ISSN: 1692-7257 - Volumen 2 – Número 42 - 2023

Revista Colombiana de Tecnologías de Avanzada

Recibido: 10 de abril de 2023
Aceptado: 15 de julio de 2023

SISTEMA DE IDENTIFICACIÓN Y CALIFICACIÓN DE ESTUDIANTES BASADOS EN TECNOLOGÍA NFC Y BLOCKCHAIN

STUDENT IDENTIFICATION AND GRADING SYSTEM BASED ON NFC AND BLOCKCHAIN BASED ON NFC AND BLOCKCHAIN TECHNOLOGY

Fabián A. Sánchez-Ruiz[*], **Sebastián Ricardo-Cárdenas**[*], **PhD. Jorge E. Gómez-Gómez**[*]

[*] **Universidad de Córdoba,** Facultad de ingeniería, Ingeniería de Sistemas y Telecomunicaciones, Semillero de investigación Pervasive Computing.
Carrera 6 No. 77- 305 Montería - Córdoba, Colombia
Tel.: 47860920, Fax + (57 604) 7860113
E-mail: {rcuetomorelo, atencioflorez61, jeliecergomez}@unicordoba.edu.co

Cómo citar: Sánchez-Ruiz, F. A., Ricardo-Cárdenas, S., & Gómez-Gómez, J. E. (2023). SISTEMA DE IDENTIFICACIÓN Y CALIFICACIÓN DE ESTUDIANTES BASADOS EN TECNOLOGÍA NFC Y BLOCKCHAIN. REVISTA COLOMBIANA DE TECNOLOGIAS DE AVANZADA (RCTA), 2(42), 23–32. https://doi.org/10.24054/rcta.v2i42.2670

Resumen: La problemática que se trabaja en el documento aborda la precariedad de los sistemas tradicionales de llamado a lista que tienen algunas universidades. Se investigo sobre las características de los NFC y como se pueden utilizar para un sistema de identificación de personal académico para las universidades. Se tuvo en mente utilizar la blockchain para aprovechar la naturaleza descentralizada de esa red para asegurar la confidencialidad de los usuarios del sistema de identificación. Se desarrollo una arquitectura para aplicar estas dos tecnologías en un solo sistema que aproveche lo mejor de los sistemas centralizados y las redes descentralizadas. Esto permitió desarrollar una Dapp que permite la lectura de NFC's, las cuales serán los carnets de los asistentes de la universidad, para acceder a su información, rol e identificación en la universidad.

Palabras clave: NFC, Blockchain, Dapps, Descentralización, Seguridad, Acceso.

Abstract: The problem addressed in the paper deals with the precariousness of the traditional roll-call systems that some universities have. Research was done on the characteristics of NFCs and how they can be used for an academic staff identification system for universities. It was kept in mind to use blockchain to take advantage of the decentralized nature of that network to ensure the confidentiality of the users of the identification system. An architecture was developed to apply these two technologies in a single system that leverages the best of both centralized systems and decentralized networks. This allowed the development of a Dapp that allows the reading of NFC's, which will be the ID cards of the university assistants, to access their information, role and identification in the university.

Keywords: NFC, Blockchain, Dapps, Decentralization, Security, Access.

1. INTRODUCCIÓN

La relación entre la tecnología y la enseñanza secundaria se ha ido estrechando con el avance de las nuevas tecnologías. En esencia, la tecnología ha venido a prestar apoyo a tareas precisas dentro de campos específicos de la educación secundaria. (Maguiño, G. et al, 2020)

En un entorno de numerosas personas como escuelas o universidades, donde el control de acceso y asistencia es una parte primordial de la gestión de la asistencia, surge la necesidad de disponer de un método eficaz y rápido para contar la asistencia en aulas, bibliotecas, laboratorios informáticos y otras instalaciones de interés académico. (A. Rodríguez. et al, 2017)

Por otra parte, los estudiantes poseen elementos de identificación como el DNI o el mismo documento de identidad registrado en su país de origen. (S. C. Gómez, 2017) De este modo, llevan un elemento que hace referencia a su identificación en el entorno en el que viven.

Parte del problema es el robo de identidad, que para demostrar que es la persona, y cuando él / ella estaba en un lugar determinado, se comprueba con su DNI único.

Dentro de esta necesidad, surgen varias alternativas para suplirla, dentro de las cuales se sugiere la implementación de dispositivos NFC dentro de los DNI que identifican a los alumnos, quienes lo presentarán al ingresar a un espacio que amerite comprobar la veracidad de su identidad. (Quishpe, A et al, 2015)

Sin embargo, en este contexto, nos centraremos en cómo la tecnología puede contribuir a la labor del personal educativo en lo que respecta a la asistencia y el control de la información en diversas situaciones dentro de un entorno escolar, ya sea público o privado. Exploraremos los diversos métodos que las instituciones educativas han utilizado a lo largo del tiempo para salvaguardar la privacidad de los estudiantes y su información académica.

