anterior).

[0003] Un ejemplo popular de un centro de contacto es un centro de contacto entrante que gestiona las llamadas entrantes para proporcionar servicios a los llamantes entrantes. Por ejemplo, un centro de contacto entrante puede proporcionar soporte para completar una venta, manejar problemas o preguntas sobre productos (e.g., instrucciones de instalación, servicio de garantía, etc.), manejar llamadas relacionadas con servicios (e.g., banca, cobranzas, policía, bomberos, alarma, etc.) y otros tipos similares de servicios. Otro ejemplo de un centro de contacto es un centro de contacto saliente que inicia las llamadas. Un centro de contacto saliente puede proporcionar telemarketing para un producto o servicio, permitir la solicitud de donaciones caritativas o políticas, proporcionar servicios de cobro de deudas, realizar encuestas o estudios de mercado, etc.

[0004] Un centro de contacto puede ser operado por la empresa u organización asociada con el producto o servicio, o un tercero empleado para proporcionar soporte al cliente. El centro de contacto puede representar a un cliente externo, donde el agente maneja las llamadas de los clientes en nombre del cliente externo. Como tal, el agente puede estar autorizado para acceder a información privilegiada del cliente utilizando las bases de datos del cliente. Por ejemplo, el cliente puede ser una institución bancaria y el agente está atendiendo una llamada para ayudar a un cliente a determinar el saldo de su cuenta. En tales casos, el agente puede acceder a los datos personales del cliente controlados por la institución bancaria para proporcionar un saldo en la cuenta.

[0005] Sin embargo, hay casos en los que el agente tiene acceso a información privilegiada del cliente cuando no existe una necesidad legítima, o está accediendo a la información con fines nefastos. Es decir, mientras que un agente del centro de contacto tiene de forma inherente el acceso autorizado a información personal e identificable, el agente generalmente solo tiene la facultad

de utilizar este acceso cuando lo necesite. Sin embargo, sin supervisión activa y control de acceso del usuario, el agente no solo puede recopilar información personal crítica a través del acceso no autorizado, sino que esa información se puede usar posteriormente para cometer fraude adicional (e.g., solicitar crédito, hacer transacciones de compra, etc.).

RESUMEN

[0006] Este Resumen se proporciona para introducir una selección de conceptos en una forma simplificada que se describe adicionalmente a continuación en la Descripción Detallada. Este Resumen no pretende identificar las características clave o las características esenciales de la materia objeto reivindicada, ni tiene la intención de ser utilizado para limitar el alcance de la materia objeto reivindicada.

[0007] De acuerdo con las implementaciones de la presente invención, se proporcionan diversos métodos implementados por computador para generar alertas sensibles al contexto con el fin de detectar y prevenir el fraude. De acuerdo con una implementación, una sesión de comunicación (e.g., una llamada) se inicia en (o se recibe por) una estación de trabajo por un representante o agente humano. La comunicación verbal entre el agente y el cliente externo se supervisa y se convierte en texto mediante técnicas de reconocimiento automático de voz (ASR). También se realiza un seguimiento de la actividad del agente en las aplicaciones que se ejecutan en la estación de trabajo. La combinación de texto convertido y la actividad del agente se evalúan en un motor de comportamiento para detectar inconsistencias entre la actividad del agente y la actividad autorizada o típica. Cuando se detectan inconsistencias, se llevan a cabo acciones de seguridad para alertar a los administradores sobre posibles fraudes y, en casos

extremos, se pueden evitar nuevas acciones del agente en la estación de trabajo para evitar fraudes adicionales. En implementaciones adicionales, cuando se detecta la posible actividad fraudulenta, el método incluye recoger evidencia electrónica de la primera estación de trabajo, en la que la evidencia se puede usar para demostrar el fraude real por parte del agente.

[0008] De acuerdo con otra implementación, se proporciona un método para analizar la actividad de llamadas para detectar un posible comportamiento fraudulento. En una o más implementaciones, el método se realiza analizando una transcripción de comunicación verbal entre un agente y un tercer cliente y un registro de la actividad del agente en un motor de comportamiento, detectando actividad fraudulenta potencial a partir de los datos analizados, identificando medidas preventivas acordes a la posible actividad fraudulenta detectada y transmitiendo medidas preventivas a una estación de trabajo remota para que se realicen una vez que se detecte una posible actividad fraudulenta.

[0009] De acuerdo con otra implementación adicional, se proporciona un método implementado por computador para análisis de la actividad realizada por el agente en una estación de trabajo. En una o más implementaciones, el método se realiza detectando una sesión de llamada en una estación de trabajo correspondiente a un agente del centro de contacto, supervisando la actividad de llamada que incluye comunicación verbal entre el agente y el tercero correspondiente a la sesión de llamada, convirtiendo en texto la comunicación verbal supervisada, enviando el texto convertido y registrando la actividad del agente durante la sesión de llamada a un motor de comportamiento acoplado comunicativamente, que recibe una notificación de una inconsistencia detectada entre la comunicación verbal supervisada y el registro de actividad del agente y

una o más acciones de seguridad y realizar las acciones de seguridad en respuesta a la notificación recibida de la inconsistencia detectada.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0010] Los dibujos adjuntos, que se incorporan y forman parte de esta especificación y en los que los mismos números representan elementos similares, ilustran implementaciones de la presente divulgación y, junto con la descripción, sirven para explicar los principios de la divulgación.

[0011] La FIG. 1 representa un diagrama de bloques de un sistema de computador de ejemplo adecuado para realizar las implementaciones de acuerdo con la presente divulgación.

[0012] La FIG. 2 es una ilustración de un sistema configurado para identificar actividad fraudulenta potencial realizada por un agente dentro de un centro de contacto, y tomar una acción preventiva una vez que se identifica la actividad, de acuerdo con una implementación de la presente divulgación.

[0013] La FIG. 3 es un diagrama de bloques de los componentes de una estación de trabajo del centro de contacto que está configurada para supervisar la actividad de un agente del centro de contacto con el fin de identificar actividad fraudulenta potencial realizada por el agente, de acuerdo con una implementación de la presente divulgación.

[0014] La FIG. 4 es un diagrama de flujo que ilustra un método para supervisar la actividad de llamada para detectar actividad fraudulenta y tomar

medidas preventivas una vez que se detecta la actividad fraudulenta potencial, de acuerdo con una implementación de la presente divulgación.

[0015] La FIG. 5 es un diagrama de flujo que ilustra un método para supervisar la actividad de llamada en una estación de trabajo para detectar actividad fraudulenta y tomar medidas preventivas una vez que se detecta la posible actividad fraudulenta, de acuerdo con una implementación de la presente divulgación.

[0016] La FIG. 6 es un diagrama de flujo que ilustra un método para evaluar la actividad de llamada supervisada para determinar la probabilidad de actividad potencialmente fraudulenta, de acuerdo con una implementación de la presente divulgación.

DESCRIPCIÓN DETALLADA

[0017] Ahora se hará referencia en detalle a varias implementaciones. Además, en la siguiente descripción detallada, se exponen numerosos detalles específicos para proporcionar una comprensión exhaustiva de la materia reivindicada. Sin embargo, un experto versado en el arte reconocerá que las implementaciones se pueden practicar sin estos detalles específicos o con equivalentes de los mismos. En otros casos, los procesos, procedimientos, componentes y circuitos bien conocidos no se han descrito en detalle para no ocultar innecesariamente aspectos y características del tema en cuestión.

[0018] Algunas partes de la descripción detallada que sigue se presentan y discuten en términos de un proceso. Aunque las operaciones y la secuencia de las mismas se muestran en una figura que describe las operaciones de este

proceso, tales operaciones y secuenciación son de ejemplo. Las implementaciones están bien adecuadas para realizar otras diversas operaciones o variaciones de las operaciones enumeradas en el diagrama de flujo de la figura de la presente, y en una secuencia diferente a la representada y descrita en este documento.

