1428-P

GESTOR DE MECANISMOS DE VALIDACIÓN DE IDENTIDAD

CAMPO DE LA INVENCIÓN

[0001] La presente invención se relaciona con sistemas de validación de identidad mediante, particularmente con sistemas de validación de identidad que involucra dispositivos de procesamiento y método de ejecución que se basa en al menos dos tipos de marcadores de identidad diferentes.

ANTECEDENTES DE LA INVENCIÓN

[0002] Muchas empresas y / o agencias gubernamentales tienen la necesidad de autenticar las identidades de clientes potenciales y / o clientes para evitar proporcionar beneficios o servicios a los perpetradores de fraude relacionado con la identidad. El Servicio de Impuestos Internos de los Estados Unidos, por ejemplo, informó que más de un millón de declaraciones de impuestos fueron identificadas como fraudulentas para 2011, y un número significativo de estas declaraciones de impuestos involucraron robo de identidad.

[0003] El fraude de identidad continúa presentando desafíos difíciles para las instituciones financieras de hoy, ya que muchos prestamistas, sin saberlo, abren cuentas de crédito basadas en aplicaciones que tienen información de identidad sintética, robada o manipulada. Es probable que los autores de fraudes técnicamente bien informados con sofisticados esquemas de engaño continúen apuntando a instituciones gubernamentales y financieras, particularmente si no existen mecanismos de detección y prevención del fraude. Equilibrar las amenazas de fraude de identidad con un servicio eficiente para clientes legítimos presenta desafíos significativos para las tecnologías de autenticación de identidad.

[0004] La privacidad y la seguridad de los registros personales o de propiedad y el acceso a bases de datos o servicios remotos se han vuelto más dependientes de las crecientes fortalezas de los métodos de autenticación; sin embargo, la fuerza relativa de la autenticación depende en gran medida de la identificación correcta de la identidad de la(s) persona(s) a la(s) a la que se ha asignado el método de autenticación.

[0005] Los métodos y mecanismos conocidos ejecutan programas de decisión que dependen de comparaciones con más bases de datos para determinar los mecanismos de validación necesarios; el nuevo gestor cuenta con un score y un catálogo que define los mecanismos de validación de identidad y no solo de acceso, que no depende de una base de datos ni de un hardware externo para validar la identidad de un cliente y no es un sistema de autenticación que permite o no el ingreso de un usuario a un sistema, ya que el gestor es un validador de identidad que verifica por diversos mecanismos que un usuario si es quien dice ser.

[0006] Los métodos de identificación tradicionales se han basado en el uso de un número de cuenta, dirección de correo electrónico o número de teléfono sin procesos más sólidos para identificar indicadores fraudulentos o de alto riesgo en combinación con la prueba o verificación de la identidad de la(s) persona(s). El nuevo gestor cuenta con un “Rule Manager” que es un motor de reglas que se encarga de validar mediante un proceso automatizado, la gestión de ciertos procesos muy variables y lógicos que se definen mediante reglas de escritura parametrizables en cada transacción con información proporcionada por el usuario y Biometría de Voz que funciona fichas de Leggo que permite integrar métodos de identificación adicional a los que se tienen actualmente.

[0007] El nuevo gestor integra canales para hacer el conteo del riesgo sin dependencia de mecanismos externos que establecen un tope y no diferencian el canal, por ejemplo entre el canal web y el canal de atención virtual como líneas telefónicas, en cambio la propuesta de incorporación de sus mecanismo de biometría y el método del nuevo gestor orquesta simultáneamente los intentos de distintos canales y contabiliza estos intentos disminuyendo la probabilidad de casos

de suplantación de identidad; superando el prejuicio de que cada cada ejecute su propia validación de identidad (por ejemplo Línea – OTP, oficina: OTP u otros independientes); pues la nueva invención orquesta para que en todos los canales que se exija lo mismo para evitar que el usuario acuda a uno u otro según su conveniencia.