2. MOTIVACIONES

Tradicionalmente, el control de asistencia en las universidades se lleva a cabo mediante una lista de firmas que los asistentes a clase rellenan uno a uno. Además, otro método habitual de control de asistencia es aquel en el que el profesor llama a cada asistente para comprobar su asistencia. (D. Majin et al, 2020) Cada uno de estos métodos cumple su objetivo de forma sencilla y sin complicaciones, por lo que la mayoría de las universidades los utilizan por defecto.

Sin embargo, el carácter rudimentario de estos métodos permite grandes lagunas de control y seguridad que ponen en peligro la veracidad y protección de los datos. En los centros de enseñanza superior es muy raro que un profesor reconozca la cara de cada uno de los alumnos de los cursos que imparte, por lo que es muy fácil que cualquiera se haga pasar por un alumno que no ha asistido a clase. Esto puede perturbar la labor del profesor a la hora de calificar equitativamente a todos los alumnos y puede empeorar la experiencia del curso.

Otro sistema muy conocido es aquel en el que los profesores realizan una actividad cada clase (un cuestionario, un taller, etc.). (A. Rodríguez. et al, 2017), y mediante la entrega de la actividad se toma asistencia. Es habitual que el profesor pida a los alumnos que escriban su DNI en la actividad para "asegurar" su identidad. Sin embargo, este método no es lo suficientemente seguro como para evitar que un tercero se infiltre en la clase y suplante la identidad de un alumno.

Las universidades que no disponen de un sofisticado sistema de control de asistencia tienden entonces a someter a sus profesores a estos rudimentarios sistemas de control de asistencia, arruinando la experiencia de los alumnos en sus cursos y dejando posibles pérdidas de información sobre asistencia.

La tecnología NFC es una de las muchas formas posibles de resolver este problema. Ventajas de la tecnología inalámbrica NFC (basada en RFID) (Haselteiner et al, 2006) satisfacen en gran medida las necesidades de las universidades en cuanto a sistemas de control de asistencia. Así, las universidades podrían proporcionar a cada uno de sus asistentes (profesores, estudiantes, administradores) tarjetas de identificación que serán necesarias para la entrada a la institución y para la entrada a determinadas aulas, en función de la función del asistente y de su respectivo horario.

Sin embargo, es bien sabido que la tecnología NFC por sí sola presenta grandes lagunas de seguridad que pueden ser fácilmente aprovechadas para robar información (Mulliner, 2009). Implantar un sistema de identificación NFC sin un sistema subyacente que respalde la información se convierte en un imperativo si se quieren aprovechar las ventajas de conectividad de las tarjetas NFC. En un entorno descentralizado, como el que proporciona la tecnología blockchain, se observa que cada participante en la red posee acceso a la

"información" de sí mismo y de los demás. Esto complica las posibles acciones de atacantes o usuarios con intenciones maliciosas, que podrían dañar la integridad de los demás usuarios y de los datos almacenados.

El uso de tarjetas NFC no mediadas en los sistemas podría presentar vulnerabilidades de seguridad (Mulliner, 2009). Esto se debe a su naturaleza convencional, definida en la norma ISO 14443. La tecnología NFC funciona por inducción en un campo magnético, donde dos antenas en espiral se colocan en sus respectivos campos cercanos. Opera en la banda de frecuencias de 13,56 MHz, lo que significa que no está sujeta a restricciones específicas y no requiere licencia para su uso. (Haselteiner et al, 2006). La falta de protocolos de seguridad en la implementación estándar de tarjetas NFC ofrece la flexibilidad necesaria para desarrollar un sistema de seguridad personalizado, que puede ser necesario o no en función de las implicaciones del proyecto.

3. TRABAJOS DE INVESTIGACIÓN RELACIONADOS

Esta sección explora diferentes estudios, artículos e investigaciones que aplican tecnologías afines para casos de uso similares.

En (S. C. Gómez, 2017) se propone combatir el problema del fraude académico mediante el desarrollo e implantación de un nuevo sistema de control de asistencia "sencillo y seguro", que hace uso de técnicas NFC. Con la implantación de la asistencia obligatoria a clase, la institución donde se desarrolla la investigación ha sufrido incrementos en los niveles de fraude estudiantil, lo que motivó la realización de este trabajo. En este trabajo se hace un análisis exhaustivo de la tecnología RFID, tecnología en la que se basa la NFC, y también de la propia NFC. El trabajo también hace un estudio de las diferentes soluciones de tarjetas de identificación disponibles en el mercado.

El objetivo de (A. Rodríguez. et al, 2017) es desarrollar un sistema que permita conocer en tiempo real el nivel de ocupación de las diferentes bibliotecas de la Universidad Politécnica de Madrid, sede del caso de estudio del artículo. La universidad venía presentando obstáculos derivados de la imposibilidad de conocer con exactitud el número actual de asistentes a sus bibliotecas, debido a un sistema obsoleto que, en época de exámenes, provocaba largas colas. Para solucionar el problema, CARD-CONTROL (A. Rodríguez. et al, 2017), un sistema que mediante la tarjeta universitaria y un dispositivo de lectura FAMOCO (Famoco, 2017) toma asistencia y controla la entrada y salida de los asistentes, para conocer en tiempo real el número de personas que se encuentran en el edificio.

