Modelos de análisis y detección

Este modelo crea un perfil único y personalizado para cada usuario, basado en su forma habitual de interactuar con el dispositivo. Al conocer sus patrones normales de uso, el sistema puede detectar cualquier comportamiento inusual que podría indicar que otra persona está accediendo al sistema sin autorización.

Información Recolectada del Usuario

> Comportamiento del Usuario

- **Uso del dispositivo celular:** Forma específica de manipulación
- **Forma de sostener el celular:** Patrones únicos de agarre
- **Uso del teclado:** Velocidad, ritmo y presión de escritura

> Información de Ubicación

- **Ubicación del usuario:** Coordenadas GPS y ubicación aproximada
- **Red utilizada:** Conectividad celular y Wi-Fi
- **Redes Wi-Fi:** Historial y redes cercanas disponibles

> Información del Dispositivo

- **Tamaño de pantalla:** Resolución y configuración
- **Preferencias de tema:** Color, tamaño de fuente, configuraciones visuales
- **Modelo y marca:** Especificaciones técnicas del dispositivo
- **Identificadores únicos:** Metadatos del dispositivo

Análisis Biométrico Comportamental

Enfoque Estricto

- **Uso de pantalla táctil:** Patrones de deslizamiento y presión
- **Uso del mouse:** Movimientos y clics característicos
- **Uso del teclado:** Dinámicas de escritura y atajos

- **Velocidad de escritura:** Ritmo y pausas personalizadas
- **Uso de atajos:** Preferencias de navegación
- **Tamaño de huella dactilar:** Biometría física única
- **Tamaño del dedo:** Área de contacto en pantalla
- **Movimiento del celular:** Patrones de acelerómetro durante uso

Enfoque Amplio

- **Preferencias de tema:** Configuraciones de color y tamaño de fuente
- **Ubicación de uso:** Patrones geográficos habituales
- **Tipo de dispositivo:** Android o iOS, preferencias de ecosistema
- **Navegador utilizado:** Preferencias de software
- **Operador celular:** Proveedor de servicios habitual
- **Aplicaciones instaladas:** Ecosistema de software personal

Modelos Generales de Comportamiento

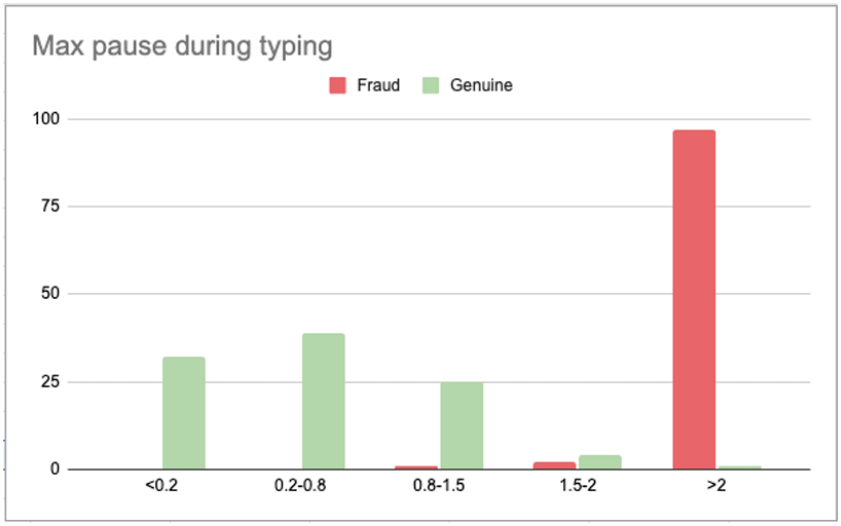
Contamos con modelos entrenados con millones de interacciones reales que ayudan a diferenciar entre comportamientos típicos de usuarios legítimos y aquellos que son característicos de acciones fraudulentas. Esto permite identificar comportamientos sospechosos, incluso si nunca antes se habían visto en el sistema.

