REVISTA ESPAÑOLA DE COMUNICACIÓN EN SALUD
2024, Suplemento 1, S24-S53
https://doi.org/10.20318/recs.2024.7687

Rastreo digital de contactos: datos de geolocalización a gran escala como alternativa al fracaso de las aplicaciones basadas en Bluetooth

Digital Contact Tracing: Large-scale Geolocation Data as an Alternative to Bluetooth-based Apps' Failure

Francisco Caravaca[a],José González-Cabañas[b], Roberto Boris Martínez[a], Ángel Cuevas[a,b], Rubén Cuevas[a,b], Martin Maier[c], María Calderón Pastor[a,e], Jorge Pleite Guerra[d]

[a] Departamento de Ingeniería Telemática, Universidad Carlos III de Madrid, España
[b] Instituto UC3M-Santander de Big Data, España
[c] Institut National de la Recherche Scientifique, España
[d] Departamento de Tecnología Electrónica, Universidad Carlos III de Madrid, España
[e] Departamento de Ingeniería de Sistemas Telemáticos, Universidad Politécnica de Madrid, España

Resumen

Introducción: Las aplicaciones móviles de rastreo de contactos desplegadas actualmente han fracasado como solución eficaz en el contexto de la pandemia COVID-19. Ninguna de ellas ha conseguido atraer al número de usuarios activos necesario para lograr una operación eficiente. **Objetivo:** ampliar la definición de los sistemas digitales de rastreo de contactos. **Metodología:** Se ha propuesto un protocolo para el rastreo de contactos utilizando información de proveedores de localización. Dicho protocolo ha sido implementado, y se ha medido su rendimiento. **Resultados:** la solución ha sido implementada, la cual además de ser eficiente garantiza la privacidad de los usuarios **Conclusión:** La solución presentada permitiría el rastreo de contactos, y con suficiente eficiencia para que escale correctamente.

Palabras clave: COVID-19; rastreo de contactos; Facebook; Google; geolocalización; privacidad.

Abstract

Introduction: Currently deployed mobile contact-tracking applications have failed as an effective solution in the context of the COVID-19 pandemic. None of them have succeeded in attracting the number of active users required for efficient operation. **Objectives:** expand the definition of digital contact tracing systems. **Methodology:** A protocol for contact tracking using location provider information has been proposed. The protocol has been implemented, and its performance has been measured. **Results:** the solution has been implemented, which in addition to being efficient guarantees the privacy of users. **Conclusion:** The presented solution would allow contact tracing, and with sufficient efficiency to scale correctly.

Keywords: COVID-19; contact tracing; Facebook; Google; geolocation; privacy.

CONTACTO: Francisco Caravaca fcaravac@pa.uc3m.es

Fecha de envío:27/03/2023
Fecha de aceptación:29/05/2023

Introducción[1]

Existe un consenso generalizado de que cualquier estrategia para luchar eficazmente contra pandemias, tras la experiencia del COVID-19, requiere un rastreo eficiente de los contactos estrechos de las personas infectadas. Estudios recientes concluyen que el rastreo manual no es lo suficientemente rápido y recomiendan el uso de sistemas digitales de rastreo de contactos capaces de utilizar información de localización a gran escala (Ferretti et al., 2020). Un elemento clave del éxito de un sistema digital de rastreo de contactos es su adopción, es decir, el porcentaje de personas que lo utilizan de forma activa y eficaz.

Singapur fue uno de los primeros países en implantar un sistema digital de localización de contactos en el caso del COVID-19 a principios de 2020. Este país optó por implantar una aplicación (app) móvil que utiliza la tecnología Bluetooth (BT) para identificar cuándo dos usuarios han estado cerca. Si uno de esos usuarios da positivo en la prueba COVID-19, el otro es identificado como posible contagio. El 20% de la población de Singapur instaló la app móvil. Pero esto no fue suficiente. De hecho, un representante del Ministerio de Sanidad de Singapur declaró que necesitarían que tres cuartas partes de los ciudadanos instalaran la app para que la estrategia de rastreo digital de contactos tuviera éxito (StraitTimes, 2020).