[0008] La combinación compacta de métodos sólidos de decisión y verificación de fraude con la inscripción o el uso de los métodos de autenticación ayudará en los desafíos de privacidad y seguridad de la autenticación en persona o remota.

BREVE DESCRIPCIÓN DE LA INVENCIÓN

[0009] En general, en un aspecto, un sistema de autenticación implementado en computadora comprende: recibir, desde un dispositivo utilizado por un usuario, una solicitud de acceso a un recurso alojado por un sistema informático; identificar, por el sistema informático, un nivel de riesgo asociado con el usuario que solicita acceso al recurso; ajustar, por el sistema informático un estándar de autenticación para el acceso al recurso, ajustar en función del nivel de riesgo identificado; determinar los valores de los factores de autenticación utilizados para autenticar el acceso del usuario al recurso; está aplicando ponderaciones a los valores de los factores de autenticación; y determinar, sobre la base de una comparación de los valores ponderados con el estándar de autenticación ajustado, si el usuario está autorizado a acceder al recurso.

[0010] Otras modalidades de este aspecto incluyen los correspondientes sistemas informáticos, aparatos y programas informáticos grabados en uno o más dispositivos de almacenamiento informático, cada uno configurado para realizar las acciones de los métodos. Un sistema de una o más computadoras se puede configurar para realizar operaciones o acciones particulares en virtud de tener software, firmware, hardware o una combinación de ellos instalados en el sistema que en funcionamiento cause o haga que el sistema realice las acciones. Uno o más

programas de computadora pueden configurarse para realizar operaciones o acciones particulares en virtud de incluir instrucciones que, cuando son ejecutadas por un aparato de procesamiento de datos, hacen que el aparato realice las acciones.

[0011] Las realizaciones anteriores y otras pueden incluir opcionalmente una o más de las siguientes características, solas o en combinación. En particular, una realización puede incluir todas las siguientes características en combinación. Las implementaciones pueden incluir una o más de las siguientes características. En algunas implementaciones, el método incluye recibir, desde el dispositivo utilizado por el usuario, información que especifique una selección de los factores de autenticación. En otras implementaciones, el método incluye recibir, desde el dispositivo utilizado por el usuario (teléfono, computadora, huella dactilar, dispositivo táctil) información que especifique los pesos que se aplicarán a los factores de autenticación. En otras implementaciones, el factor de autenticación comprende uno o más de un factor recopilado, un factor en tiempo real y un factor observado.

BREVE DESCRIPCIÓN DE LAS FIGURAS

Figura 1, corresponde a un diagrama de flujo del método de operación del Sistema autenticador de identidad de acuerdo con una modalidad de la presente invención.

Figura 2, corresponde a un diagrama de flujo del método de generación del test de identidad de acuerdo con una modalidad de la presente invención.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

[0012] La presente invención se relaciona con un sistema y un método para la autenticación de múltiples factores y la validación de un usuario. Las implementaciones de la tecnología divulgada se describirán más detalladamente a continuación con referencia a los dibujos adjuntos, en los que se representan varias realizaciones de la tecnología divulgada. Sin embargo, esta tecnología divulgada puede estar incorporada en muchas formas diferentes y no debe interpretarse como limitada a las implementaciones establecidas en este documento; más bien, estas implementaciones se proporcionan para que esta divulgación sea exhaustiva y completa, y transmita completamente el alcance de la tecnología divulgada a aquellos expertos en el arte.

[0013] Ciertas implementaciones de ejemplo de la tecnología divulgada pueden permitir la determinación y gestión efectivas del riesgo de fraude de identidad. Ciertas implementaciones pueden ser utilizadas para detectar actividades sospechosas y/o fraudulentas asociadas con el proceso de establecimiento de una nueva cuenta. Por ejemplo, un sujeto que busca establecer una nueva cuenta (como una cuenta de crédito, cuenta bancaria, cuenta de servicios públicos, etc.) o solicitar un beneficio o servicio (como un reembolso de impuestos, etc.) puede proporcionar un conjunto básico de información de identidad como un nombre, dirección, número de teléfono, número de seguro social, etc. En una implementación de ejemplo, toda o parte del conjunto de información de identidad se puede utilizar para consultar una o más bases de datos públicas y/o privadas para obtener información independiente.

