INVESTIGACIÓN

Comunicación de Campo Cercano (NFC) para la transferencia segura de información en transacciones P2P

Near Field Communication (NFC) for the secure transfer of information in P2P transactions.

Guillermo de J. Vidal [1*]

Recibido: 03/2023 | Aceptado: 05/2023 | Publicado: 12/2023

Resumen

En la actualidad Cuba se encuentra en un proceso de bancarización de la economía que tiene como objetivo fundamental promover el uso de las pasarelas digitales de pago existentes Transfermóvil y ENZONA para las transacciones comerciales en los sectores privado y estatal, buscando reducir de forma progresiva el uso del dinero en efectivo empleado hasta ahora en los intercambios comerciales. Este proceso trae consigo la incorporación de nuevos usuarios a estas plataformas de comercio electrónico, así como un aumento del volumen de datos y de la información que se gestionan en dichos sistemas, lo que puede dar lugar al incremento del riesgo en la seguridad de la información con la que se efectúan las transacciones, al surgir nuevos actores que puedan aprovecharse del uso masivo de estas tecnologías por parte la población para la incidencia de ciberdelitos. Por tanto, se hace necesario el reforzamiento de la seguridad en estas transacciones, así como el mejoramiento de la eficiencia con que se realizan. Mediante los métodos de investigación análisis-síntesis e histórico-lógico

1* Universidad de las Ciencias Informáticas (UCI). guillermodjvu@gmail.com

en este trabajo se propone el estudio de la tecnología NFC (Comunicación de Campo Cercano) para evaluar sus ventajas respecto a otras tecnologías de intercambio de información para las transacciones comerciales, así como su posible implementación en las aplicaciones móviles de las pasarelas digitales Transfermóvil y ENZONA con el objetivo de añadir una nueva capa de seguridad a las transferencias en los intercambios comerciales y agilizar los procesos en que se llevan a cabo.

Palabras clave: Seguridad; transacciones; comercio; electrónico; eficiencia.

Abstract

Currently, our country is in a state of bankarization of the economy whose main objective is to promote the use of existing digital payment gateways Transfermóvil, ENZONA and Banca Móvil for commercial transactions in the private and state sectors, seeking to reduce progressively the use of cash used up to now in commercial exchanges. This process brings with it the incorporation of new users to these electronic commerce platforms, as well as an increase in the volume of data and information that is managed in said systems, which can lead to an increase in the risk of information security. with which transactions are carried out, when new actors emerge that can take advantage of the massive use of these technologies by the population for the incidence of cybercrimes. Therefore, it is necessary to strengthen security in these transactions, as well as improve the efficiency with which they are carried out. Using the analysis-synthesis and historical-logical research methods, this paper proposes the study of NFC (Near Field Communication) technology to evaluate its advantages over other information exchange technologies for commercial transactions, as well as its possible implementation of the Transfermóvil and ENZONA digital gateways in mobile applications with the aim of adding a new security layer to transfers in commercial exchanges and streamlining the processes in which they are carried out.

Keywords: *Security; transactions; e-commerce; efficiency.*

Introducción

La tecnología NFC ha revolucionado la forma en que las sociedades modernas interactúan con el mundo digital y físico. Desde su introducción, ha demostrado ser una herramienta versátil y poderosa, con aplicaciones en una amplia gama de industrias y sectores. Su importancia radica en su capacidad para facilitar la comunicación inalámbrica y el intercambio de datos a corta distancia, lo que ha impulsado avances significativos en áreas como los pagos móviles, la autenticación de dispositivos y la conectividad. La tecnología NFC ha mejorado la eficiencia, la comodidad y la seguridad en la vida diaria de las personas, y su adopción cada vez mayor la convierte en un estándar a tener en cuenta. Para un país como el nuestro que se encuentra sumido en un proceso de transformación e informatización de la sociedad, y más recientemente en un proceso de bancarización gradual de la economía, se hace conveniente el evaluar qué ventajas y desventajas, así como cuales aportes pudieran traer las tecnologías de este tipo sobre nuestra sociedad adaptadas a nuestro contexto nacional.