Un elemento clave del éxito de un sistema digital de rastreo de contactos es su adopción, es decir, el porcentaje de personas que lo utilizan de forma activa y eficaz

Aunque no está claro cuál es la tasa de adopción a partir de la cual una app BT de rastreo de contactos se convierte en eficaz para controlar una pandemia, algunos estudios preliminares sugirieron que para mitigar la pandemia del COVID-19 sería necesaria la adopción por parte del 60% de la población de un país (Ferretti et al., 2020; Hinch et al., 2020). Algunos estudios de simulación muestran que si la adopción es inferior al 20%, el beneficio de una aplicación de localización de contactos BT es muy pequeño, pero podemos observar un impacto significativo con una tasa de adopción superior al 40%. Una vez más, nos referimos a la tasa de personas que utilizan activamente la aplicación, y no al número de instalaciones.

Las aplicaciones nuevas de rastreo de contactos basadas en BT tienen un problema importante, tienen que conseguir desde cero el alto índice de adopción necesario en un breve periodo de tiempo. Por lo que sabemos, ni los investigadores ni las instituciones públicas o privadas han propuesto una estrategia convincente para alcanzar la tasa de adopción requerida. Por el momento, parece que el éxito de cualquier app de localización de contactos BT depende únicamente de la responsabilidad de las personas, y en el caso del COVID-19 eso no ha sido suficiente.

A pesar del problema descrito y del fracaso de la aplicación de Singapur, la mayoría de los países occidentales, especialmente en Europa, también optaron por aplicaciones móviles que utilizan la tecnología BT como sistema de rastreo de contactos. En concreto, la mayoría de estos países optaron por utilizar el protocolo descentralizado de rastreo de proximidad con preservación de la privacidad (DP-3T). El principal objetivo del diseño de DP-3T es ofrecer garantías de privacidad total. En concreto, se pretende garantizar que las aplicaciones de rastreo de contactos que utilicen este protocolo no puedan ser mal utilizadas en el futuro para prácticas intrusivas en la privacidad de los usuarios, como la publicidad o la vigilancia masiva. A pesar de que los autores de este trabajo creemos que el protocolo DP-3T ofrece garantías de privacidad muy sólidas, algunos autores han expuesto que la solución no ofrece garantías de privacidad plenas.

Para apoyar a las autoridades sanitarias (HAs) dispuestas a desplegar aplicaciones de rastreo de contactos, Google y Apple desarrollaron el denominado sistema Google-Apple Exposure Notification (GAEN) (Apple and Google, 2021) inspirado en el protocolo DP-3T. GAEN se integró en iOS y Android. El sistema operativo (OS) se limita a registrar los encuentros del usuario con BT y ofrece esta información a la aplicación móvil, que implementa el algoritmo para identificar los contactos de riesgo. A pesar de este esfuerzo, por lo que sabemos, ninguna de las apps de rastreo de contactos existentes ha contribuido significativamente a mitigar la transmisión del virus asociado al COVID-19.

Por ejemplo, los primeros datos de las autoridades sanitarias suizas indicaron que sólo el 12% de las personas infectadas informaban de que son seropositivas a través de la aplicación (Salathé et al., 2020). En España, esta cifra se reducía a aproximadamente el 2% en la práctica, a pesar de un documento basado en un estudio piloto

[1] Una parte del contenido de este artículo ha sido publicada en la revista Electronics https://doi.org/10.3390/electronics10091093. Toda la parte de implementacion y evaluación de la solución propuesta son totalmente originales.

realizado en La Gomera (Islas Canarias) que planteaba expectativas mucho mayores sobre la eficacia de la aplicación (Rodríguez et al., 2021). Por último, un informe sobre la aplicación en el Reino Unido (Inglaterra y Gales) (Wymant et al., 2021) presentaba resultados bastante positivos sobre la contribución de la aplicación. Sin embargo, al leer el informe en detalle encontramos los resultados bastante decepcionantes. Aunque el informe afirma que el número de usuarios activos oscila entre el 24,2% y el 33,2%, no discute por qué el número de usuarios activos se redujo en gran medida de 16,5M a 13M durante diciembre de 2020 y enero de 2021, lo que implica en realidad un 21% de usuarios activos. En realidad, se trata de una cuestión muy importante, ya que justo en medio de uno de los peores periodos de la pandemia en el Reino Unido, el número de usuarios activos disminuyó casi un 20%. Esto refleja claramente la insatisfacción de los usuarios con la aplicación. Además, el informe muestra la opacidad de este tipo de soluciones para proporcionar datos útiles a las HAs. Los autores se basaron en modelos para estimar diferentes métricas para analizar la eficiencia de la app. Una vez más, los resultados son decepcionantes.