[0014] En ciertas implementaciones de ejemplo, la información independiente puede procesarse para determinar/detectar/calificar los primeros indicadores de riesgo. Los diversos pasos del proceso, como se describió anteriormente, pueden comprender una etapa inicial de un proceso de evaluación de riesgos de varias etapas. En ciertas implementaciones de ejemplo, si los puntajes asociados con los indicadores iniciales de riesgo están por debajo de un cierto umbral (lo que indica bajo riesgo), entonces el sujeto puede pasar a una etapa posterior.

[0015] Como se puede apreciar en la Fig. 1, cada vez que un cliente se contacta sea presencial, telefónica o virtualmente, los distintos medios invocan el servicio del Gestor de Mecanismos de Validación de Identidad con el número de documento del afiliado interesado en realizar una transacción.

[0016] El Gestor de Mecanismos de Validación de Identidad recibe la información de la fuente de contacto y en el segmento Orquestador verifica la información del afiliado y los mecanismos de validación de identidad disponibles. Al pasar al método de completitud valida toda la información existente del afiliado. Supervisando que el individuo no haga parte de la lista restrictiva que le impida hacer transacciones, calificar el nivel de riesgo para segmentarlo ya sea bajo, medio o alto o si se trata de un cliente de tipo preferencial.

[0017] Con la información aunada del afiliado en el Administrador de Reglas el Gestor de Mecanismos de Validación de Identidad regresa el medio necesario para validar la identidad, ya sea a través del lector de huellas dactilar, o le indica al asesor para que a través del teléfono le lea las preguntas reto o valide la identidad por biometría de voz o en caso de ser virtual o en cabina le exponga en la pantalla del equipo los mecanismos que requiere superar para validar la identidad.

[0018] Esta asignación de mecanismos de validación de identidad haciendo usos de hardware son correspondiente a la información existente del cliente y las reglas que componen el método de solución Gestor de Mecanismos de Validación de Identidad.

[0019] Por último, el Gestor de Mecanismos de Validación de Identidad revisa los resultados de cada uno de los mecanismos de validación de identidad que determinen si han sido o no aprobado y le informa al afiliado o al asesor si el interesado puede avanzar con la transacción.

[0020] El Gestor de Mecanismos de Validación de Identidad recibe la solicitud de los afiliados por medios tales como teléfono, teléfono inteligente, computadora, dispositivos móviles o micrófonos y con el número de documento consulta en los servidores la información del afiliado considera la criticidad de la transacción a

realizar en un mecanismo configurado de procesamiento que segmenta el nivel de riesgo del cliente consecuencia del cálculo de un calificación, el análisis de posible cliente restrictivo, diferenciación de cliente preferencial y asignación eficiente de los mecanismos de validación a usar basado en la información anteriormente descrita. Lo que permite asignar mecanismos de validación que evitan la suplantación de identidad, brindando una mejor experiencia de usuario, y con optimización en los costos de validación de identidad.

