

## **TITULO DE LA INVENCION:**

### **MÉTODO DE PROTECCIÓN DE TRANSACCIONES PARA TARJETAS DE CRÉDITO O DEBITO**

## **DESCRIPCIÓN**

### **SECTOR TECNOLÓGICO**

El siguiente método ofrece una protección rápida y eficaz contra los hurtos informáticos, es aplicable en tarjetas de crédito y débito; este método se puede aplicar no solo en transacciones de crédito, sino además en todo trámite que requiera una validación por el cliente.

### **ESTADO DE LA TÉCNICA**

Comprar artículos o adquirir servicios por Internet es una alternativa muy utilizada actualmente por la facilidad y comodidad que ofrece, sin embargo, el crecimiento de este tipo de mecanismo transaccional ha traído consigo que personas inescrupulosas utilicen este medio para estafar a usuarios incautos que lo utilizan, resultado de esto es la reticencia de algunos compradores que evitan realizar compras online con sus tarjetas de crédito por miedo a resultar víctimas de fraude.

Los delitos informáticos cada vez toman más relevancia, con el paso de las nuevas tecnologías también se pone en evidencia la vulnerabilidad de las mismas. Según el diario El Espectador.com, del 23 de abril del 2012: “Delitos informáticos causan pérdidas millonarias a bancos y empresas. De acuerdo con el estudio del cibercriminólogo desarrollado por el Registro de Direcciones de Internet para América Latina y Caribe (Lacnic), el phishing o robo de datos personales

significa pérdidas anuales por unos US\$ 93 mil millones de dólares, y afecta a unos 2.500 bancos que operan en la región, en tanto los robos a cuentas de clientes suman otros US\$ 761 millones de dólares. / Asimismo, según cifras del estudio de McAfee Inc. y Science Applications International Corporation, 25% de las organizaciones han sufrido la paralización o atraso de una fusión o adquisición, o bien de la implementación de un nuevo producto o solución, a causa de una filtración de datos o por una amenaza creíble de filtración de datos. / Cabe mencionar que empresas e instituciones de todo el mundo gastaron 338 mil millones de dólares en 2011, para combatir ataques ciber criminales, dos tercios de los cuales fueron delitos de fraude económico, de acuerdo con números ofrecidos durante el Programa de Ciberseguridad y Ciberdelitos de la ONU...”

Esta vulnerabilidad informática es creciente, Kapersky Labs ha cuantificado cuánto dinero puede hacer un pirata informático vendiendo en el mercado negro la información que extrae de internet. De acuerdo a los cálculos realizados por la firma, un pirata informático puede llegar a vender los datos de una tarjeta de crédito por US\$ 10, la imagen de un pasaporte escaneado por US\$ 25 y un pasaporte hecho en base a ese escaneo por US\$ 1.000. Las cifras se multiplican a medida que los ciber criminales infectan no cientos sino miles de computadores.

Si bien el problema es conocido hace muchos años, aun no se materializan soluciones para los usuarios de tarjetas de crédito. A continuación expondré la solución más avanzada que han planteado para estos delitos:

- Que sea un sitio web de confianza
- Que sea un sitio web conocido

### Tecnología SSL

Para que estas dos condiciones se cumplan, debe existir un nivel de seguridad en el sitio que se conoce por las siglas “SSL” (Secure Socket Layer). El SSL es un sistema de seguridad que encripta la información enviada por el usuario, de tal manera que ésta sólo puede ser descifrada por el ordenador que recibe la información y posee la clave secreta para hacerlo. ¿Qué es lo que protege el sistema SSL? Principalmente el número de tarjeta de crédito, para evitar que caiga en manos de personas indebidas y también los datos confidenciales del comprador, para que no se almacenen en ninguna base de datos comercial. La página debe disponer de un Certificado Digital,

Este método sin duda es bueno, nos da garantía de portal del compra, pero la pericia de los hackers va más allá de entrar a un lugar certificado, ellos pueden acceder a las claves así no estemos comprando. El crimen ocurre sin que nos demos cuenta, acceden a la cuenta y desaparecen el monto sin dejar rastro.

A nivel nacional está la patente concedida 11082169 “MÉTODO PARA PROCESAR DE MANERA SEGURA UNA TRANSACCIÓN” la cual aporta un sistema encriptado de claves para protegerse a la hora de hacer una transacción.

La solución que se planteara a continuación ofrece un método que divide una misma cuenta en dos saldos, un saldo de acceso con un tope básico anidado en una base de datos y un saldo de respaldo para eventuales situaciones de mayor gasto, este método junto con los otros anteriormente descritos ofrecen alternativas de seguridad.

### **Descripción detallada del método**

Lo que se plantea es tener dos bases de datos que puedan tener niveles de seguridad, una de ellas con un saldo tope básico, útil para transacciones cotidianas de bienes habituales, ropa, servicios, electrodomésticos, ejemplo de

esto puede ser un tope de \$2000 dólares; y un saldo de respaldo para la misma cuenta alojada en una base de datos de respaldo que pueda contener todo el saldo que pueda y quiera tener el cliente, pero esta base de respaldo no estará disponible para ninguna clase de compra.

Por tanto este método se planeta así:

El usuario desde una terminal (4) un computador o un dispositivo móvil como una laptop, un celular o una Tablet, mediante página web o app accede a su portal de banca, el allí solicita acceder a la base de datos de respaldo (3), donde podrá modificar el saldo tope en la base de datos primaria (2), podrá aumentar o reducir este saldo tope el cual es el que está disponible para compras.