[0019] Algunas partes de la descripción detallada se presentan en términos de procedimientos, operaciones, bloques lógicos, procesamiento y otras representaciones simbólicas de operaciones en bits de datos que se pueden realizar en la memoria del computador. Estas descripciones y representaciones son los medios utilizados por los versados en el arte de procesamiento de datos para transmitir de manera más efectiva la sustancia de su trabajo a otros expertos en la materia. Un procedimiento, una operación ejecutada por computador, un bloque lógico, un proceso, etc., están aquí, y en general, se concibe como una secuencia autocontenida de operaciones o instrucciones que conducen a un resultado deseado. Las operaciones son aquellas que requieren manipulaciones físicas de cantidades físicas. Por lo general, aunque no necesariamente, estas cantidades toman la forma de señales eléctricas o magnéticas capaces de almacenarse, transferirse, combinarse, compararse y manipularse de otro modo en un sistema informático. A veces ha resultado conveniente, principalmente por razones de uso común, referirse a estas señales como bits, valores, elementos, símbolos, caracteres, términos, números o similares.

[0020] Sin embargo, se debe tener en cuenta que todos estos y términos similares se deben asociar con las cantidades físicas apropiadas y son simplemente etiquetas convenientes aplicadas a estas cantidades. A menos que se indique específicamente lo contrario en las siguientes discusiones, se apreciará que a lo largo de las discusiones se utilicen términos como "acceso", "escritura",

"incluido", "almacenamiento", "transmisión", "recorrido", "asociación". "identificación" o similares, para referirse a la acción y procesos de un sistema informático o dispositivo informático electrónico similar que manipula y transforma los datos representados como cantidades físicas (electrónicas) dentro de los registros y memorias del sistema informático en otros datos representados de forma similar como cantidades físicas dentro de las memorias o registros del sistema informático u otros dispositivos de almacenamiento, transmisión o visualización de información.

[0021] Las implementaciones descritas en este documento se pueden discutir en el contexto general de instrucciones ejecutables por computador que residen en alguna forma de medio de almacenamiento legible por computador, tal como módulos de programa, ejecutados por uno o más computadores u otros dispositivos. A modo de ejemplo, y no de limitación, los medios de almacenamiento legibles por computador pueden comprender medios de almacenamiento informático no transitorios y medios de comunicación. Generalmente, los módulos del programa incluyen rutinas, programas, objetos, componentes, estructuras de datos, etc., que realizan tareas particulares o implementan tipos de datos abstractos particulares. La funcionalidad de los módulos de programa se puede combinar o distribuir como se desee en diversas implementaciones.

[0022] Los medios de almacenamiento informático incluyen medios volátiles y no volátiles, extraíbles y no extraíbles implementados en cualquier método o tecnología para el almacenamiento de información tal como instrucciones legibles por computador, estructuras de datos, módulos de programa u otros datos. Los medios de almacenamiento informático incluyen, pero no se limitan a, memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM),

ROM programable borrrable eléctricamente (EEPROM), memoria flash u otra tecnología de memoria, ROM de disco compacto (CD-ROM), discos versátiles digitales (DVD) u otro almacenamiento óptico, casetes magnéticos, cinta magnética, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que se pueda usar para almacenar la información deseada y a la que se pueda acceder para recuperar esa información.

[0023] Los medios de comunicación pueden incorporar instrucciones ejecutables por computador, estructuras de datos y módulos de programa, e incluyen cualquier medio de entrega de información. A modo de ejemplo, y no de limitación, los medios de comunicación incluyen medios cableados tales como una red cableada o conexión de cableado directo, y medios inalámbricos tales como medios acústicos, de radiofrecuencia (RF), infrarrojos y otros medios inalámbricos. Las combinaciones de cualquiera de los anteriores también se pueden incluir dentro del alcance de los medios legibles por computador.

[0024] Las implementaciones de la presente invención se describen dentro del contexto de un centro de contacto, e.g., un centro de contacto utilizado para facilitar las interacciones y/o comunicaciones entre agentes y clientes a través de una red telefónica, como el manejo de llamadas entrantes y salientes. En una o más implementaciones, se emplea un centro de contacto para proporcionar servicios a clientes en nombre de un tercer cliente a través de diversos sistemas y métodos de interacción y/o comunicación con el cliente. Una configuración típica de un centro de contacto incluye, por ejemplo, una ubicación centralizada ubicada remotamente desde una parte sustancial -si no la gran mayoría- de los clientes o clientes que contribuyen al volumen de llamadas. Por ejemplo, para los centros de contacto que operan bajo el ámbito de una institución

bancaria, en lugar de utilizar empleados bancarios, la institución puede ser un cliente de un tercer proveedor que opera el centro de contacto, y los contratos con el centro de contacto para proporcionar servicios bancarios a sus clientes. En tal ejemplo, al menos una parte de los servicios de banca personal llevados a cabo por teléfono u otros canales de comunicación de larga distancia son proporcionados por los agentes del centro de contacto a través de la interacción directa con los clientes.

[0025] De acuerdo con una o más implementaciones, un centro de contacto puede soportar la interacción y/o la comunicación entre un agente y un cliente a lo largo de uno o más canales de comunicación. Un tipo de interacción implica comunicaciones telefónicas entre un agente y un cliente a través de una red telefónica (e.g., red móvil, red pública conmutada, combinaciones de red conmutada pública y móvil, etc.). Otros tipos de interacciones y/o comunicaciones entre un agente y un cliente también incluyen, pero no se limitan a: videoconferencia, texto, mensajes de texto, comunicaciones basadas en Internet, etc.

[0026] Los centros de contacto, por diseño, permiten a los agentes empleados acceder a información personal e identificable, clientes de clientes mantenidos por los clientes correspondientes. Por ejemplo, un cliente que es un banco puede almacenar información personal utilizada para identificar clientes y otra información bancaria relacionada con el cliente (e.g., activos del cliente, etc.), mientras que otro cliente (e.g., compañía de seguros, proveedor de servicios de salud y otros) pueden tener acceso a registros de salud de empleados y/o clientes individuales. Debido a que esa información (e.g., financiera y de salud) es fácilmente accesible, un agente puede usar potencialmente esa información para beneficio personal. Por ejemplo, un agente puede solicitar crédito usando

información relacionada con un cliente, un agente puede comprar artículos en línea usando información de la tarjeta de crédito asociada con un cliente, o un agente puede vender información personal de salud de un cliente conocido.

[0027] Para abordar estos problemas, las implementaciones de la presente invención proporcionan la capacidad de identificar, recopilar evidencia y prevenir la actividad fraudulenta realizada por los agentes del centro de contacto durante el cumplimiento de las operaciones normales del centro de contacto. Otras implementaciones de la presente invención proporcionan la capacidad de alertar a los administradores del sistema cuando se detecta una posible actividad fraudulenta, y/o bloquear el acceso posterior/continuo del agente de centro de contacto fraudulento a la información personal e identificable del cliente.

[0028] Las implementaciones de la presente invención describen técnicas para detectar actividad fraudulenta potencial con base en información recopilada supervisando la actividad de llamadas durante las sesiones de llamadas (e.g., solicitudes de servicio o información, etc.) y comparando la actividad y el comportamiento del agente que recibe datos potencialmente sensibles o información valiosa desde el punto de vista financiero para ejemplos bien definidos de comportamiento apropiado, o alternativamente para un comportamiento potencialmente fraudulento. Por ejemplo, cierta actividad puede coincidir con un patrón de actividad que se sabe está asociado con actividad fraudulenta. En otros ejemplos más, cuando las actividades de un agente están fuera de las normas estadísticas asociadas con un grupo de agentes, dicha actividad puede indicar actividad fraudulenta potencial. Una vez que se ha marcado la posible actividad fraudulenta de un agente, se puede realizar una investigación adicional para determinar si se ha llevado a cabo una actividad fraudulenta real y se pueden emplear otras medidas de seguridad para la prevención. Además de la prevención

activa y directa (e.g., deshabilitar más actividad del agente), la actividad fraudulenta puede ser disuadida entendiendo que la actividad de los agentes está siendo supervisada, el comportamiento fraudulento puede ser detectado con éxito y que la actividad fraudulenta está sujeta al riesgo de enjuiciamiento criminal.

[0029] Mientras que las siguientes configuraciones de ejemplo se muestran como que incorporan características y elementos enumerados específicos, se entiende que dicha descripción es de ejemplo. En consecuencia, las implementaciones son muy adecuadas para aplicaciones que implican elementos, características o disposiciones diferentes, adicionales o menores.