Análisis Comparativo de Comportamientos

Patrón de Interacción	Comportamiento Fraudulento	Comportamiento de Usuario Legítimo
Alternar entre aplicaciones	Múltiples veces	Nunca
Ingreso de DNI/ID	Pegar texto / Tipeo alternado	Tipeo manual normal
Navegación en formularios	Uso de teclado	Uso de mouse

Ejemplo: Análisis de Pausas Durante Escritura

Gráfico de Pausas Máximas Durante Escritura del DNI



Interpretación:

- **Usuarios Legítimos:** Pausas distribuidas naturalmente
- **Usuarios Fraudulentos:** 95% presenta pausas extremas (>2 segundos), indicativo de consulta externa

Análisis de Uso de DNI con Pegar/Copiar

Gráfico de Detección de Pegado de DNI

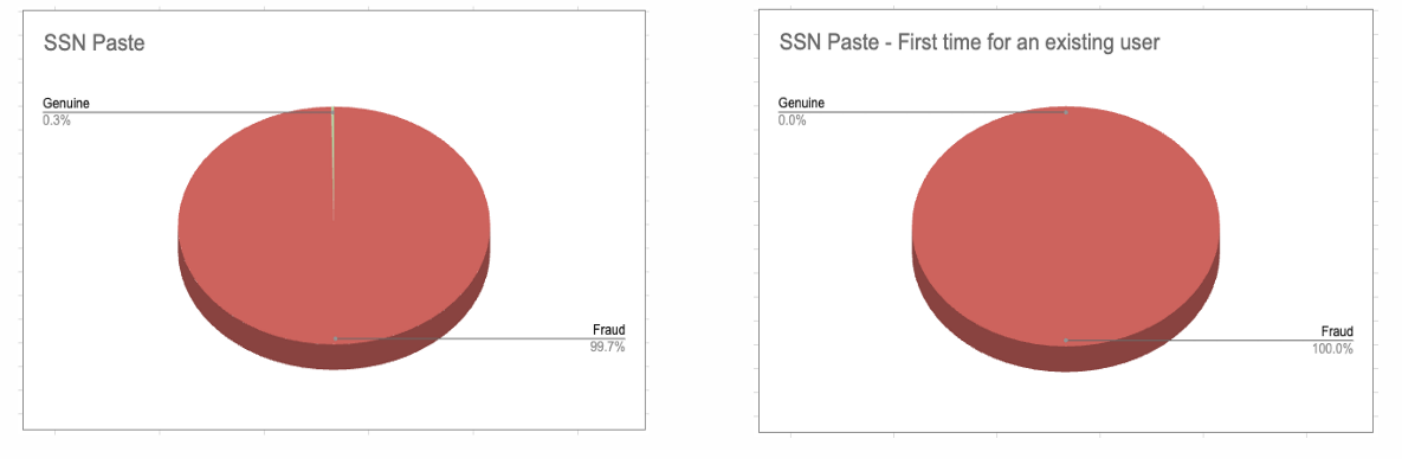


Gráfico Izquierdo - "SSN Paste" (Pegado de SSN):

- **Fraud (Fraude): 99.7%** - Representado en color rojo oscuro
- **Genuine (Genuino): 0.3%** - Representado en color rojo claro/rosado
- Muestra que cuando se detecta pegado de número de identificación, casi la totalidad de los casos (99.7%) son fraudulentos

Gráfico Derecho - "SSN Paste - First time for an existing user" (Pegado de SSN - Primera vez para usuario existente):

- **Fraud (Fraude): 100.0%** - Representado completamente en color rojo
- **Genuine (Genuino): 0.0%** - Sin representación visual
- Muestra que cuando un usuario existente utiliza "pegar" por primera vez, el 100% de los casos son fraudulentos

Modelos de Comportamiento para Defraudadores Identificados

A través del análisis histórico, se han identificado patrones comunes en personas que previamente han intentado realizar fraudes. Estos modelos almacenan y actualizan de forma continua esta información, lo que permite detectar cuando un intento de acceso o transacción se asemeja al comportamiento de estos defraudadores conocidos.