(Guzman, 2020) explora la conveniencia de un sistema descentralizado en el contexto de un sistema de venta de billetes de transporte público. Para realizar tal implementación, el trabajo analiza las diferentes alternativas de tecnologías a utilizar, siendo Ethereum entre ellas, la más viable, mediante contratos inteligentes. La autenticación de los usuarios se realiza mediante tarjetas NFC, aseguradas mediante la base de datos descentralizada. La arquitectura expuesta en este trabajo de grado ha sido una fuente de gran inspiración para nuestra implementación, aunque son casos de uso bastante diferentes.

El objetivo principal de (Muñoz, 2019) es el uso de blockchain en uno de sus mejores campos de aplicación, como son los pagos a terceros con una entidad bancaria de por medio. El apoyo que proporciona a esta investigación radica en el uso de la máquina Ethereum y la suite Truffle para la creación de la app expuesta en el documento.

En (Andrés, 2018) se hace énfasis en un modelo de seguridad telemática sobre NFC, que establece varios niveles de protección con compatibilidad e integración en el desarrollo de aplicaciones de pago móvil. Los componentes que forman parte de este modelo permiten controlar la autenticación con certificados digitales, la unicidad de las transacciones mediante la tokenización y el cifrado de datos mediante algoritmos robustos, lo que, sumado a los estándares de seguridad de aceptación de pagos móviles, determina la eficacia de su aplicación para mitigar las vulnerabilidades que se producen en este entorno.

Un artículo de investigación que proporciona información relevante es (Zheng, 2017), que presenta principalmente las bases y conceptos fundamentales de la tecnología blockchain, mostrando todo lo que la compone, cómo se estructura tanto la cadena como cada bloque que forma parte de ella, y cómo se puede escribir y quién puede escribir dentro de ella. Tendencias que apuntan a la blockchain, de las cuales es primordial en el desarrollo de este artículo, la descentralización de los sistemas.

Gran parte de este artículo se ha inspirado en (Gomez et al., 2023; Gómez et al., 2016; Elamaran et al., 2018; Munoz-Ausecha et al., 2023; Gómez 2017; Gomez2020), un artículo de los mismos autores, que explora temas similares de vinculación de sistemas centralizados y descentralizados,

tecnología NFC y blockchain, pero centrándose en el campo de la medicina y el acceso a la información del historial médico. La arquitectura explorada en (Gómez et al., 2023) ha servido de base para plantar la arquitectura propuesta en este artículo.

4. ARQUITECTURA DEL SISTEMA

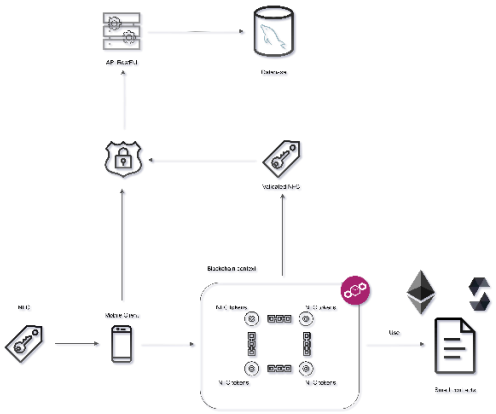

Fig. 1. Arquitectura general del sistema - Fuente: autor

4.1 Cliente

Desde que el uso de dispositivos móviles se hizo frecuente, la facilidad de llevar muchos tipos de sensores en el bolsillo se ha incrementado, por lo tanto, es probable que el dispositivo móvil que llevemos, cuente con un dispositivo lector de tarjetas o gadgets NFC, el cual es utilizable bajo programación especializada en dispositivos portátiles como teléfonos.

Gracias a estas facilidades, abre muchas puertas a los grupos tecnológicos en la creación de herramientas que fomenten el uso programático de estos componentes del dispositivo móvil. Así las cosas, la obtención de información almacenada con la ayuda del lector de sensores NFC, como la lectura de datos, es posible gracias a la contribución de la comunidad de desarrolladores mediante el uso del SDK de Flutter.

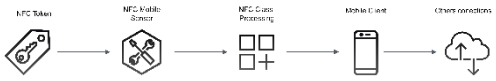

Fig. 2. Cliente móvil - Fuente: autor

(Fig. 1) Arriba se muestra de forma resumida y concisa cómo funciona el cliente móvil.

A partir de un gadget NFC propiedad del alumno, se evalúa su autenticidad dentro de la cadena de bloques, Blockchain; dentro de estos hay información escrita que será procesada por un módulo dedicado a obtener el formato NDEF (Haselteiner et al, 2006) del NFC.

Una vez obtenida la información extraída de la NFC, ésta queda a disposición de la aplicación móvil para ser serializada y/o utilizada por otros servicios a los que la aplicación esté conectada.