SISTEMA DE COMPUTADOR DE EJEMPLO

[0030] La FIG. 1 es un diagrama de bloques de un ejemplo de un sistema informático 100 capaz de realizar las implementaciones de la presente descripción. El sistema informático 100 representa ampliamente a cualquier dispositivo o sistema informático de un solo procesador o multiprocesador capaz de ejecutar instrucciones legibles por computador. Los ejemplos del sistema informático 100 incluyen, sin limitación, estaciones de trabajo, computadores portátiles, terminales del lado del cliente, servidores, sistemas informáticos distribuidos, dispositivos portátiles o cualquier otro sistema o dispositivo informático. En su configuración más básica, el sistema informático 100 incluye típicamente al menos una unidad de procesamiento y memoria 101, y un bus de dirección/datos 109 (u otra interfaz) para comunicar información. Según la configuración exacta y el tipo de entorno del sistema informático, la memoria del sistema generalmente representa cualquier tipo o forma de dispositivo de almacenamiento volátil o no volátil o medio capaz de almacenar datos y/u otras instrucciones legibles por computador. Los ejemplos de memoria del sistema

incluyen, sin limitación, volátiles (tales como RAM 102), no volátiles (tales como ROM 103, memoria flash, etc.), o cualquier otro dispositivo de memoria adecuado. En una o más implementaciones, la memoria puede incluir un búfer marco para almacenar unidades de datos de píxeles en un dispositivo de visualización 110.

[0031] El sistema informático 100 también puede comprender un subsistema gráfico opcional 105 para presentar información a un usuario, por ejemplo, mostrando información en un dispositivo de visualización conectado 110, mediante un cable de video 111. De acuerdo con las implementaciones de la presente invención reivindicada, el subsistema de gráficos 105 se puede acoplar directamente al dispositivo de visualización 110 a través del cable de video 111. En implementaciones alternativas, el dispositivo de visualización 110 se puede integrar en el sistema informático (e.g., un computador portátil o panel de visualización de netbooks) y no requerirá un cable de video 111.

[0032] Además, el sistema informático 100 también puede tener características/funcionalidades adicionales. Por ejemplo, el sistema informático 100 también puede incluir almacenamiento adicional (extraíble y/o no extraíble) que incluye, pero no se limita a, discos magnéticos u ópticos o cinta. Los medios de almacenamiento informático incluyen medios volátiles y no volátiles, extraíbles y no extraíbles implementados en cualquier método o tecnología para el almacenamiento de información tal como instrucciones legibles por computador, estructuras de datos, módulos de programa u otros datos. La RAM 102, la ROM 103 y el dispositivo de almacenamiento de datos externo (no mostrado) son todos ejemplos de medios de almacenamiento informático.

[0033] El sistema informático 100 también comprende un dispositivo de entrada alfanumérico opcional 106, un dispositivo de dirección o control de cursor

opcional 107 y una o más interfaces de comunicación de señal (dispositivos de entrada/salida, (e.g., una tarjeta de interfaz de red) 108. El dispositivo de entrada alfanumérico opcional 106 puede comunicar las selecciones de información y comando al procesador central 101. El dispositivo de dirección o control de cursor opcional 107 está acoplado al bus 109 para comunicar información de entrada de usuario y selecciones de comandos al procesador central 101. La interfaz de comunicación de señal (dispositivo de entrada/salida) 108, también acoplada al bus 109, puede ser un puerto serie. La interfaz de comunicación 108 también puede incluir mecanismos de comunicación inalámbrica. Usando la interfaz de comunicación 108, el sistema informático 100 puede acoplar comunicativamente a otros sistemas informáticos a través de una red de comunicación tal como Internet o una intranet (e.g., una red de área local).

[0034] En algunas implementaciones, un medio legible por computador que contiene un programa informático se puede cargar en el sistema informático 100. Todo o una parte del programa informático almacenado en el medio legible por computador luego se puede almacenar en la memoria del sistema y/o en varias partes de dispositivos de almacenamiento. Cuando se ejecutan por las unidades de procesamiento 101 y/o 105, un programa informático cargado en el sistema informático 100 puede hacer que el procesador 101 y/o 105 realice y/o sean un medio para realizar las funciones de las implementaciones de ejemplo descritas y/o ilustradas en la presente. Adicional o alternativamente, las implementaciones de ejemplo descritas y/o ilustradas en este documento se pueden implementar en firmware y/o hardware.

[0035] La FIG. 2 es una ilustración de un sistema 200 para controlar la actividad del agente con base en la comunicación verbal convertida realizada entre un agente y un cliente (llamante) para detectar actividad fraudulenta

potencial realizada por un agente dentro de un centro de contacto, de acuerdo con las implementaciones de la presente descripción. Uno o más componentes del sistema 200 se pueden implementar, por ejemplo, mediante el sistema informático 100 de la FIG. 1 con el propósito de controlar la actividad de agentes y/o estaciones de trabajo para identificar actividad fraudulenta potencial y realizar acciones adicionales una vez que se detecta la actividad, de acuerdo con una implementación de la presente divulgación.

[0036] De acuerdo con una o más implementaciones, el Sistema 200 incluye un centro de contacto 210 operado por uno o más agentes de una empresa u organización para manejar las interacciones con los clientes de la empresa u organización. En implementaciones alternativas, el centro de contacto puede operar en nombre de una empresa u organización cliente y gestionado por un proveedor de servicios a terceros. De acuerdo con dichas implementaciones, los agentes pueden ser entrenados y encargados de proporcionar soporte e información a uno o más clientes 270 con respecto a productos y/o servicios asociados con un negocio u organización cliente. Además de responder a las solicitudes de soporte e información, las tareas que los agentes del centro de contacto 210 pueden realizar incluyen (pero no se limitan a) ayudar al cliente a completar una venta de un producto o servicio, ayudar al cliente a acceder a la información administrada por el cliente, o guiar cooperativamente al cliente para manejar temas y problemas con productos o servicios proporcionados u ofrecidos por el cliente.

[0037] Los clientes 270 pueden interactuar con agentes en estaciones de trabajo 230 a través de una o más redes de comunicación 250 y 255. Por ejemplo, la red de comunicación 255 puede incluir un sistema de redes informáticas interconectadas (e.g., internet) que permite la comunicación directa entre un

usuario y un cliente. Además, la red de comunicación 250 puede ser cualquier combinación de redes telefónicas que están configuradas para conectar un cliente a un agente en una estación de trabajo particular, como una red de telefonía móvil, una red telefónica pública conmutada (PSTN) basada en línea terrestre, etc.

[0038] De acuerdo con una o más implementaciones, el centro de contacto 210 puede incluir una red 220 de estaciones de trabajo 230, que incluyen estaciones de trabajo 230A-N, cada estación de trabajo es atendida por uno o más agentes. En una o más implementaciones, una estación de trabajo se puede compartimentar como una unidad escalable, y está configurada para proporcionar recursos esenciales que un agente utiliza para manejar las solicitudes de un cliente en nombre de un cliente. Por ejemplo, una estación de trabajo puede integrar un sistema informático (no mostrado) y un componente telefónico (no mostrado) en una plataforma de trabajo individual. Al proporcionar una infraestructura que incluye recursos sustanciales de estación de trabajo y recursos humanos (agente), un centro de contacto 210 puede instalar y mantener grandes volúmenes de llamadas de manera eficiente. Además, al proporcionar una ubicación centralizada para estaciones de trabajo, los agentes tienen acceso inmediato a información, recursos y supervisores para ayudar a lograr y mantener la más alta calidad de servicio a los clientes del cliente.

[0039] Como se representa en la figura 2, cada sistema informático de estación de trabajo está configurado para acceder al menos a un recurso 240 de un cliente a través de una red de comunicación 255. Por ejemplo, el sistema informático de estación de trabajo puede ejecutar una aplicación operada por el cliente que está configurada para acceder una base de datos que contiene información relacionada con los clientes del negocio u organización del cliente. El sistema informático de estación de trabajo también se puede configurar para

proporcionar comunicación entre un cliente y un agente en la estación de trabajo. Por ejemplo, la comunicación puede incluir comunicaciones de voz con base en Internet, navegación de un sitio web compartido al que acceden simultáneamente el cliente y el agente, comunicación basada en texto, etc. En una o más implementaciones, el componente telefónico de una estación de trabajo está configurado para proporcionar comunicación (e.g., voz) entre un cliente y un agente que atiende la estación de trabajo. Por ejemplo, el componente telefónico puede estar acoplado a un teléfono correspondiente del cliente a través de la red de comunicación 250 y/o la red 255.