[0021] El método de validación de identidad de acuerdo con una modalidad de la presente invención comprende los siguientes pasos:

1. Recibir en el Gestor de Mecanismos de Validación de Identidad una solicitud de validación de cada uno de los canales de contacto y los cuales están configurados. La solicitud es recibida por el micro servicio “RestRequest”, el cual valida los datos enviados conforme a estructura, tipos de datos, datos requeridos.
2. Autentica la petición utilizando “Jano”.
3. Registra la información en “Redis” donde se mantendrá esperando la respuesta por el “ID de Request”.
4. Determina si es una solicitud no iniciada, valida si la transacción y el medio de solicitud existen.
5. Se envía la información del “Request” hacia “Completion” y se inicia el proceso de completitud de los datos de la petición.
6. Se llaman los servicios de completitud externos del Gestor de Mecanismos de Validación de Identidad dentro los que se encuentran:
    I. Apolo = Aplicación usada por un asesor para asistir telefónicamente a los clientes y desde el que se invoca la solución.
    II. Reconocer = Consulta bases de datos externos de burós de crédito.
    III. Catálogo de Transacciones, Canales, Mecanismos
    IV. Test de Identidad = Mecanismo de preguntas reto creado con la información del afiliado.
    V. Cartera = Recurso que permite calificar los clientes preferenciales.

VI. Calificación de Riesgo = Basada en información financiera del cliente en la organización.

VII. Azure AD

VIII. Lista restrictiva = Lista compuesta por investigación de Antifraude o información de fuentes externas.

7. Se envían los datos de completitud al micro-servicio de “RuleProcessor” que será el encargado de orquestar las reglas para determinar la lista de mecanismos a aplicar al cliente.
8. Se determinan por los datos que se extrajeron en Completitud, más los datos del propio “Request” inicial, y teniendo en cuenta una serie de reglas que se deben cumplir la lista de mecanismos a aplicar.
9. Se determinan las validaciones que el cliente ha pasado en un tiempo determinado
10. Se realiza las consultas necesarias para completar la información requerida
11. Se envían los datos de completitud y la lista de mecanismos a ser aplicados al micro-servicio “ExecuteMechanism”, el cual busca de la lista de mecanismos a aplicar el primero que no haya sido validado y llama el servicio externo al Gestor de Mecanismos de Validación de Identidad que inicia el mecanismo de validación.
12. Se envían los datos recolectas más la respuesta de la iniciación del primer mecanismo no válido a “SendResponse”. Este almacena toda la petición en la Base de Datos para posteriores peticiones.
13. Inserta los datos en “Redis” donde “RestRequest” está esperando para enviar la respuesta de la petición
14. Se inicia una petición de validación del mecanismo iniciado. Se mantiene leyendo de Redis la respuesta.
15. Se valida que la petición de inicio haya sido ejecuta correctamente y que esté vigente la solicitud
16. Se envía a validar el mecanismo, donde es llamado el servicio de validación correspondiente al mismo mecanismo iniciado

17. Se verifica que la validación haya sido exitosa y se marca el mecanismo como válido en la lista de mecanismos
18. Envía respuesta de mecanismo no válido.

[0022] La prueba de identidad son preguntas retos basadas en la información del afiliado, dicha información es menor a 3 años, por lo que es fácil de recordar y es amena en la experiencia de usuario. Estas preguntas pueden ser respondidas telefónicamente con la asistencia de un asesor o por una computadora o dispositivo móvil en la página web donde se exponen las preguntas.

[0023] Como se puede apreciar en la Figura 2, el proceso para la realización de la prueba de identidad comprende las siguientes etapas:

1. El test de identidad recibe una solicitud proveniente de alguno de los canales de contacto con número de documento.
2. La información inicial recibida se usa para consultar en la tabla de calificación de riesgo, el segmento al que pertenece el afiliado y conocer de esta forma los parámetros que deberán ser usados.
3. Los parámetros consultados según el nivel de riesgo del cliente permiten identificar la cantidad de intentos y fallos por día, mes y año.
4. Posterior al conocimiento de parámetros del afiliado se pasa a buscar la cantidad de ingresos previos realizados, para reconocer si se debe considerar las restricciones establecidas por los parámetros.
5. Con la identidad realizados anteriormente, se indaga en cada una de las sesiones si ha aprobado o reprobado en los intentos.
6. Una vez validado los intentos y resultados se consultan los tres parámetros que concuerdan con el nivel de riesgo del cliente.
7. Los tres parámetros son Acidez, Poder de discriminación y Dificultad. Acidez mide el porcentaje de preguntas reprobadas, Poder de discriminación mide la capacidad de diferenciar que el afiliado sea quien dice ser y Dificultad es definido por el comité de Riesgos y Antifraude, calificando la dificultad de la pregunta de 1 a 5, siendo 1 fácil y 5 difícil.