4.2 Blockchain en entornos descentralizados

Las redes descentralizadas, por su propia definición, son públicas por naturaleza. En el contexto de blockchain, toda la información almacenada en esta tecnología es accesible a cualquier individuo que forme parte de la red, como se ha destacado anteriormente (IBM, 2022). Esta característica de transparencia se aplica igualmente a plataformas como Ethereum, que se selecciona como entorno principal para la ejecución de contratos inteligentes en nuestro sistema de gestión educativa.

Sin embargo, es importante tener en cuenta que sería imprudente y potencialmente contraproducente intentar alojar información educativa sensible, como expedientes académicos y datos de los estudiantes, en una red descentralizada. La necesidad de preservar la privacidad y la seguridad de estos registros es primordial, y aunque la tecnología blockchain ofrece numerosas ventajas, no es la más adecuada para la gestión de datos educativos sensibles. En su lugar, deben explorarse alternativas que equilibren la innovación tecnológica con una protección adecuada de los datos críticos en el ámbito de la educación secundaria y universitaria.

No obstante, las características inherentemente públicas de estas redes las convierten en candidatas ideales para la implantación de un sistema de autenticación avanzado. La transparencia y accesibilidad inherentes a las redes descentralizadas, como blockchain, proporcionan un entorno propicio para garantizar la autenticidad e integridad de la información en un sistema de gestión educativa. Esto significa que, en lugar de ver estas propiedades como limitaciones, podemos aprovecharlas como ventajas clave en el diseño de un sistema de autenticación robusto.

En el sistema en desarrollo, cada usuario autenticado con el rol de "estudiante" tendrá la capacidad de registrar y eliminar tarjetas NFC, que servirán como claves de acceso a su información confidencial en el módulo centralizado. Cada entrada en la cadena de bloques representará una etiqueta NFC, y cuando un usuario registre una etiqueta NFC como propia, esta información se

registrará en la cadena de bloques mediante contratos inteligentes. Esto, a su vez, permitirá que todas las demás blockchains registradas previamente tengan conocimiento de la nueva entrada. Una representación visual de este proceso se presenta en la Fig. 3

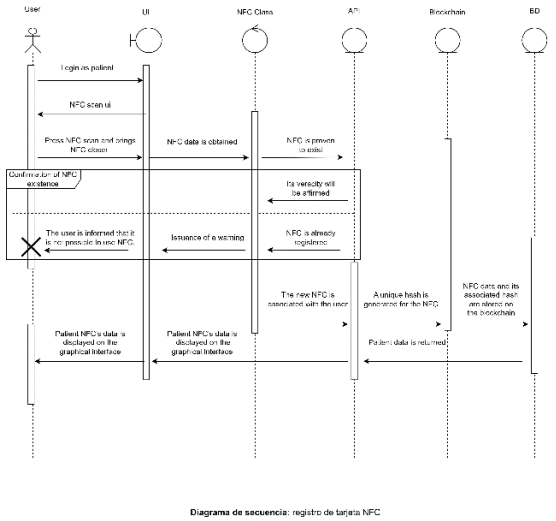

Fig. 3. Descentralizado - Fuente: autor

Al llevar a cabo el proceso de registro de una nueva tarjeta NFC, es importante tener en cuenta que el contrato inteligente no almacena ninguna información sensible que vincule ese bloque en la blockchain con el usuario propietario de la tarjeta NFC. Esto garantiza que la información personal y sensible de los estudiantes o profesores permanezca segura y confidencial en todo momento.

En lugar de almacenar datos personales en el contrato inteligente, cada vez que se crea un nuevo bloque en la blockchain, se genera un hash único que sirve como identificador único para ese bloque dentro de la red. Este hash se almacena en la carga útil NFC, que es la información contenida en la tarjeta NFC. Como último paso del flujo de registro, la carga útil NFC, junto con el hash generado y el UID (identificador único) NFC, se envía al sistema. Este proceso garantiza que la información almacenada en la blockchain es anónima y que la única entidad que puede asociar la NFC con su propietario es el sistema centralizado, que tiene acceso a los datos relacionados con el UID de la NFC.

El flujo de datos durante el registro de una tarjeta NFC puede visualizarse con más detalle en la Figura 3. Este enfoque de diseño protege la privacidad de los usuarios al tiempo que permite una autenticación segura y eficiente en el contexto educativo.

4.3 Entorno centralizado

Se sabe entonces que la red descentralizada tiene un carácter público, por lo tanto, para cumplir con los estándares del enfoque de seguridad propuesto, se propone incorporar un componente centralizado a la arquitectura. Este módulo será el encargado de almacenar la información confidencial de cada usuario de la red pública, como documento de identificación, curso de estudio, horario, etc. Para lograr lo anterior, el módulo se implementará como un servicio web, siguiendo los estándares RESTful API (Lokesh, 2018), para que pueda ser consumido eficazmente por cualquier otro producto o servicio desarrollado en torno al sistema, desacoplando el servicio del cliente.