Materiales y métodos

Near-field communication (NFC) o comunicación de campo cercano es una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos definida en el estándar ISO/IEC 18092. Haciendo uso de la banda 13.56 MHz permite alcanzar tasas de transferencias por lo general de hasta 424 kbit/s lo que posibilita el intercambio de información instantánea para las cláusulas de autentificación de personas/equipos, así como para la transferencia rápida de pequeñas cantidades de información. Siendo posible trabajar también a velocidades cercanas a 106 kbit/s, 212kbit/s, 424 kbits/s en un rango máximo cercano a los 20 cm, teniendo en cuenta el entorno en el que se realice el intercambio. El protocolo NFCIP-1 que define el modo de comunicación de esta tecnología es capaz de poner a trabajar a las dos partes a una determinada velocidad y luego reajustar el parámetro de la misma en cualquier instante de tiempo. Los equipos con tecnología NFC son capaces de enviar y recibir datos simultáneamente.

Estos funcionan en dos modos:

Modo Activo: Ambos dispositivos con el chip NFC generan un campo electromagnético para leer/escribir la información.

Modo Pasivo: Un solo dispositivo genera el campo electromagnético y el otro aprovecha para leer/escribir la información, el iniciador de la comunicación es el encargado de generar este campo.

Esta serie de características convierten a la comunicación de campo cercano en un candidato perfecto para la realización de transacciones comerciales, por su inmediatez con el trabajo de los datos, y la obtención de un canal rápido y seguro donde estas puedan ser llevadas a cabo.

En la actualidad en nuestro país para la transferencia de información relacionada con las transacciones comerciales en entornos P2P (ej. Pago de servicios en tiendas, cafeterías, restaurantes, Transferencia de dinero de una persona a otra, etc.) son llevados a cabo principalmente de dos maneras:

- Introducción manual de los parámetros asociados a la transferencia.
- Autocompletado mediante el escaneo del código QR vinculados a los parámetros asociados a la transferencia.

Siendo este último el que más facilidades y comodidades brinda al usuario final.

Para el caso de la introducción manual de los parámetros asociados a la transferencia, esta trae consigo una serie de problemáticas asociadas a la seguridad y la eficiencia de las transacciones:

- Errores Humanos: Existe la posibilidad de cometer errores a la hora de escribir el número de la cuenta destinataria, el monto a enviar, u otros datos relevantes dando como resultado el fallo de la transacción o la incorrecta realización de la misma.
- Lentitud: El proceso de teclear manualmente los detalles de la transferencia trae consigo una pérdida de tiempo considerable, que afecta directamente a la eficiencia con que se realiza la operación.
- Incomodidad: Introducir manualmente los parámetros asociados a una transferencia puede llegar a ser incómodo, en particular en teléfonos con defectos en la pantalla o con pantallas pequeñas.
- Riesgo: Al ser los datos introducidos manualmente da un mayor margen a que estos puedan ser interceptados por terceros.

Para el caso del autocompletado mediante el escaneo del código QR vinculado a los parámetros asociados a la transferencia también inciden una serie de factores que atentan contra la seguridad y eficiencia de las transacciones:

- Suplantación de identidad: Al realizar el escaneo del código QR, existe la posibilidad de que ciberdelincuentes puedan suplantar la identidad de una persona o establecimiento con el objetivo de solicitar información confidencial o redirigir al usuario a sitios maliciosos.
- Vulnerabilidad en las aplicaciones de escaneo: Cuando el código QR se realiza mediante aplicaciones de terceros no vinculados con el funcionamiento oficial de una institución bancaria esto puede traer consigo riesgos a la seguridad que podrían ser aprovechadas por los ciberdelincuentes para el robo de información.
- Phishing/Aplicaciones maliciosas: Cuando el código QR se ejecuta tiene la capacidad de ser dirigido a descargar una aplicación maligna que pueda infectar al dispositivo con malware para acceder a información personal o ejecutar procesos dañinos. También puede redirigir a sitios web maliciosos que contengan malware y phishing que podrían convertir al usuario en víctima de robo de información personal o financiera.
- Problemas de parámetros ambientales: Se necesita de una serie de parámetros óptimos para que el sensor de una cámara analiza y ejecute las instrucciones del código QR. Estas vienen dadas por las especificaciones con que el fabricante realiza el hardware, los parámetros ambientales más comunes que afectan el proceso suelen ser el enfoque y la luminosidad, lo que puede traer consigo demoras en la realización de la transacción ante un dispositivo que no es capaz de analizar bien el código.
- Información visible: Ambos métodos tienen como desventaja en común la cantidad de información presente en pantalla a la hora de realizar una tarea, esto trae consigo la existencia de un mayor riesgo de que los datos se vean comprometidos o interceptados por terceros malintencionados al ser posible que estos observen la información ingresada.

Ej. Para el caso particular de una transferencia común entre dos personas (P2P) empleando como pasarela de pago la aplicación Transfermóvil V.1230628 y como entidad el Banco Metropolitano es posible observar durante el proceso, y en texto plano parámetros como:

1 Tarjeta o Cuenta del destinatario, 2 Monto a transferir, 3 Moneda a emplear en el intercambio, 4 Tipo de cuenta desde donde se va a efectuar la transacción, 5 Móvil en el que se confirma la transacción.

Resultados y discusión

Mediante el uso de la tecnología NFC se propone brindar una mayor comodidad, velocidad y seguridad en la transferencia de la información en transacciones P2P. Esto se debe a una serie de características propias de dicho sistema que le permiten superar o complementar a las tecnologías con las que estas transacciones se llevan a cabo actualmente:

Facilidad de uso: El intercambio de información mediante la tecnología NFC se produce al acercar de manera física dos dispositivos compatibles entre sí en un área cercana no mayor a 20 cm lo que autentifica a ambas partes e inicia el proceso. Lo que implica que los usuarios solo necesitan acercar sus teléfonos para iniciar una transacción.

-Rapidez: Al operar con un bajo volumen de datos a una velocidad relativamente alta, esto hace posible el intercambio casi instantáneo de la información, convirtiéndolo en algo particularmente útil en entornos donde se hace necesario el brindar un servicio de pago rápido (MiPymes, tiendas con gran aglomeración de personas, eventos, etc.)

-No repudio: Al ser necesario una interacción física entre los dispositivos para iniciar la transacción el margen de error en la transferencia es mínimo en concepto de quien es el emisor de la transferencia, el receptor de la transferencia, o si esta fue llevada a cabo o no.

-Seguridad: La tecnología NFC admite un conjunto de técnicas que la proveen de una seguridad especialmente robusta como puede ser:

Autentificación de dispositivos: Previa realización de una transacción los dispositivos NFC involucrados se autentifican entre sí para asegurarse de que son dispositivos autorizados y confiables, estos evitan la interferencia de la operación por parte de terceros.

Encriptación de los datos: Los datos transmitidos durante el proceso de transferencia de información entre dispositivos NFC son encriptados para garantizar la protección y confidencialidad de los datos. Para este proceso son admitidos una serie de elementos que combinados entre sí añaden más capas de seguridad al proceso como pueden ser el uso del SE (Elemento Seguro) chip de seguridad de propósito específico dedicado al almacenamiento y procesamiento de las llaves criptográficas y a realizar operaciones de encriptación y desencriptación, protocolo TLS para conexión segura, algoritmos de criptografía simétrica y asimétrica y firma digital. La incorporación de estos elementos individualmente o en su conjunto está definida por la implementación que tengan los sistemas que vayan a hacer uso de ella.

Registro de transacciones: Es posible llevar un registro de las transacciones llevadas a cabo, información de las partes involucradas, tiempo en que se realizó la transacción y que datos fueron transmitidos en ella. Este registro constituye una evidencia de la transacción y puede ser empleado para resolver disputas o reclamaciones de no repudio en el caso de darse.