Por ejemplo, los autores afirman:

> Nuestro análisis sugiere que se evitó un número relativamente grande de casos de COVID-19 mediante el rastreo de contactos a través de la app del NHS, que oscila entre aproximadamente 200 mil y 900 mil dependiendo de los detalles del método, en comparación con los 1,9 millones de casos que realmente se produjeron (Wymant et al., 2021, p. 410).

La gran variación registrada indica claramente que no es posible evaluar con precisión la eficacia de las aplicaciones basadas en BT y que buscan poner la privacidad por encima dew la eficiencia para controlar las infecciones.

Además, las pruebas científicas ponen de manifiesto que la transmisión aérea de COVID-19 es irrefutable (Scientific Brief: SARS-CoV-2 and Potential Airborne Transmission, 2020; Prather et al., 2020; Lednicky et al., 2020), otra limitación importante de las actuales aplicaciones de rastreo de contactos BT. Las apps están diseñadas para identificar el contacto a corta distancia entre dos individuos, es decir, a menos de dos metros de distancia. Sin embargo, la transmisión aérea implica que es posible el contagio entre dos personas a distancias mayores. Por lo tanto, las aplicaciones existentes de rastreo de contactos por vía aérea pueden pasar por alto una fracción importante de contactos que deberían identificarse como contactos de riesgo.

Por último, soluciones como DP-3T, diseñadas con el objetivo principal de ofrecer una privacidad total, presentan otras carencias importantes en la lucha contra una pandemia. Algunas de ellas son: 1) Incluso si la tasa de adopción fuera alta, la mayoría de las apps desplegadas requieren que los usuarios infectados declaren voluntariamente su condición de positivos a través de la app, dejando una tarea muy importante como es el control de una pandemia en manos de la decisión de los individuos. Por ejemplo, un primer estudio realizado en Suiza demuestra que 1/3 de los usuarios de la app que dieron positivo no utilizaron la app para informar de su caso (Salathé et al., 2020). 2) No se puede evaluar el rendimiento y la eficiencia de la app de rastreo de contactos, ni siquiera cua´ntos usuarios infectados se han detectado a través de la app, como reconocen los autores del protocolo DP-3T (Salathé et al., 2020). Y 3), no son capaces de proporcionar información de contexto agregada y no invasiva de la privacidad, que podría ser de gran valor para mejorar nuestros conocimientos sobre los patrones de transmisión de COVID-19 u otros virus. Por ejemplo, en este documento, consideramos que revelar estadísticas agregadas del tipo lugares (restaurantes, instalaciones deportivas, transporte público, hospitales, etc.) que los usuarios infectados visitaron mientras podían contagiar puede ser útil para identificar sesgos estadísticos en el tipo específico de lugares que pueden revelar puntos calientes para la transmisión del virus.

Dado el contexto descrito, el principal objetivo de este trabajo es ampliar la definición de los sistemas digitales de rastreo de contactos teniendo en cuenta los siguientes elementos clave: 1) evitar soluciones que requieran una adopción masiva desde cero, como ha demostrado la experiencia; 2) las soluciones de rastreo de contactos deben diseñarse para considerar como referencia una distancia de transmisión aérea superior a dos metros; 3) orientar el diseño de las soluciones estableciendo como objetivo principal la eficiencia en la lucha contra la pandemia (es decir, salvar vidas y mitigar el impacto en la economía) en lugar de la privacidad. Por supuesto, la solución propuesta debe cumplir las leyes de protección de datos y privacidad vigentes en el país donde se implante.