El servicio web expondrá los puntos de acceso necesarios para almacenar, leer, actualizar y eliminar asistentes de red, incluyendo toda la información asociada a los mismos. Además, también expondrá puntos de acceso para la lectura y registro de nuevas tarjetas, lo que implicará llamadas al módulo descentralizado, aspectos que se tratarán con más detalle más adelante.

El sistema centralizado gestionará una sección de autenticación y autorización basada en el estándar JSON Web Tokens (JWT) (Jones, 2015), que reforzará la seguridad global del módulo, protegiendo los puntos de acceso sólo a aquellos terminales que posean la clave secreta.

Restringir el acceso al módulo a sólo aquellos terminales que posean la clave secreta garantizará que sólo se pueda acceder al módulo descentralizado a través de la sección de autenticación del módulo centralizado, que, mediante un registro e inicio de sesión en el punto de acceso, proporcionará un token de acceso. Este token de acceso es crucial para la seguridad del sistema, ya que desbloquea todos los puntos de acceso del módulo centralizado a los terminales, y también proporciona una forma segura de controlar qué terminal está accediendo a estos servicios.

Además, cada uno de los puntos de acceso estará protegido por un sistema de roles. Dependiendo del tipo de usuario (ADMIN, ESTUDIANTE, PROFESOR) que se encuentre en el Token Web JSON (JWT) proporcionado, el terminal podrá acceder a determinados edificios y/o salas. Los estudiantes tendrán acceso exclusivamente a los puntos de acceso relacionados con el registro de la tarjeta NFC, la modificación de su información personal, además de los edificios de estudio relacionados con sus horarios. Los profesores podrán modificar la información personal de cualquier alumno, pero deberán utilizar el punto de

acceso del lector NFC para autenticar primero al alumno. Los administradores tendrán acceso a todos los puntos de acceso, incluidos los relacionados con la modificación de usuarios y roles. Esta estrategia de roles garantiza un control de acceso preciso y seguro en el sistema, asegurando que cada usuario tenga la capacidad adecuada en función de su rol dentro de la Plataforma.

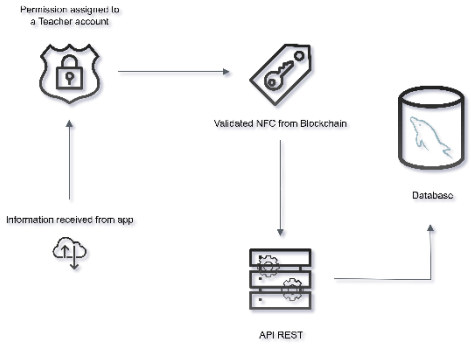

Fig. 4. Entorno centralizado - Fuente: autor

El estándar JWT (JSON Web Token) hace uso de un algoritmo de encriptación HS256 (Jones, 2015). Se sabe que este algoritmo de cifrado tiene un proceso de firma en el que hace uso de una clave secreta que, para mayor seguridad, puede generarse aleatoriamente en el momento de empaquetar la aplicación para su distribución. El uso de dicha clave secreta ofrece la libertad de, en caso de fuga, simplemente reiniciar la aplicación, junto con una nueva clave, y cualquier token generado previamente quedaría completamente desactivado.

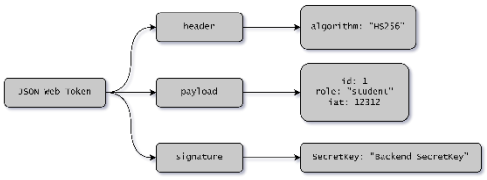

Fig.5 Estructura de la firma JWT - Fuente: autor

La figura 5 muestra un esquema de la arquitectura de un JWT, que se compone de: Cabecera, que describe la estructura y el cifrado del token; Firma, que es la clave secreta mencionada anteriormente; y Carga útil, que contiene el id del usuario, su rol y la fecha de caducidad del token. En el sistema propuesto, el identificador no forma parte de la información personal del usuario, sino que es un código generado aleatoriamente para identificar a cada usuario en la base de datos centralizada. Por ello, este identificador no tiene ningún valor confidencial fuera del sistema, de modo que si se expusiera la carga útil del token, no se expondría información personal.