Expansión: La tecnología NFC se encuentra cada vez más presente en las sociedades modernas siendo usada ampliamente en varios países y por diversos sectores que hacen uso de ella para automatizar sus procesos de pago, además de ser un estándar incluido por los principales fabricantes de dispositivos móviles, lo que ha contribuido a su masiva acogida.

Contexto nacional: Actualmente en nuestro país convergen una serie de factores para los que se hace propicio la incorporación de nuevas tecnologías con el objetivo de informatizar la sociedad. Uno de los sectores que se vería más beneficiados respecto a la informatización de su campo lo constituye el sector de la economía y más concretamente las transacciones comerciales digitales, la introducción de una polí-tica de reordenamiento monetario, y más recientemente la impulsión del desarrollo del comercio electrónico y la bancarización de las operaciones en efectivo han traído como consecuencia la rápida y masiva adopción de estos servicios por parte de la población. Los principales

bancos del país el Banco Metropolitano (BANMET), el Banco Popular de Ahorro (BPA) y el Banco de Crédito y Comercio (BANDEC) ofrecen sus servicios de comercio electrónico a través de dos pasarelas de pago fundamentales: ENZONA y Transfermóvil. Estas pasarelas cuentan cada una con una aplicación para dispositivos móviles a través de las cuales brindan sus servicios. La implementación de la tecnología NFC como ayuda a las transacciones comerciales en dichas pasarelas constituiría una mejora al proceso y a la calidad de las operaciones, buscando complementarse a este ecosistema como una de las alternativas a las vías existentes para la realización de las transferencias que se contemplan en la actualidad (manual y QR) (IOS, 2013; IOS, 2014; Vedat, 2012; Alonso, 2023). Para lograr esto se propone la implementación de una función sobre las apk existentes que permita a los dispositivos que ejecuten las aplicaciones de estas pasarelas hacer uso de la conexión NFC siempre y cuando las condiciones técnicas del terminal lo permitan, con el objetivo de realizar el intercambio de información relacionado a los parámetros de la transacción mediante esta vía.

Conclusiones

La tecnología NFC (Near Field Communication) ha demostrado ser una herramienta de gran importancia en las sociedades modernas. A través de su capacidad para facilitar la comunicación inalámbrica de corto alcance, NFC ha impactado positivamente en diversos aspectos de la vida diaria de las personas en los lugares donde esta se pone en práctica, simplificando los intercambios comerciales, mejorando la experiencia de los usuarios y añadiendo más seguridad a las transacciones. Nuestro país no se encuentra exento del desarrollo y utilización de estas tecnologías por lo que se hace necesario un análisis en profundidad sobre estas y de qué forma pudieran impactar positivamente al desarrollo de la informatización de nuestra sociedad.

Referencias

Fuentes Puebla, T. (2023). Banco Central de Cuba anuncia nuevas medidas de bancarización para reordenar los flujos monetarios. Cubadebate. http://www.cubadebate.cu/noticias/2023/08/02/banco-central-de-cuba- anuncia-nuevas-medidas-de-bancarizacion/

International Organization for Standardization. (2013). ISO 18092:2013 Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1).

International Organization for Standardization. (2014). ISO 13157-1:2014 Information technology- Telecommunications and information exchange between systems - NFC Security-Part 1: NFC-SEC NFCIP-1 security services and protocol.

Vedat Coskun, Kerem Ok and Busra Ozdenizci. (2012). Near Field Communication from theory to practice. John Wiley & Sons Ltd.

Alonso Falcón, R., Figueredo Reinaldo O. y Héctor Rodríguez Y. (2023) Pasarelas de pago e infraestructura tecnológica:Puntos clave para la bancarización. (+ Video) Cubadebate. http://www.cubadebate.cu/noticias/2023/08/22/pasarelas-de-pago-e-infraestructura-tecnologica-puntos- claves-para-la-bancarizacion-video/