En este artículo, proponemos un sistema alternativo de trazado digital de contactos basado en los tres elementos clave anteriores como principios fundamentales de diseño:

1) Alta tasa de adopción: Proponemos utilizar información de localización en tiempo real de (literalmente) miles de millones de personas de todo el mundo que ya está disponible en bases de datos de grandes empresas BigTech como Facebook (FB), Google, Apple, operadores de telecomunicación, etc. En este documento nos referiremos a estas empresas como proveedores de localización o *Location Providers* (LPs) por sus siglas en inglés. Algunos de estos LPs, principalmente Google y Facebook, tienen una tasa muy grande de usuarios activos, más del 50%, en muchos países occidentales.
2) Identificación de contactos en el rango de transmisión aérea: Para geolocalizar a los usuarios tanto en exteriores (GPS.gov, 2017) como en interiores (Google, 2020) con una precisión de pocos metros, estas empresas BigTech utilizan una combinación de técnicas que se basan en múltiples señales, como la información de localización GPS, la potencia de la señal WiFi SSIDs, las señales de la red celular, etc.
3) Requisitos legales y éticos: Estamos interesados en realizar el rastreo de contactos sólo para los individuos que han dado positivo de COVID-19. La identidad de los individuos infectados es información sensible manejada por la Autoridad Sanitaria o *Health Authority* (HA) (por sus siglas en inglés) de cada país, que también es responsable de ejecutar la estrategia de rastreo de contactos. Por lo tanto, la HAs tiene la identidad de los individuos infectados mientras que el LP tiene los datos para realizar el rastreo de contactos de esos individuos. Proponemos un sistema que permite llevar a cabo el rastreo de contactos utilizando los datos de los LP sobre aquellos individuos que dieron positivo en las pruebas, tal y como informaron las HA. Incluso las leyes de protección de datos más restrictivas, como la GDPR (EU, 2016), prevén explícitamente excepciones en las que los datos personales pueden utilizarse para controlar epidemias y su propagación (véase el artículo 6 del GDPR (EU, 2016), considerando 46). Sobre esta base jurídica podría ser posible un acuerdo para realizar un intercambio de datos entre los LP y los HA. Sin embargo, para proporcionar mayores garantías de privacidad, proponemos una arquitectura sencilla y un protocolo de comunicación que permitan el intercambio de información entre un LP y una HA limitando significativamente la capacidad de (1) las HAs para obtener el grafo de contactos de un individuo, es decir la estructura y conexión de contactos de los distintos usuarios y (2) los LPs para conocer la identidad de los individuos infectados.

Hay pocos trabajos que expongan el fracaso de las aplicaciones de rastreo de contactos desplegadas y propongan soluciones alternativas que no dependan de nuevas aplicaciones móviles

Hay pocos trabajos en la literatura que expongan el fracaso de las aplicaciones de rastreo de contactos desplegadas y propongan soluciones alternativas que no dependan de nuevas aplicaciones móviles (Mokbel, Abbar, & Stanojevic, 2020; Reichert, Brack, & Scheuermann, 2020; Nakamoto, Wang, Guo, & Zhuang, 2020; Rahman, Khan, Khandaker, Sellathurai, & Salan, 2020). Creemos que sería importante realizar pruebas piloto con las más prometedoras para medir su eficacia. Hasta donde sabemos, nuestro trabajo es el primero que propone una solución que proporciona altas garantías de privacidad para implementar el rastreo de contactos aprovechando los datos de geolocalización que están disponibles en las bases de datos de las BigTechs.

Este trabajo es un propuesta prometedora pero es importante hacer patente que no tenemos pruebas de si nuestro sistema resolverá el problema del rastreo de contactos. Sin embargo, creemos que es una alternativa técnicamente sólida que merece la pena explorar. Además, sirve al propósito principal de este trabajo: animar a la comunidad investigadora a revisar el diseño de soluciones digitales de rastreo de contactos para crear futuras medidas de mitigación más efectivas y eficientes frente a futuras oleadas de COVID-19 y otras pandemias.