4.4 Posibles ataques

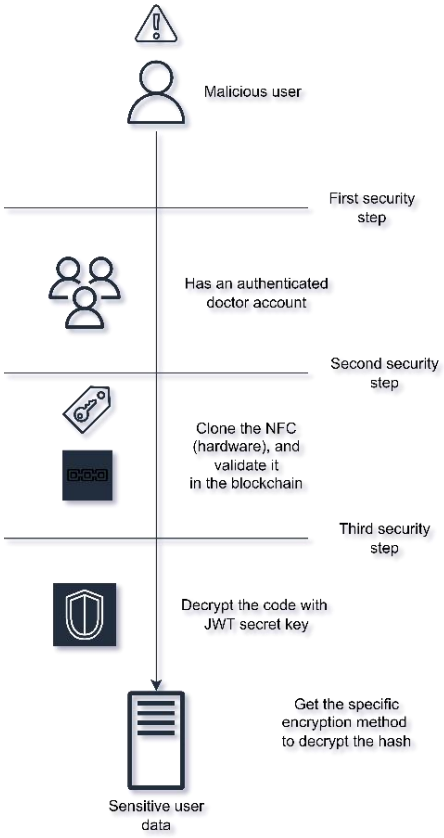

Fig.6 Barreras de seguridad - Fuente: autor

Es bien sabido que ningún sistema es seguro, y que la mayoría de los ataques se deben a filtraciones de fallos de seguridad o a ingeniería social, como el phishing. Hay muchos mecanismos de seguridad que los desarrolladores pueden utilizar para evitar comprometer los datos, sin embargo, ningún sistema es suficientemente inmune a la ingeniería social.

Teniendo en cuenta lo anterior, el sistema de seguridad propuesto consta de tres muros de seguridad a través de los cuales una entidad maliciosa tendrá que pasar para obtener datos comprometedores. Véase la figura 6. Para demostrar el sistema de seguridad propuesto, se considera la siguiente situación hipotética:

Un atacante quiere obtener la información sensible de un paciente concreto, esta información se encuentra en la base de datos. El atacante sabe que el sistema de identificación funciona con tarjetas

NFC y descubre que éstas pueden ser fácilmente clonadas, por lo que el atacante decide clonar la tarjeta NFC de su víctima.

Para que una tarjeta NFC clonada sea útil en el sistema propuesto, es necesario que el método de clonación utilizado también clone el UID de la tarjeta y, además, que la tarjeta en la que se clona la información sea del mismo tipo que acepta nuestro sistema. Suponiendo que el método de clonación del atacante cumpla lo anterior, el atacante ya habría traspasado uno de los muros de seguridad del sistema, véase la figura 6.

En este punto, el atacante tiene una NFC con la carga útil y el UID exactos de la NFC de un paciente, datos que aún no exponen información sensible del paciente. Sin embargo, el atacante aún no ha podido pasar el primer muro de seguridad del sistema, que requiere una cuenta de usuario de la aplicación con el rol de PROFESOR. Como se mencionó en la sección sobre el entorno centralizado, las cuentas de usuario creadas en el sistema siempre tienen por defecto el rol de ESTUDIANTES, por lo que conseguir una cuenta de PROFESOR sólo sería posible mediante ingeniería social.

5. ARQUITECTURA DEL SISTEMA

5.1 Lecturas en la Blockchain

Para analizar la velocidad de lectura de los bloques almacenados en la blockchain, se diseñarán escenarios específicos. Dado que la blockchain se basa en una estructura de datos conocida como "lista enlazada" (NIST, 2023), evaluaremos las tasas de lectura dentro de esta estructura.

5.2 Blockchain local

En este apartado se realizará un análisis de una blockchain con diferentes tamaños, alojada en la misma máquina y llamando a todos sus bloques, que proporcionará información sobre los tiempos de llamada y presentación.

Capturando los datos dentro de la aplicación y tabulándolos, se obtienen los siguientes datos:

Se realizó un análisis de lectura en tres momentos diferentes, todos con el mismo número de bloques, y se calculó una media para establecer un tiempo estándar. Con estos datos, se construyó el siguiente gráfico:

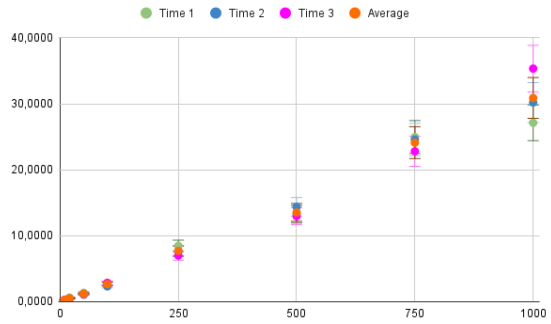

Fig.7. Tiempo estimado de lectura - Fuente: autor

A partir de este diagrama de dispersión, que ofrece un pequeño resumen de los tiempos para cada cantidad de datos, es posible calcular las medidas de tendencia central y las medidas de dispersión.

A continuación, procedemos a calcular la media del número de datos y el tiempo medio:

Tabla 1: Medias aritméticas - Fuente: autores

$\frac{1}{N}\sum_{i=1}^{N} Amount$	335
$\frac{1}{N}\sum_{i=1}^{N} Time$	10,13

Se realiza un cálculo de la desviación típica para, a continuación, calcular el coeficiente de correlación (JMP, 2021) que indicará la relación entre las variables para demostrar su dependencia.

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N}(Amount-\overline{Amount})^2}{N}} = 351{,}8167136 \quad (1)$$

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N}(Time-\overline{Time})^2}{N}} = 11{,}03980112 \quad (2)$$

Una vez que tenemos la desviación típica y las medias aritméticas, procedemos a calcular la covarianza.