Indicadores Específicos para Estafas de Transferencia

Indicador	Valor	Prevalencia Relativa	Prevalencia en Fraude	Fuerza de Indicación
Transferencia de cuenta limpia	Sí	0.4%	98.7%	67
Múltiples cambios posición teléfono-oído	Sí	1.5%	67.7%	58
Nuevo beneficiario	Sí	0.24%	98.7%	46
Estado de llamada durante login	EN CURSO	2.3%	68.3%	35
Usuario senior	Verdadero	17.2%	93.2%	18

Indicadores de Teléfono Robado

Indicador	Valor	Prevalencia Relativa	Prevalencia en Fraude	Fuerza de Indicación
Nombre Wi-Fi	Azizi 423	0%	64.2%	999
Señal Bluetooth	46542342134	0%	34.7%	999
ID de ubicación	642547854652321	0.05%	34.2%	750
Nuevo ISP	Verdadero	0.4%	88.3%	574
Estado SIM	No SIM detectada	0.03%	64.7%	67
Nueva ubicación	Verdadero	4%	66.7%	65
Nuevo beneficiario	Sí	0.24%	98.7%	46

Modelos Adicionales

Detección de Malware

Permite identificar comportamientos que podrían estar siendo generados por software malicioso instalado en el dispositivo.

Indicadores Técnicos:

- Patrones de automatización perfecta
- Timing inhumano en interacciones
- Secuencias repetitivas de acciones
- Acceso a recursos del sistema sin intervención del usuario

Detección de Bots

Diferencia entre un humano y un sistema automático, lo que es clave para prevenir fraudes automatizados.

Características de Detección:

- Análisis de entropía en movimientos
- Patrones de timing demasiado consistentes
- Ausencia de micro-movimientos naturales
- Secuencias de acciones predecibles

Análisis de Riesgo por Actividad

Evalúa el riesgo de una acción específica (como una transferencia o un inicio de sesión) considerando el contexto en el que se realiza.

Factores Contextuales:

- Horario de la transacción
- Monto involucrado
- Tipo de beneficiario
- Historial de transacciones similares

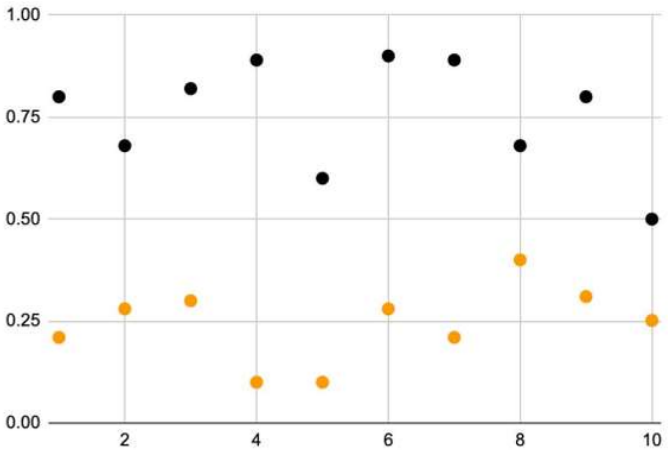
Análisis de Conexiones

Analiza las relaciones entre usuarios, dispositivos y redes para detectar patrones organizados de fraude.

Métricas de Conexión:

- Usuarios compartiendo infraestructura de red
- Dispositivos utilizados por múltiples identidades
- Patrones temporales coordinados
- Ubicaciones físicas compartidas

ANÁLISIS DE DIFERENCIAS EN TAMAÑO DE HUELLA DACTILAR



El gráfico presenta un análisis de dispersión que mide el tamaño de la huella dactilar detectada durante el uso del dispositivo móvil. Esta métrica biométrica permite identificar si el usuario actual corresponde al propietario legítimo del dispositivo.