8. Consultados los parámetros del afiliado, pasa a la tabla de cuestionarios, donde se encuentra enlistado la cantidad de preguntas disponibles para el afiliado y busca el cuestionario que cumpla con los parámetros acordes el nivel de riesgo del cliente.
9. Por último, una vez se ha seleccionado el cuestionario, el programa consulta cual es el porcentaje o calificación mínima para aprobar las preguntas. Cabe aclarar que cada una de las preguntas cuentan con un valor diferente; las preguntas con mayor dificultad tienen mayor valor.
10. El porcentaje de aprobación del cuestionario es parametrizable según el nivel de riesgo de cliente. Es decir que es parametrizable el porcentaje requerido de aprobación.
11. En el caso práctico el afiliado e interesado en realizar la transacción, se le exponen unas preguntas las cuales retorna al mecanismo con las respuestas seleccionados y dependiendo acierto o desaciertos conseguir validar su identidad para continuar con la transacción requerida.

[0024] Las realizaciones se pueden implementar en circuitos electrónicos digitales, o en hardware de computadora, firmware, software o en combinaciones de los mismos. El aparato de la invención puede ser implementado en un producto de programa de computadora tangiblemente incorporado o almacenado en un dispositivo de almacenamiento legible por máquina para su ejecución por un procesador programable; y las acciones del método pueden ser realizadas por un procesador programable que ejecuta un programa de instrucciones para realizar funciones de la invención operando sobre datos de entrada y generando salida.

[0025] La invención puede implementarse ventajosamente en uno o más programas informáticos que son ejecutables en un sistema programable, incluido al menos un procesador programable acoplado para recibir datos e instrucciones de, y para transmitir datos e instrucciones a, un sistema de almacenamiento de datos, al menos un dispositivo de entrada y al menos un dispositivo de salida. Cada programa de computadora se puede implementar en un lenguaje de programación procedimental u orientado a objetos de alto nivel, o en lenguaje ensamblador o de

máquina si se desea; y, en cualquier caso, el lenguaje puede ser un lenguaje compilado o interpretado.

[0026] Los procesadores adecuados incluyen, a modo de ejemplo, microprocesadores de propósito general y especial. Generalmente, un procesador recibirá instrucciones y datos de una memoria de solo lectura y/o una memoria de acceso aleatorio. Generalmente, una computadora incluirá uno o más dispositivos de almacenamiento masivo para almacenar archivos de datos; tales dispositivos incluyen discos magnéticos, como discos duros internos y discos extraíbles; discos magneto-ópticos; y discos ópticos. Los dispositivos de almacenamiento adecuados para incorporar de manera tangible instrucciones y datos de programas de computadora incluyen todas las formas de memoria no volátil, incluidos, a modo de ejemplo, dispositivos de memoria semiconductora, como EPROM, EEPROM y dispositivos de memoria flash; discos magnéticos como discos duros internos y discos extraíbles; discos magneto-ópticos; y discos CD ROM. Cualquiera de los anteriores puede ser complementado o incorporado en ASIC (circuitos integrados específicos de la aplicación).

[0027] Otras modalidades están dentro del alcance y el espíritu de la divulgación de la descripción. Por ejemplo, debido a la naturaleza del software, las funciones descritas anteriormente se pueden implementar utilizando software, hardware, firmware, cableado o combinaciones de cualquiera de estos. Las características que implementan funciones también pueden estar físicamente ubicadas en varias posiciones, incluida la distribución de tal manera que partes de las funciones se implementan en diferentes ubicaciones físicas.