[0040] Como se presenta en la Figura 2, un sistema de supervisión de fraude en un centro de contacto 210 tal como el sistema 200 también incluye un centro de seguridad 260 que está acoplado comunicativamente a la pluralidad de estaciones de trabajo 230 del centro de contacto 210, y está configurado para recibir información relacionada con actividades realizadas por agentes en una pluralidad de sistemas informáticos asociados con las estaciones de trabajo 230. En una implementación, el centro de seguridad 260 se puede implementar como uno o más dispositivos informáticos (e.g., servidores) que incluyen una o más unidades de procesamiento, uno o más dispositivos de almacenamiento y memoria, y uno o más dispositivos de visualización. La una o más unidades de procesamiento pueden ejecutar instrucciones programadas almacenadas en uno o más dispositivos de memoria para implementar un motor de observación 261 que recibe y procesa continuamente información desde estaciones de trabajo en uno o más centros de contacto. Por ejemplo, un módulo de colector de información 263 del motor observador 261 está acoplado comunicativamente a cada una de las estaciones de trabajo 230A-N, y está configurado para recibir información que se puede usar para controlar la actividad de agentes y se puede usar para determinar cuándo se está realizando una actividad fraudulenta potencial. La información se

puede almacenar en un almacenamiento en el centro de seguridad 260 para un acceso posterior, tal como cuando se realiza un análisis de la información en un momento posterior.

[0041] En una o más implementaciones, la información recogida por el módulo de recopilación de información 263 incluye una transcripción convertida de la comunicación verbal entre un cliente y el agente de servicio, así como un registro de la actividad que el agente realiza que responda a (i.e., que ocurre temporalmente cerca de) la comunicación verbal. En una o más implementaciones, la conversión de voz a texto se puede realizar localmente en la estación de trabajo del agente, e.g., mediante una aplicación de seguridad asociada con el motor del observador que se ejecuta en el sistema informático de la estación de trabajo. El discurso se puede convertir y transmitir en tiempo real o en partes discretas (fragmentos) desde la estación de trabajo. De acuerdo con implementaciones alternativas, la comunicación verbal en sí misma se puede grabar y transmitir, bien sea, en tiempo real (e.g., transmitida) o en partes discretas (fragmentos) al centro de seguridad 260 y convertirse en una conversión ASR 264 implementada por el motor observador 261.

[0042] En una implementación, la detección de fraude se puede realizar localmente en un monitor correspondiente de una estación de trabajo, o se puede realizar remotamente en el centro 260 de seguridad, donde la detección se basa en la información recogida de una aplicación observadora correspondiente que se ejecuta en la respectiva estación de trabajo. Por ejemplo, el centro de seguridad 260 puede incluir una unidad de detección de fraude 266 que está configurada para detectar una actividad fraudulenta potencial que está siendo realizada por un agente en una estación de trabajo. En otra implementación, la unidad de detección de fraude está ubicada en una estación de trabajo, en la que la detección y las

medidas subsiguientes tomadas se controlan localmente en esa estación de trabajo. En otras implementaciones adicionales, la detección de fraude se realiza en múltiples ubicaciones, tales como localmente en la estación de trabajo y de forma remota en el centro de seguridad.

[0043] La unidad de detección de fraude puede determinar la actividad fraudulenta potencial (e.g., la unidad de detección de fraude 266) comparando el registro de actividad del agente y la transcripción convertida de la comunicación verbal con un modelo de comportamiento 265 de las actividades históricas y/o ideales del agente, realizadas en circunstancias similares. Por ejemplo, se puede realizar una búsqueda por palabra clave o un análisis contextual en la transcripción para determinar un posible propósito de la llamada, o el modelo de comportamiento 265 puede ser específico para un cliente o cliente en línea de negocios particular. Una vez que se detecta actividad potencialmente fraudulenta, se pueden tomar medidas de seguridad, preventivas y/o correctivas, para eliminar o minimizar el riesgo para el cliente afectado. La(s) medida(s) de seguridad apropiada(s) que se tomarán se pueden determinar utilizando un motor de políticas 267 que considera una serie de factores y selecciona qué medida(s) de seguridad, si corresponde, debe realizar en respuesta a la actividad potencialmente fraudulenta detectada.

[0044] La FIG. 3 Es un diagrama componente de una estación de trabajo 300 del centro de contacto configurada para supervisar la actividad de un agente del centro de contacto y la comunicación verbal intercambiada entre el agente del centro de contacto y una persona que llama con el fin de identificar actividad fraudulenta potencial realizada por el agente, de acuerdo con una implementación de la presente divulgación. De acuerdo con una o más implementaciones, la estación de trabajo 300 se puede implementar como, por ejemplo, el sistema 100

de la FIG. 1 (descrito anteriormente) con el fin de supervisar la actividad de un agente y/o estación de trabajo correspondiente para identificar posibles actividades fraudulentas y realizar acciones adicionales una vez que se detecte la actividad. Además, la estación de trabajo 300 es representativa de las estaciones de trabajo 230A-N en la FIG. 2.

[0045] En una o más implementaciones, la estación de trabajo 300 está configurada para permitir la supervisión en tiempo real, la detección de fraude y la prevención del fraude, como se hace a través de las implementaciones de la presente invención. Por ejemplo, los diferentes componentes de la estación de trabajo 300 operan juntos para supervisar la comunicación y hacer seguimiento de la actividad del agente con el fin de detectar y documentar actividad fraudulenta, y para tomar acciones posteriores con el fin de prevenir futuros fraudes.

[0046] Como se describió previamente, cada estación de trabajo en un centro de contacto se puede organizar como una unidad escalable, y contiene componentes esenciales para permitir que un agente asistente se comunique con un cliente, y para proporcionar servicios a ese cliente en nombre de un cliente. Por ejemplo, el recurso de comunicación 320 permite que el agente se comunique con el cliente, y puede incluir un teléfono u otro dispositivo basado en voz o texto. Según otras implementaciones, el recurso de comunicación 320 también puede incluir una interfaz de comunicación con base en Internet que permite al agente comunicarse mediante protocolos basados en Internet a dispositivos informáticos en red similar (e.g., un dispositivo informático utilizado por un cliente). Como se representa, la estación de trabajo 300 también incluye un recurso informático 310 de propósitos múltiples.

[0047] En una implementación, el recurso informático 310 está configurado para acceder a los recursos del cliente. Por ejemplo, cuando maneja o participa en una interacción con un cliente (e.g., manejando una llamada de un cliente), el agente que actúa en nombre de un cliente y a través del recurso informático 310 tiene acceso a recursos basados en el cliente (e.g., aplicaciones, bases de datos, etc.) que contienen información personal e identificable relacionada con el cliente. En una o más implementaciones, se puede acceder a la información desde dispositivos de almacenamiento de datos ubicados remotamente, accesibles a una aplicación que se ejecuta en la estación de trabajo 300 a través de una conexión de red segura (e.g., el recurso de comunicación 320).

[0048] Además, el recurso informático 310 se puede configurar para permitir la comunicación primaria o de soporte con un cliente. Por ejemplo, el recurso informático 310 se puede usar para habilitar o facilitar el acceso simultáneo de un sitio web por parte del cliente y el agente. De acuerdo con otras implementaciones, el recurso informático 310 se puede usar junto con una cámara de video y/o un micrófono para habilitar y facilitar la funcionalidad de videoconferencia entre un cliente y el agente. Además, las capacidades del recurso informático 310 se pueden utilizar para implementar la supervisión de la comunicación entre un cliente y un agente, el seguimiento de la actividad del agente en el recurso informático 310, la detección de fraude y/o la prevención del fraude independientemente de o en combinación con otros componentes en la estación de trabajo 300, o componentes o dispositivos ubicados remotamente (e.g., ubicados en un centro de seguridad).

[0049] La estación de trabajo 300 también incluye una aplicación 330 de observación, que está configurada para controlar la comunicación entre un cliente

y un agente y hacer seguimiento de la actividad de los componentes dentro de la estación de trabajo 300 y/o la actividad del agente correspondiente solo o junto con esos componentes. En las implementaciones, la aplicación de observador 330 se puede ejecutar mediante el recurso informático 310, y representa una instanciación de una aplicación distribuida. En una o más implementaciones, la aplicación de observador 330 incluye una unidad de supervisión 332 configurada para detectar y registrar la comunicación verbal entre un agente y un cliente durante una sesión de contacto (llamada). En una o más implementaciones, por ejemplo, la comunicación verbal se puede grabar en una pluralidad de cadenas discretas o fragmentos de conversación y almacenar en un búfer en la estación de trabajo 300.