Para modificar este saldo tope, la base de datos de respaldo le exigirá al usuario o sea a la terminal (4) que diligencie la clave de acceso a esta, acá se podrán usar todo tipo métodos de validación de claves ya existentes; si el usuario no logra validar esta clave, la base de datos e respaldo, BDR, (3) cierra el proceso y envía mensaje de alerta al dispositivo del titular de la cuenta.

Si la validación de la clave (5) es positiva la base de respaldo evaluara si existe saldo suficiente en la BDR (3) para modificar el saldo tope en la base de datos principal, BDP (2), si la solicitud de la terminal (4) es reducir el saldo tope de la BDP (2), no existirá ningún impedimento para mandar el saldo de compra al saldo de reserva. Pero si no existe saldo para modificar el saldo tope de la BDP (2) enviara un mensaje al dispositivo (4) indicándole que es inviable la operación porque no hay saldo.

Si la BDR (3) valida la existencia de saldo de reserva, enviara el saldo necesario a la BDP (2) y ajustara el suyo propio, y enviara mensaje de texto del éxito de la operación al dispositivo del titular.

De esta manera el cliente podrá modificar a su antojo la cantidad de dinero disponible para compras, podrá tener un monto pequeño y en caso de robo electrónico no perderá mucho, pero al contar con un saldo de respaldo, podrá contar con una cuenta que bien puede ser de ahorros, corriente o crédito, con un monto alto y cuando necesite operaciones grandes como viajes, vehículos, inmuebles o traspasos podrá modificar dicho saldo tope para ser usado en cualquier portal de compra (6).

**Descripción de las figuras:**

1. Figura1. Muestra la arquitectura de comunicación del sistema entre las bases de datos, la terminal y la tarjeta bancaria (1).
2. Figura 2. Esquema del método.

## FIGURAS

Figura 1.

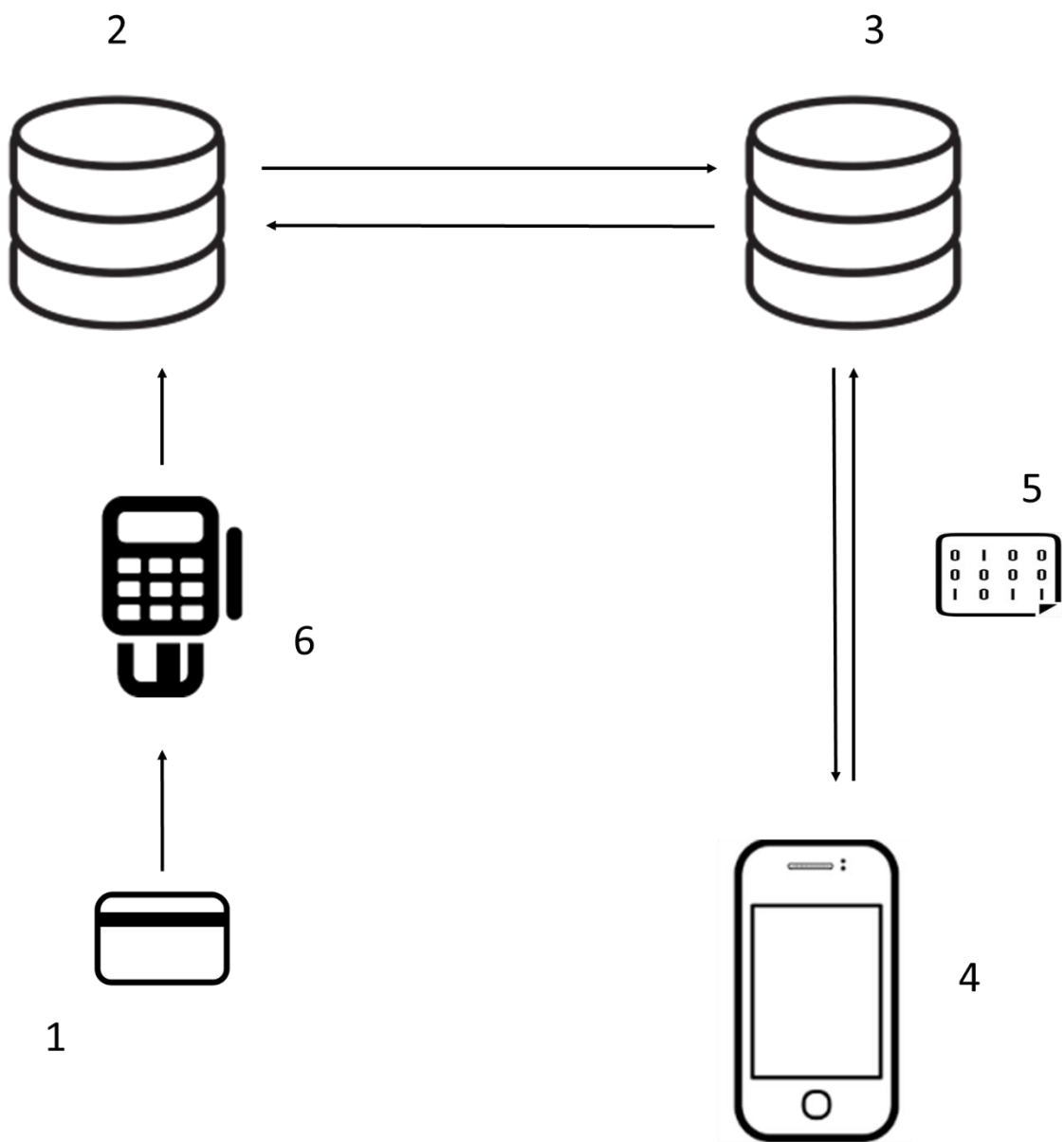


Figura 2.