Es un número que muestra la dirección de la correlación entre un par de variables, es decir, nos permite saber cómo se comporta una variable en función del comportamiento de otra variable. (Marta, 2020)

De este modo:

$$S_{xy} = \frac{1}{n}\sum_{i=0}^{n} x_i \cdot y_i - \overline{x}\overline{y}$$

Por lo tanto:

$$S_{xy} = \frac{1}{n}\sum_{i=0}^{n} amount \cdot time - \overline{amount} \cdot \overline{time}$$

Se obtiene:

$$S_{xy} = 3874{,}498646$$

El coeficiente de correlación se calcula a partir de este valor.

Este término es la medida específica que cuantifica la fuerza de la relación lineal entre dos variables en un análisis de correlación (NIST, 2023). En este contexto, se utilizará para examinar la relación entre el tiempo y la cantidad de datos y para determinar la fuerza y la dirección de esta relación. El coeficiente de correlación proporcionará información sobre la magnitud de la dependencia lineal entre estas dos variables.

Se calcula del siguiente modo:

$$r = \frac{S_{xy}}{\sigma x \cdot \sigma y} = 0{,}9975571738$$

De este resultado se deduce lo siguiente:

"Si el coeficiente de correlación lineal toma valores cercanos a 1 la correlación es fuerte y directa, y será tanto más fuerte cuanto más se aproxime a 1." (JMP, 2021) ("If the linear correlation coefficient takes values close to 1, the correlation is strong and direct, and the closer it is to 1, the stronger it is")

Sabiendo que tienes una correlación realmente fuerte y directa, puedes ejecutar una regresión lineal para determinar o tratar de predecir que, a una cierta cantidad de datos, cuánto tiempo se tardará en realizar.

Una vez que se tienen todos los datos, sólo es cuestión de obtener todas las incógnitas de una ecuación lineal.

$$y = m \cdot x + b$$

Por lo tanto, hay que encontrar a y b, definidos como sigue:

$$m = \frac{r \cdot \sigma \cdot time}{\sigma Amount} = 0{,}0313$$

$$a = \overline{Time} - b \cdot \overline{Amount} = -0{,}36$$

De este modo:

$$y = 0{,}0313 \cdot x - 0{,}36$$

Cuando se trazan junto con los puntos obtenidos:

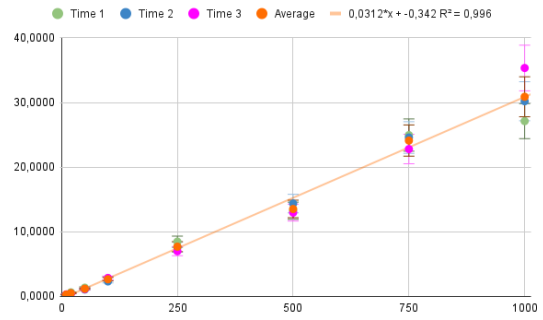

Fig.8. Tiempos de lectura estimados con regresión - Fuente: autor

Al concluir y analizar todos estos resultados, se extrajeron varias conclusiones.

1. Se muestra una alta relación lineal entre el número de bloques dentro de la blockchain con el tiempo que se tarda en leer datos de la blockchain.
2. A partir de una alta cantidad de datos, como se observa después de los 1000 datos, otras variables son las que hacen participación en el resultado de lo que es el tiempo de lectura.

6. CONCLUSIONES

A lo largo de la investigación se ha revisado la literatura en busca de opciones para la creación de un sistema de seguridad para tarjetas NFC basado en

el blockchain. Se ha llegado a la conclusión de que aprovechando la naturaleza de los sistemas descentralizados es posible sacar provecho de la aplicación de este sistema, ya que todos los usuarios, presentados por blockchains en la cadena de bloques, tienen conocimiento de la existencia de los demás usuarios en la red. Esto convierte a todos los clientes en propietarios de la información de todo el sistema en un momento dado, dejando de lado la centralización de los datos como única fuente de verdad.

Dentro de este orden de ideas, proponemos la creación de una DAPP (aplicación descentralizada), implementando tecnologías DLT (Distributed Ledger Technologies), como Blockchain y Ethereum, que exponen APIs de desarrollo a disposición de los desarrolladores para la creación de contratos inteligentes que interactúan con su propia red viviendo en la blockchain. Para ello se ha seleccionado la suite de desarrollo Ganache, que ofrece todo un conjunto de herramientas para el desarrollo de DAPPs. Esta Dapp se encargará de la parte de seguridad del NFC dentro de las tarjetas, de forma que cada tarjeta tendrá un código único que representa un bloque de la blockchain.

Además, la Dapp también hace uso del SDK Flutter para reconocer y extraer información útil de las tarjetas NFC a través de su hardware de control NFC dedicado. La app actuará como lector NFC y será utilizada por profesores y supervisores para pasar lista e identificar a sus alumnos. Esta aplicación se comunica a su vez con el módulo centralizado, un servidor conectado a una base de datos relacional que almacena toda la información sensible de los asistentes al sistema. Para añadir un nuevo asistente al sistema, la aplicación mina la blockchain para obtener un nuevo identificador único que identifique al asistente en el sistema y, a continuación, se comunica con el módulo centralizado para intentar asignar la tarjeta leída al nuevo bloque de la blockchain. En consecuencia, para que un asistente se registre en el sistema, la blockchain primero tiene que admitir al nuevo usuario para que la NFC pueda escribirse con la información, evitando así el acceso a información sensible en caso de NFC clonadas.