[0050] La unidad de supervisión 332 también está configurada para hacer seguimiento la actividad realizada por el agente asistente durante la sesión o partes de la sesión, de modo que se puede generar un registro de uso que indique en qué momentos se utilizó el recurso de comunicación 320 o se accedió a los datos de un cliente, y cualquier actividad realizada por el agente en cualquier campo de cualquier aplicación de co-ejecución, y/o en el nivel del sistema operativo. Por lo tanto, la unidad de supervisión 332 puede seguir cuando el recurso informático 310 se conecta y desconecta (e.g., inicia y cierra sesión) del centro de contacto y/o los recursos en una estación de trabajo correspondiente, cuando el recurso informático 310 está ejecutando una aplicación de un cliente, cuando el recurso informático 310 está accediendo a un recurso particular del cliente, y cualquier otra actividad cuantificable que se realiza en el recurso informático 310.

[0051] De acuerdo con una o más implementaciones, la unidad de supervisión 332 puede hacer seguimiento al estado de un agente asistente en la

estación de trabajo 300 con base en la entrada proporcionada al recurso informático 310 por el agente. Por ejemplo, la unidad de supervisión 332 puede determinar la disponibilidad del agente asistente basándose en el estado de inicio de sesión del recurso informático 310. En otros casos, la unidad de supervisión 332 puede hacer seguimiento cuándo el agente está en una pausa, o salir a la hora del almuerzo, según el historial de actividad del recurso informático 310, o según el estado de inicio de sesión proporcionado por el agente al recurso 310.

[0052] Como se muestra en la Figura 3, la aplicación de observador 330 también incluye la unidad de conversión 334. En una o más implementaciones, la conversación grabada entre el agente y el cliente se recibe en la unidad de conversión 334 y una representación textual se genera por la unidad de conversión 334. La representación textual puede incluir, por ejemplo, una transcripción de la conversación. En una o más implementaciones, la representación textual se genera usando un sistema de reconocimiento automático de voz (ASR). De acuerdo con una o más implementaciones, se puede generar una representación textual para toda la conversación grabada (detectada) para una sesión. De acuerdo con implementaciones alternativas, se puede generarse la representación textual a través de una pluralidad de fragmentos. En una o más implementaciones, los fragmentos se pueden organizar en función de una duración de tiempo, o siempre que se detecten pausas en la conversación que superan un cierto umbral. En aún otras implementaciones, los fragmentos se pueden organizar analizando la grabación de la conversación o la representación textual de la conversación y aplicando un análisis contextual a la representación textual para identificar pausas naturales o interrupciones en las conversaciones.

[0053] Con base en la información recopilada por la aplicación de observador 330, se puede realizar un análisis adicional. Por ejemplo, se puede

usar la información recopilada de una o más estaciones de trabajo para establecer una línea base de la actividad específica del agente para un agente individual, para agentes como un grupo, para un propósito específico (e.g., venta de un producto, solicitud de servicio) y/o para un cliente específico o una línea de negocios específica de un cliente. La información también se puede usar para establecer una línea base de actos fraudulentos frecuentes o comunes. Las ilustraciones de los datos de la línea base incluyen el tiempo promedio de manejo o participación en una interacción con un cliente, el tiempo promedio que asiste a un cliente en una llamada, el tiempo promedio de acceso a un recurso del cliente, la cantidad de veces que se accede a un recurso del cliente, el momento en el que el agente puso a los clientes en espera, los datos o entradas que ingresa un agente, la aplicación o la información a la que accede el agente, etc. Esta información se puede agregar para establecer el comportamiento apropiado u óptimo de un agente entre un grupo de agentes, para una tarea o propósito específico o para un cliente específico o una línea de negocios basada en una comparación con el promedio estadístico. Esta información también se puede usar para determinar si ha ocurrido una actividad fraudulenta potencial, como cuando la actividad del agente cae fuera de la norma estadística o realiza acciones que no están dentro del alcance de la actividad de seguimiento normal para el propósito/cliente/línea de negocio, como se describirá más detalladamente a continuación.

[0054] Como se representa, la aplicación del observador 330 también incluye una unidad de detección de fraude 336. Con base en la información recogida por la unidad de control 332, la unidad de detección de fraude 336 puede determinar cuándo ciertas actividades o combinación de actividades realizadas en o por los componentes de la estación de trabajo 300 y/o el agente asistente pueden constituir actividades potencialmente fraudulentas que está realizando el

agente. Por ejemplo, según lo determinado por la unidad de prevención de fraude 336, la información recopilada puede coincidir con ciertas reglas o patrones de actividades que se sabe que ocurren cuando se realiza un fraude. En otros casos, se puede detectar una actividad fraudulenta potencial cuando la actividad del agente cae fuera de la norma estadística de un grupo de agentes, ese agente particular, o para el propósito determinado/cliente/línea de negocio.

[0055] Según una o más implementaciones, la unidad de prevención de fraudes 336 determina la actividad potencialmente fraudulenta comparando continuamente la actividad del agente rastreado (e.g., como un registro de la actividad del agente) y la representación textual convertida de la conversación entre el agente y el cliente de una sesión de llamada con un modelo de comportamiento que agrega datos de interacciones similares bajo las mismas condiciones o parámetros sustancialmente similares. Como tal, la unidad de prevención de fraude 336 puede proporcionar notificación que un agente está llevando a cabo una actividad fraudulenta potencial en la estación de trabajo 300. Por ejemplo, la notificación se puede proporcionar a través de un gráfico del centro de contacto.

[0056] En una o más implementaciones, el análisis realizado para detectar actividad fraudulenta potencial se puede realizar por la unidad de prevención de fraude 336 en la estación de trabajo local, una unidad de prevención de fraude remota (e.g., por un motor de comportamiento que se ejecuta en un servidor remoto tal como el centro de seguridad 260 descrito anteriormente con respecto a la figura 2), o una combinación de las unidades de prevención de fraude local y remoto. Cuando el análisis se realiza mediante un motor de comportamiento de ejecución remota, el registro de actividad y la representación textual se pueden transmitir desde la estación de trabajo del

agente al motor de comportamiento (que se ejecuta de forma remota). De acuerdo con una o más implementaciones, la transmisión del registro de actividad y la representación textual, el análisis de los materiales transmitidos y la detección de posibles fraudes pueden ocurrir en tiempo real. Alternativamente, la detección de un posible comportamiento fraudulento se puede realizar durante un período de análisis posterior a la ocurrencia.

[0057] Cuando se detecta una actividad fraudulenta potencial, se pueden promulgar uno o más protocolos de seguridad para hacer cumplir una o más políticas de seguridad. Estas políticas pueden incluir la realización de acciones de seguridad tales como: marcar la actividad del agente supervisión como una posible actividad fraudulenta; generar una notificación a un administrador del sistema; generar un informe de actividad fraudulenta potencial para el administrador del sistema; supervisar la actividad adicional del agente; y suspender más actividad del agente en la estación de trabajo. Según una o más implementaciones, la (s) acción (es) de seguridad específica (s) seleccionada (s) a ser realizadas se pueden determinar durante o como resultado del análisis para detectar actividad fraudulenta potencial, y se pueden basar en, por ejemplo, la probabilidad o certeza de actividad fraudulenta que ha ocurrido o está a punto de ocurrir, la gravedad o exposición al riesgo de la posible actividad fraudulenta detectada, el historial de empleo del agente en el centro de contacto, el cliente o la línea de negocio, etc.

[0058] La FIG. 4 es un diagrama de flujo 400 que ilustra un método para controlar la actividad del agente para un posible comportamiento fraudulento y realizar medidas preventivas una vez que se detecta la actividad potencialmente fraudulenta, de acuerdo con una o más implementaciones de la presente divulgación. Las etapas 410-460 describen etapas de ejemplo que comprenden el

proceso 400 representado en la figura 4 de acuerdo con las diversas implementaciones descritas en este documento. En una implementación, el proceso 400 se implementa al menos en parte como instrucciones ejecutables por computador almacenadas en un medio legible por computador y ejecutadas en un dispositivo informático. De acuerdo con diversas implementaciones, el método descrito en el diagrama de flujo 400 se puede implementar y/o ejecutar mediante uno o más componentes de los sistemas 100, 200 y 300 de las FIGS. 1-3, respectivamente.