Características del Gráfico:

- Título: "Finger size"
- Eje X: Secuencia temporal de mediciones (escala de 2 a 10)
- Eje Y: Tamaño relativo de la huella dactilar (escala de 0.00 a 1.00)
- Puntos Negros: Representan sesiones identificadas como fraudulentas
- Puntos Naranjas: Representan sesiones de usuarios legítimos

Interpretación de Patrones

Sesiones de Usuarios Legítimos (Puntos Naranjas)

Rango de valores: 0.00 - 0.40 Características observadas:

- Consistencia en el tamaño de huella a lo largo de toda la sesión
- Variación mínima entre mediciones sucesivas
- Agrupación de valores en rangos específicos que corresponden al usuario registrado
- Estabilidad temporal que refleja el uso natural del dispositivo

Significado: Los usuarios legítimos mantienen un tamaño de huella constante porque utilizan consistentemente los mismos dedos y con la misma presión habitual.

Sesiones Fraudulentas (Puntos Negros)

Rango de valores: 0.50 - 1.00 Características observadas:

- Mayor variabilidad en el tamaño de huella
- Valores significativamente diferentes al perfil biométrico registrado
- Inconsistencia entre mediciones dentro de la misma sesión
- Tendencia hacia valores más altos que sugieren diferencias físicas

Significado: Los defraudadores presentan huellas de tamaño diferente al usuario legítimo, lo que indica que se trata de una persona física distinta utilizando el dispositivo.

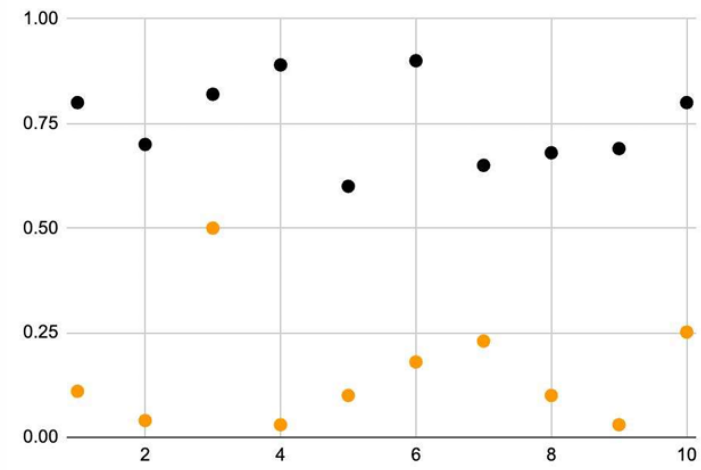
Aplicación Práctica

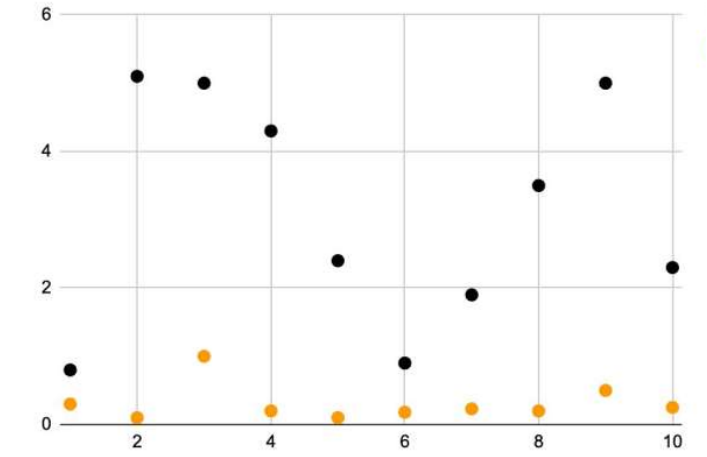
Detección de Uso No Autorizado: El sistema puede identificar inmediatamente cuando una persona diferente al propietario registrado está utilizando el dispositivo, basándose en las diferencias anatómicas naturales entre individuos.

Casos de Detección:

- Dispositivos robados siendo utilizados por terceros
- Acceso no autorizado por familiares o conocidos
- Uso fraudulento después de pérdida del dispositivo
- Suplantación de identidad con dispositivos comprometidos

ANÁLISIS DE MOVIMIENTOS DEL CELULAR





La forma en que las personas sostienen y mueven sus dispositivos móviles durante el uso constituye una firma biométrica única y personal. Estos patrones de movimiento reflejan hábitos motores inconscientes que son extremadamente difíciles de replicar por personas no autorizadas.