La combinación de sistemas centralizados y descentralizados es, por tanto, posible, y proporciona un nivel de seguridad único que solo puede lograrse combinando estos dos sistemas. La verificación de la veracidad de las NFC en la blockchain garantiza la autenticidad de los datos, gracias a la descentralización. Por otro lado, el módulo centralizado actúa como medio de almacenamiento de datos sensibles, accesibles únicamente a través de las claves previamente validadas en la blockchain. Juntos, la combinación de estos dos sistemas ofrece seguridad y robustez en el sistema de identificación y validación de datos.

Agradecimiento

Gracias a la Universidad de Córdoba por financiar este proyecto de investigación según la convocatoria interna con código de proyecto FI-05-19. También agradecemos al grupo de investigación SOCRATES del programa de Ingeniería de Sistemas y Telecomunicaciones por apoyar el desarrollo de este proyecto.

REFERENCIAS

Maguiño, G., Amaru, M., Vela, R., Lidia, S., Lozano, R., Alberto, R. Fernando, G. (2020) “Tecnología en el proceso educativo: nuevos escenarios”.

A. Rodríguez-González et al. (2017) “Uso de tarjeta universitaria y tecnología móvil para el control de acceso a instalaciones universitarias y su posterior análisis en términos de rendimiento académico y control de asistencia en clase”.

S. C. Gómez. (2017) “Control de asistencia mediante técnicas NFC”.

Quishpe A. Jorge & Villarreal, Germania & Camacho L. (2015). “NFC: La nueva tecnología para la educación universitaria”.

D. A. G. Majin and O. D. G. Tez (2020) DISEÑO Y DESARROLLO DE UNA APLICACIÓN MÓVIL EN ANDROID PARA EL CONTROL DE ASISTENCIA DE ESTUDIANTES DEL INSTITUTO TECNOLÓGICO DEL PUTUMAYO.

Haselsteiner, E., & Breitfuß, K. (2006) “Near field communication (NFC)”. pág 2.

Mulliner, C. (2009). “Vulnerability analysis and attacks on NFC-enabled mobile phones. 2009 International Conference on Availability, Reliability and Security”.

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2010). Guía sobre seguridad y privacidad de la tecnología RFID. pág 31.

Famoco (2017) “Android terminal equipment and payment solutions”.

Guzmán, E. A. (2020). “Sistema autónomo de cobro de pasajes para el transporte público con Blockchain”.

Muñoz Tapia J. (2019) “Desarrollo de una Dapp basada en Ethereum y React”.

Andrés C. Cristhian C. María U. Gonzalo S. Ciro RADICELLI. Diego B. (2018) “Modelo de seguridad para garantizar la integridad de pagos móviles sobre near field communication (NFC)”.

Zheng, Z. Xie, S. Dai, H. Chen X. Wang, H. (2017). “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”.

J. E. Gómez Gómez, S. Ricardo Cárdenas, y F. Sánchez Ruiz, (2023) “Sistema de identificación de pacientes basado en tecnología NFC y Blockchain”, Investigación e Innovación en Ingenierías, vol. 11, n.º 2, pp. 1–15.

IBM (2022) “¿Qué es la tecnología de blockchain?”

Lokesh G. (2018) “¿What is REST? - REST API Tutorial”.

Jones, M. B., Bradley, J., & Sakimura, N. (2015). “RFC 7519: JSON Web Token (JWT). IETF Datatracker”.

NIST. (2023) “Linked list”.

JMP. (2021) “Coeficiente de correlación”.

Marta -superprof. (2020) “Covarianza de una muestra”.

Gómez, J., Oviedo, B., & Zhuma, E. (2016). Patient monitoring system based on internet of things. Procedia Computer Science, 83, 90-97.

Elamaran, V., Arunkumar, N., Babu, G. V., Balaji, V. S., Gomez, J., Figueroa, C., & Ramirez-González, G. (2018). Exploring DNS, HTTP, and ICMP response time computations on brain signal/image databases using a packet sniffer tool. IEEE Access, 6, 59672-59678.

Munoz-Ausecha, C., Gómez, J. E. G., Ruiz-Rosero, J., & Ramirez-Gonzalez, G. (2023). Asset Ownership Transfer and Inventory Using RFID UHF TAGS and Ethereum Blockchain NFTs. Electronics, 12(6), 1497.

Gómez, J. E. (2017). El internet de las cosas oportunidades y desafíos. Ingeniería E Innovación, 5(1).

Gomez, J. G. (2020). Principales desafíos y oportunidades de los sistemas de Internet de las cosas médicas-IoMT. Ingeniería e Innovación, 8(22).