[0059] En 410, el método incluye detectar una inicialización de sesión de llamada. La sesión de llamada puede comprender, por ejemplo, una llamada entrante iniciada por un cliente y recibida en una estación de trabajo asignada a un agente y se puede recibir a través de un dispositivo telefónico a través de una red de voz (e.g., red 250 de la figura 2), y/o como una comunicación con base en Internet a través de una interfaz de red a Internet (e.g., la red 255 de la figura 2). Alternativamente, la sesión de llamada también puede comprender una llamada saliente, iniciada por el agente (e.g., marcando un número de teléfono) o un sistema automatizado que realiza la marcación (u otro direccionamiento) y facilita la conexión entre el agente y el cliente. Según una o más implementaciones, la llamada (bien sea, entrante o saliente si el sistema la inicia automáticamente) se puede recibir en un grupo compartido o en una cola de llamadas, accesible a cualquiera de una serie de agentes en un número correspondiente de estaciones de trabajo.

[0060] Una vez recibido en la etapa 410, se supervisa la sesión de llamada. La supervisión de la sesión de llamada consiste, por ejemplo, en hacer seguimiento el estado de la telefonía o la interfaz de telefonía del computador (CTI) de la interfaz utilizada para conectar un agente con el cliente, supervisar la

comunicación verbal (conversación) que tiene lugar entre el agente y el cliente durante la sesión de llamada y el seguimiento de la actividad del agente en cualquier aplicación que se ejecute en la estación de trabajo. En una o más implementaciones, la comunicación de audio se puede supervisar usando protocolos de comunicación de voz y video-teleconferencia, tales como el Protocolo de Transporte en Tiempo Real (RTP), y/o el Protocolo de Inicio de Sesión (SIP). Los protocolos específicos utilizados se pueden adherir a los estándares de la industria (e.g., el estándar H.323 para señalización y control de llamadas). La comunicación de audio se captura de acuerdo con el (los) protocolo (s) aplicable (s), y los paquetes de datos que representan la comunicación se generan y transmiten al dispositivo receptor y al usuario. De acuerdo con una o más implementaciones, los paquetes de datos transmitidos pueden ser interceptados inicialmente y convertidos a texto (ver etapa 420 a continuación) antes del envío al dispositivo receptor (y al usuario).

[0061] Como se discutió previamente, la supervisión permite la recopilación de información relacionada con las actividades de los agentes y/o actividades que se realizan sobre los recursos utilizados por los agentes. En una implementación, se controla la actividad electrónica de los agentes (e.g., actividad de la computadora, actividad del teléfono, etc.). Además, la información supervisada se puede recoger en una ubicación centralizada para almacenamiento y análisis. En una implementación, el método incluye supervisar un primer agente en una primera estación de trabajo, y en particular supervisar las interacciones del agente con los recursos (e.g., recurso informático) de la estación de trabajo. Además, se puede supervisar la interacción del agente con un recurso del cliente. Por ejemplo, se supervisa la interacción con una base de datos de clientes. Además, se supervisa la interacción del agente con el sistema de comunicación para determinar cuándo el agente maneja o está involucrado en una

interacción (e.g., en una llamada) y si el agente está disponible para ayudar a un nuevo cliente a través de otra interacción (e.g., tomar otra llamada).

[0062] En una implementación, la supervisión es continua, en la que la supervisión se realiza cuando el agente maneja o está involucrado en una interacción (e.g., manejo de llamadas), y cuando el agente no está manejando o no está involucrado en una interacción. Es decir, se supervisa toda la actividad del agente y/o las actividades que se llevan a cabo sobre los recursos de la estación de trabajo. En otras implementaciones, la supervisión se realiza de forma periódica o aleatoria. Por ejemplo, solo se necesita una muestra estadística para determinar la actividad fraudulenta y, en lugar de desperdiciar recursos, la supervisión se realiza de forma no continua.

[0063] En la etapa 420, la comunicación verbal se convierte en una representación textual. En una o más implementaciones, se genera una transcripción de la conversación usando técnicas de reconocimiento automático de voz (ASR) (e.g., software). De acuerdo con una implementación, la conversación se puede grabar y almacenar en tiempo real (e.g., en un búfer en la memoria), y la conversión se genera a partir de los datos grabados en el búfer. La conversión se puede realizar para la conversación de acuerdo con incrementos predeterminados (e.g., 10, 30, 60 segundos), de modo que, en otro momento la conversión se realiza de forma incremental. La conversación y la conversión segura resultante se pueden generar mediante el almacenamiento temporal de incrementos de duración después de la detección de palabras clave predefinidas utilizadas en la conversación. En implementaciones alternativas, la conversación se puede convertir en tiempo real (e.g., como una transmisión) para toda o partes de la conversación. De acuerdo con implementaciones adicionales, la conversación se puede grabar y transmitir para ser convertida remotamente (e.g., en el centro de

seguridad 260 de la Figura 2), bien sea en su totalidad (después de que se haya completado la llamada), o en fragmentos a intervalos predefinidos.

[0064] En la etapa 430, la representación textual (e.g., transcripción) de toda o partes de la comunicación entre el agente y el cliente generado en la etapa 420 se evalúa con un registro de la actividad del agente al que se le hizo seguimiento en la etapa 410. En una o más implementaciones, la evaluación del texto y el registro de actividad se realizan en un motor de comportamiento implementado como parte de una aplicación de supervisión u observación e instanciado en un servidor acoplado comunicativamente a una o más estaciones de trabajo en uno o más centros de contacto. El motor de comportamiento evalúa los datos de entrada del texto convertido y el registro de actividad comparando los datos de entrada con un modelo de comportamiento que incluye un comportamiento potencialmente fraudulento estadístico y/o aprobado y/o conocido de acuerdo con uno o más parámetros. Estos parámetros pueden incluir, por ejemplo, un comportamiento histórico y/o aprobado que responda a los escenarios determinados en circunstancias similares (e.g., fines definidos), o para productos, servicios o clientes específicos. De acuerdo con una o más formas de implementación, una línea de negocio de producto, servicio, cliente o cliente específico puede tener un modelo de comportamiento correspondiente único.

[0065] En una o más implementaciones, la evaluación se puede realizar analizando la conversación entre el agente y el cliente para determinar temas estadísticamente probables. Por ejemplo, se puede realizar una búsqueda por palabra clave en términos de propósito común, como "dirección", "número de tarjeta de crédito" o "problema". Otros ejemplos de posibles palabras clave de interés incluyen, pero no se limitan a, información de devolución de autorización de mercancía (RMA), prescripciones médicas, reservas de viajes, números de

cuenta, etc. El texto convertido próximo a los términos buscados se puede analizar más exactamente determinar con precisión el propósito de la llamada o un tema particular de la conversación. Las acciones del agente que respondan o correspondiente a los términos que se referencian en el registro de actividad (e.g., a través del sellado de tiempo) se evalúan luego a la vista de la conversación.

[0066] En una o más implementaciones, las acciones se evalúan de acuerdo con la aplicación y el nivel de campo. Así, por ejemplo, la aplicación y el campo dentro de la aplicación utilizada por un agente para ingresar una secuencia de números proporcionada por un cliente en respuesta a la frase "tarjeta de crédito" se rastrean y evalúan estadísticamente tanto para normal, aprobado y/o actividad fraudulenta potencialmente conocida. De acuerdo con implementaciones alternativas, la evaluación se puede realizar aplicando un análisis contextual y/o una coincidencia de patrón del texto convertido y se puede realizar adicionalmente la actividad del agente en relación con un modelo de comportamiento además de, o en lugar de una búsqueda por palabra clave.

[0067] En la etapa 440, cualquier inconsistencia entre las acciones del agente (según se inspecciona en el registro de actividad) y las correspondientes acciones autorizadas y/o estadísticamente normales según el modelo de comportamiento se detectan durante la evaluación realizada en la etapa 430. Si no se detectan inconsistencias, el proceso vuelve a la etapa 420 para implementaciones en las que la conversión y evaluación del texto se realizan en tiempo real (e.g., transmitido) durante la llamada, o a la etapa 430 para las implementaciones en las que la conversión de texto se realiza un tiempo antes de la evaluación (e.g., usando un búfer, o una parte grabada). Sin embargo, el proceso avanza a la etapa 460 y finaliza cuando la conversación completa (o parte evaluada de la conversación convertida) finaliza sin detectar ninguna incoherencia

entre las acciones del agente y el comportamiento aprobado según el modelo de comportamiento.