Gráfico 1: Acelerómetro Durante Toque de Botón

Este gráfico analiza las lecturas del acelerómetro del dispositivo específicamente en los momentos cuando el usuario realiza toques en botones de la interfaz.

Estructura del Gráfico:

- Medición: Intensidad de movimiento captada por sensores de aceleración
- Eje Temporal: Secuencia de eventos de toque (2 a 10)
- Eje de Intensidad: Magnitud del movimiento (0.00 a 1.00)
- Diferenciación: Puntos negros para fraude, naranjas para usuarios legítimos

Usuarios Legítimos:

- Rango de movimiento: 0.00 - 0.50
- Patrón característico: Movimientos controlados y predecibles
- Estabilidad: Variaciones mínimas entre toques sucesivos
- Explicación: Los usuarios familiares con su dispositivo desarrollan patrones motores automáticos que resultan en movimientos económicos y precisos

Usuarios Fraudulentos:

- Rango de movimiento: 0.50 - 1.00
- Patrón característico: Movimientos erráticos e impredecibles
- Inestabilidad: Gran variación entre diferentes acciones
- Explicación: La falta de familiaridad con el dispositivo genera movimientos compensatorios, nerviosismo y patrones motores atípicos

Gráfico 2: Pausa Máxima de Actividad Durante Sesión

Este análisis mide los intervalos de inactividad más prolongados que ocurren durante una sesión de uso del dispositivo, proporcionando información sobre los procesos cognitivos del usuario.

Estructura del Gráfico:

- Medición: Duración de pausas en segundos
- Eje Temporal: Progresión de la sesión (2 a 10)
- Eje de Duración: Tiempo de pausa máxima (0 a 6 segundos)
- Diferenciación: Puntos negros para fraude, naranjas para usuarios legítimos

Análisis de Comportamientos Cognitivos

Usuarios Legítimos:

- Rango de pausas: 0 - 1.5 segundos
- Características: Flujo continuo y natural de interacción
- Procesamiento: Acceso inmediato a información personal memorizada
- Navegación: Conocimiento intuitivo de la interfaz y procesos

Usuarios Fraudulentos:

- Rango de pausas: 1.5 - 6+ segundos
- Características: Interrupciones prolongadas y frecuentes
- Procesamiento: Necesidad de búsqueda, verificación o consulta externa
- Navegación: Incertidumbre sobre procedimientos y datos requeridos

Casos Especiales y Excepciones

Situaciones Atípicas en Usuarios Legítimos

El sistema está diseñado para reconocer circunstancias excepcionales donde el propietario legítimo puede exhibir patrones anómalos:

Condiciones de Estrés:

- Situaciones de emergencia que alteran comportamiento motor
- Presión temporal que afecta patrones habituales
- Circunstancias de riesgo que generan nerviosismo

Condiciones Físicas:

- Lesiones temporales en manos o dedos
- Efectos de medicación que afectan coordinación
- Fatiga extrema que altera precisión motora

Condiciones Ambientales:

- Uso durante transporte que introduce vibraciones externas
- Condiciones climáticas que afectan manipulación del dispositivo
- Iluminación deficiente que requiere mayor concentración

Detección Inmediata: El análisis de movimientos proporciona evaluación de riesgo en tiempo real desde los primeros segundos de interacción, sin requerir completar transacciones o procesos específicos.

Invisibilidad para el Usuario: La recopilación de datos biométricos de movimiento ocurre de manera transparente durante el uso normal, sin generar fricción adicional en la experiencia del usuario.

Resistencia a Falsificación: Los patrones de movimiento son resultado de años de desarrollo motor personal, haciéndolos extremadamente difíciles de replicar conscientemente por actores maliciosos.

Adaptabilidad Contextual: El sistema aprende y se adapta a las variaciones naturales del usuario legítimo, mejorando su precisión con el tiempo mientras mantiene sensibilidad para detectar uso no autorizado.

Revision #24
Created 28 June 2025 20:36:14 by roger de avila
Updated 30 June 2025 14:13:40 by roger de avila