[0068] Cuando se detecta una inconsistencia, o, alternativamente, si se detecta una acción que es conocida o que puede ser potencialmente fraudulenta, el proceso pasa a la etapa 450 para realizar acciones de seguridad. Se pueden implementar diversas técnicas para determinar que la actividad de un agente es potencialmente fraudulenta y que requiere más atención. Por ejemplo, en una implementación, un agente puede estar involucrado en una actividad sospechosa que generalmente es indicativa de actividad fraudulenta. En particular, cuando un agente está accediendo a información personal e identificable (e.g., a través de una base de datos de clientes) relacionada con un cliente de un cliente, pero no está ayudando al cliente (e.g., no en una llamada con el cliente), esa actividad es sospechosa. Esta actividad se puede identificar como que coincide con los criterios, y conduce a la determinación de que el agente pudo haber realizado una actividad fraudulenta potencial. Puede ser necesaria una investigación adicional para determinar si se ha producido un fraude real. Por otro lado, si la supervisión determina que el agente posicionado está accediendo a una base de datos de clientes para información del cliente y que el agente está ayudando actualmente a ese cliente en relación con la información accedida, entonces la actividad y el acceso a la base de datos del cliente están autorizados.

[0069] La determinación de que se ha producido una actividad fraudulenta potencial se puede realizar en un centro de seguridad que está centralizado en una pluralidad de estaciones de trabajo de un centro de contacto. En particular, el centro de seguridad está configurado para recibir una pluralidad de información relacionada con las actividades de agentes y/o actividades que se realizan sobre recursos de la pluralidad de estaciones de trabajo. Esa información,

recopilada en cada una de las estaciones de trabajo, luego se entrega a través de una red de comunicación al centro de seguridad para su posterior análisis, y más específicamente para determinar cuándo ha ocurrido una actividad fraudulenta potencial.

[0070] Por ejemplo, la determinación de que se ha producido una actividad fraudulenta potencial se basa en si la información relacionada con las actividades de un agente y/o las actividades que se realizan sobre los recursos de una estación de trabajo violan cualquier regla predefinida o predeterminada (e.g., un modelo de comportamiento). Las reglas se pueden definir por uno o más parámetros y/o criterios en el modelo de comportamiento. Más particularmente, se puede determinar que se ha producido una actividad fraudulenta potencial cuando la información indica una violación de una regla. Como ilustración, la regla puede definir una línea base de transacciones, acciones o actividades realizadas por uno o más agentes junto con el uso de los recursos de estación de trabajo (e.g., teléfono, recurso informático, etc.). Por ejemplo, la línea base se puede definir por un promedio estadístico en relación con una actividad asociada con el agente y/o la pluralidad de agentes. Además, la línea base se puede dirigir o corresponder a al menos una primera actividad. Por ejemplo, la línea base puede describir el número promedio de llamadas salientes realizadas por agentes durante un período de tiempo predefinido (e.g., 1 hora, 2 horas, turno diario, etc.). En otro ejemplo, la línea base puede describir el número de veces que un agente deja a los clientes en espera durante un período y/o la duración del tiempo de espera cada vez que un cliente se deja en espera.

[0071] Se puede supervisar y descubrir una condición atípica que se realiza por un agente, en donde la condición atípica se encuentra fuera de la línea base. Es decir, el valor atípico exhibe patrones de actividad inusuales. Si la

condición atípica satisface la regla (e.g., parámetros y/o criterios), entonces se puede hacer una determinación que ha ocurrido una actividad fraudulenta potencial. Además, la condición atípica puede coincidir con la actividad fraudulenta conocida que está asociada con la regla. Debido a que en ocasiones pueden aparecer valores atípicos, un número inusualmente elevado de valores atípicos puede ser una indicación de fraude. Se necesita una investigación adicional para determinar si hay fraude real.

[0072] En un ejemplo, la actividad potencial de fraude por parte de un agente se produce cuando hay tiempos excesivos de retención de llamadas, cuando se compara con un promedio estadístico de una pluralidad de agentes en el centro de contacto. Un agente que se registra teniendo excesivos tiempos de espera, puede estar intentando acceder fraudulentamente a información personal e identificable mientras tiene una llamada activa con un cliente. En este escenario, en un esfuerzo por vencer a una solución antifraude, el agente del centro de contacto puede poner en espera a un cliente de teléfono válido y luego acceder a la información personal e identificable de otro cliente. En otro ejemplo más, la posible actividad fraudulenta de un agente se produce cuando un agente genera una llamada saliente en un momento que es incongruente con las acciones de otros agentes. Es decir, el patrón típico de los agentes en el centro de contacto muestra que los agentes están manejando las llamadas entrantes. Otro patrón puede mostrar que el agente individual durante un período histórico solo ha manejado las llamadas entrantes. El agente del centro de contacto podría tratar de superar una solución antifraude estableciendo una "llamada telefónica" falsa simplemente haciendo una llamada saliente y luego accediendo fraudulentamente a la información personal e identificable del cliente. En otro ejemplo, la actividad fraudulenta potencial de un agente se produce cuando un agente está accediendo a formularios y exhibe características fuera de un promedio estadístico que incluye

acciones de otros agentes o de ese agente en particular. Por ejemplo, la duración del agente dentro de las formas o páginas identificadas de la aplicación se compara con la línea base normal con base en los promedios estadísticos de todos los agentes del centro de contacto para determinar cualquier desviación.

[0073] En la etapa 450 y en respuesta a la actividad potencialmente fraudulenta detectada, se pueden promulgar uno o más protocolos de seguridad para aplicar una o más políticas de seguridad para el agente y/o en la estación de trabajo del agente. La identidad de la estación de trabajo se puede determinar, por ejemplo, a partir de la información utilizada para determinar que se ha producido una posible actividad fraudulenta. Por ejemplo, la información de identificación de un recurso informático sobre el que se produjo la actividad se puede referenciar para determinar la estación de trabajo correspondiente dentro de la cual se realizó la actividad. Tras la identificación, se puede recopilar información adicional relacionada con la estación de trabajo, como determinar el agente que está programado para trabajar en el momento en que se produjo la posible actividad fraudulenta. Las políticas de seguridad pueden incluir la realización de acciones de seguridad tales como: marcar la actividad del agente supervisión como una posible actividad fraudulenta; generar una notificación a un administrador del sistema; generar un informe de actividad fraudulenta potencial para el administrador del sistema; supervisar la actividad adicional del agente; y suspender más actividad del agente en la estación de trabajo. Según una o más implementaciones, la (s) acción (es) de seguridad específica (s) que se seleccionan para realizar se pueden determinar durante o como resultado del análisis para detectar actividad fraudulenta potencial, y se pueden basar en, por ejemplo, la probabilidad o certeza de que ha ocurrido actividad fraudulenta o está a punto de ocurrir, la gravedad o exposición al riesgo de la posible actividad

fraudulenta detectada, el historial de empleo del agente en el centro de contacto, el cliente o la línea de negocio, etc.

[0074] Las Figuras 5 y 6 representan los procesos 500 y 600 realizados por un dispositivo informático cliente y un centro de seguridad, respectivamente, para detectar y prevenir el comportamiento potencialmente fraudulento utilizando un análisis de reglas con base en el contexto. En una o más implementaciones, el proceso 500 representa una parte o la totalidad del proceso 400 descrito anteriormente con respecto a la figura 4 que se realiza en la estación de trabajo del agente durante una llamada supervisada. De forma similar, en una o más implementaciones, el proceso 600 representa una parte o la totalidad del proceso 400 descrito anteriormente que se realiza en un centro de seguridad (e.g., el centro de seguridad 260 de la Figura 2) localizado remotamente desde la estación de trabajo. Las etapas 510-570 describen etapas de ejemplo que comprenden el proceso 500 representado en la figura 5 de acuerdo con las diversas implementaciones descritas en este documento. Las etapas 610-660 describen etapas de ejemplo que comprenden el proceso 600 representado en la figura 6, de acuerdo con las diversas implementaciones descritas en este documento. En una implementación, uno o ambos procesos 500 y 600 se implementan al menos en parte como instrucciones ejecutables por computador almacenadas en uno o más medios legibles por computador y ejecutados en uno o más dispositivos informáticos. De acuerdo con diversas implementaciones, los métodos descritos en los diagramas de flujo 500 y 600 se pueden implementar y/o ejecutar por uno o más componentes de los sistemas 100, 200 y 300 de las FIGS. 1-3, respectivamente.

[0075] En una o más implementaciones, el proceso 500 se puede realizar mediante una aplicación de supervisión u observación que se ejecuta en un

dispositivo informático de la estación de trabajo. La etapa 510 corresponde a la etapa 410 descrita anteriormente, y comienza por la detección de una inicialización de una sesión de llamada en una estación de trabajo (e.g., a través de un teléfono o un canal de comunicación con base en Internet) correspondiente a un agente. De acuerdo con una o más implementaciones, una inicialización de sesión de llamada se puede detectar determinando un cambio en el estado de telefonía de una estación de trabajo o componente de estación de trabajo utilizado por el agente. Una vez que se detecta una sesión de llamada, la supervisión de la actividad de llamada comienza en la etapa 520. Como se discutió anteriormente con respecto a la etapa 410, la supervisión de la actividad de llamada incluye acciones de seguimiento del agente durante la llamada. En la etapa 530, los paquetes de datos que capturan la actividad de voz (e.g., comunicación verbal/conversación entre el agente y el cliente durante la sesión de llamada se generan según uno o más protocolos de transmisión con base en Internet (e.g., SIP/RTP) y se convierten en texto. Como se describió anteriormente, la conversión a texto se puede realizar automáticamente, y en tiempo real (e.g., como una secuencia), en fragmentos de acuerdo con intervalos predefinidos, o retroactivamente desde una grabación de partes o la totalidad de la conversación.

[0076] En la etapa 540, el texto convertido y el registro de la actividad del agente se envían a un motor de comportamiento. En una o más implementaciones, el motor de comportamiento se puede implementar como parte de una aplicación de seguridad/observación correspondiente que se ejecuta en un dispositivo informático de servidor acoplado comunicativamente (e.g., en un centro de seguridad remoto). El texto convertido y el registro de actividad del agente se procesan y analizan en el motor de comportamiento de ejecución remota, y la instanciación local de la aplicación de supervisión se notifica en la etapa 550 siempre que se observen inconsistencias entre el comportamiento esperado que

respondan al texto convertido (con base en un modelo de comportamiento) y las acciones correspondientes en el registro de actividad del agente. Además, el registro de actividad también se puede analizar para detectar cualquier acción que caiga fuera de las normas estadísticas o acciones identificadas (e.g., marcadas) como consistentes con un comportamiento fraudulento o potencialmente fraudulento. Si no se recibe ninguna notificación de comportamiento inconsistente o potencialmente fraudulento del motor de comportamiento, el proceso se repite continuamente desde la etapa 520 para cada intervalo supervisado, período de interés o incidente de actividad de llamada durante el resto de la llamada.

[0077] Por otro lado, cuando se recibe una notificación en la etapa 550, también se pueden recibir acciones de seguridad adicionales en 560 que se han seleccionado como acciones apropiadas para realizar en respuesta al comportamiento inconsistente y/o potencialmente fraudulento detectado. De lo contrario, se puede generar una receta de seguridad (e.g., una lista de acciones de seguridad intensificadas) (e.g., mediante un motor de seguridad ejecutado localmente) en respuesta a la notificación y/o información recibida del motor de comportamiento en respuesta a la actividad detectada de interés. En la etapa 570, la prescripción de seguridad (e.g., lista de acciones de seguridad) recibida desde el motor de comportamiento o generada en la etapa 560 se realiza para limitar aún más la actividad del agente y/o recopilar información adicional para evaluar. De acuerdo con otras implementaciones opcionales, los datos recolectados mientras se supervisa la actividad del agente durante la conversación y la representación textual de la conversación se pueden destilar y agregar al modelo de comportamiento, agregando así un punto de datos adicional para el uso en la evaluación del comportamiento adicional en circunstancias similares.

[0078] En una o más implementaciones, el proceso 600 se puede realizar mediante una aplicación de observación que implementa un motor de comportamiento y se ejecuta en un dispositivo informático de un centro de seguridad. En la etapa 610, se recibe una representación textual (tal como una transcripción) de toda o una parte de una comunicación de voz entre un agente y un cliente durante una llamada supervisada y un registro de la actividad realizada por el agente durante la llamada en un control y/o aplicación de seguridad que se ejecuta en un sistema informático, como un servidor. En una o más implementaciones, la Etapa 610 se puede ejecutar en respuesta a la realización de la etapa 510 del proceso 500 descrito anteriormente en un dispositivo informático de cliente acoplado de forma comunicativa. En implementaciones alternativas, se puede recibir una grabación de todas o parte de la comunicación de voz además de, o en lugar de la representación textual, por lo que la etapa 610 incluye convertir la grabación en una representación textual (e.g., usando técnicas de reconocimiento automático de voz).

[0079] En la etapa 620, el texto recibido (o convertido) y el registro de actividad recibido en la etapa 610 se analiza en un motor de comportamiento comparando las acciones en el registro de actividad a la vista de la comunicación verbal con un modelo de comportamiento. En una o más implementaciones, el modelo de comportamiento puede comprender una pluralidad de reglas de comportamiento que mapean una o más entradas de texto a una o más salidas de acción. Cuando se determina que una acción en el registro de actividad no corresponde a ninguna de las asociaciones de comportamiento (e.g., una acción inconsistente) o, alternativamente, cuando se determina que una acción en el registro de actividad coincide con una regla de comportamiento señalada como potencialmente actividad fraudulenta, la acción se identifica en la etapa 640, marcada en el sistema como potencialmente fraudulenta, y el proceso avanza a la

etapa 650. Cuando no se detecta ninguna incoherencia o actividad potencialmente fraudulenta, el proceso se repite a sí mismo, comenzando en la etapa 610.

[0080] En la etapa 650, se identifican las acciones de seguridad apropiadas a realizar (ya sea por el centro de seguridad, por un administrador del sistema, por un supervisor de agente o por la aplicación de supervisión que se ejecuta en el dispositivo informático cliente de la estación de trabajo del agente). La identificación de las acciones de seguridad apropiadas se puede realizar usando un motor de seguridad y/o aplicando un conjunto de reglas de seguridad predefinidas que mapean ciertos parámetros de la actividad potencialmente fraudulenta para acciones de seguridad. Los parámetros considerados pueden incluir, pero no se limitan a, el tipo o el carácter del acto potencialmente fraudulento, una frecuencia del acto por parte de otros agentes, una frecuencia del acto por parte del agente específico, el cliente específico, el producto o servicio específico, la línea de negocio específica, la atrocidad o severidad del acto, el riesgo para el cliente y/o un cliente, la disponibilidad de seguridad y/o administradores del sistema, la criminalidad del acto y el potencial de disuadir futuras acciones similares en respuesta a una o más acciones de seguridad. Finalmente, las acciones de seguridad determinadas en la etapa 650 se comunican a la estación de trabajo del agente en la etapa 660. Siempre que sea posible, cualquier acción que se pueda realizar o prescribir para realizar en la aplicación de supervisión que se ejecuta en el centro de seguridad también se puede realizar en la etapa 660.

[0081] Por lo tanto, de acuerdo con las implementaciones de la presente invención, se describe el método y sistemas para supervisar la actividad de llamadas que utilizan la voz convertida a texto para detectar y prevenir el fraude

dentro de un centro de contacto.

[0082] La descripción anterior, a los fines de la explicación, se ha descrito con referencia a implementaciones específicas. Sin embargo, las discusiones ilustrativas anteriores no pretenden ser exhaustivas o limitar la invención a las formas precisas divulgadas. Son posibles muchas modificaciones y variaciones a la vista de las enseñanzas anteriores. Las implementaciones se eligieron y describieron con el fin de explicar mejor los principios de la invención y sus aplicaciones prácticas, para permitir así a otros versados en el arte utilizar mejor la invención y diversas implementaciones con diversas modificaciones que se pueden adecuar para el uso particular contemplado.

[0083] Se describen así implementaciones de acuerdo con la invención. Si bien la presente divulgación se ha descrito en implementaciones particulares, se debe apreciar que la invención no se debe considerar como limitada por dichas implementaciones.