Finalmente, hemos desarrollado una implementación de la solución propuesta y hemos hecho pruebas de rendimiento que demuestran que su implementación técnica es viable y cumpliría los requisitos de inmediatez necesarios en la identificación de contactos estrechos en el contexto de una pandemia.

Contexto de la solución propuesta

Razonamiento de la solución

Proponemos una solución novedosa de rastreo de contactos que puede utilizar potencialmente datos de geolocalización de miles de millones de usuarios para encontrar a personas que han estado en contacto con individuos con test positivo. Nos referimos a ellos como contactos de riesgo. La información de geolocalización es propiedad de empresas BigTech denominadas Proveedores de Localización o *Location Provider* (LP) en este documento, y la información de los usuarios que han dado positivo es propiedad de las Autoridades

Sanitarias o *Health Authority* (HA). El núcleo de nuestra solución puede describirse como sigue: Las autoridades sanitarias envían a los proveedores de localización los ID de los usuarios infectados. Las LP utilizan la información de localización que poseen para encontrar los contactos de riesgo de los ID recibidos (de acuerdo con las directrices proporcionadas por expertos en epidemiología) y devuelven la lista de IDs de contactos de riesgo a la HA. Por último, las HAs se ponen en contacto con los contactos de riesgo para informarles del protocolo de prevención que deben seguir.

A efectos prácticos, proponemos utilizar el número de teléfono móvil de las personas como ID de usuario en nuestra solución. Los LPs conocen el número de teléfono móvil de una parte importante de los usuarios que utilizan sus servicios ya que se usa para aspectos de seguridad como el doble factor de autenticación, la recuperación de calves, etc., y es razonable suponer que los HAs registran el teléfono móvil de los usuarios infectados para comunicarse con ellos.

Desgraciadamente, el intercambio directo de datos en claro entre las HAs y los LPs presenta importantes problemas de privacidad. En concreto, los LPs no deben recibir IDs en claro de los individuos infectados y los HAs no deben poder vincular las identificaciones de los contactos de riesgo con su correspondiente usuario infectado. Nuestra solución aborda este reto permitiendo la realización de la tarea de rastreo de contactos con fuertes garantías de privacidad. Para ello, definimos una arquitectura y un protocolo de comunicación que implican, además de a los LPs y las HAs, a dos actores más: un proveedor de identidades (IDP por sus silgas en inglés) y una autoridad independiente de terceros (ITPA por sus siglas en inglés).

¿Por qué utilizar datos de geolocalización?

Adopción: La principal limitación del rastreo de contactos basado en aplicaciones móviles es la necesidad de conseguir una alta tasa de usuarios activos. Este es un importante cuello de botella que hasta ahora ha hecho fracasar todos los intentos en esta línea.

Nuestra solución evita este cuello de botella utilizando datos de geolocalización a gran escala ya disponibles y propiedad de empresas BigTech. Para comparar explícitamente la penetración de los datos de BigTechs frente a las aplicaciones móviles de BT, la tabla 1 muestra para 18 países para los que hemos encontrado datos sobre el número de instalaciones de aplicaciones de localización de contactos: 1) la tasa de penetración de los smartphones, el sistema operativo Android (Dimoco, 2020; StatCounter Global Stats, 2020; Demographics of Mobile Device Ownership and Adoption in the United States, 2020) y los usuarios activos mensuales o *monthly* active *user* (MAU) comunicados por FB; (Facebook, 2020) y 2) la tasa de penetración de la aplicación móvil de rastreo en base al número de instalaciones, así como una estimación de su penetración en términos de usuarios activos. Son datos obtenidos en los años 2020 y 2021. La lista de fuentes que hemos utilizado para informar sobre el número de instalaciones de aplicaciones móviles puede consultarse aquí (FDVT, 2021). Nótese que, hasta donde sabemos, Suiza es el único país que informa del porcentaje de usuarios activos de su app, 63% a 21 de diciembre de 2020 (Swiss Federal Statistical Office, 2020). Para tener una estimación de la fracción de usuarios activos de otros países que comunican el número de instalaciones, aplicamos la proporción suiza al número total de instalaciones.

Según nuestra estimación, ninguno de los países alcanza una tasa de adopción significativa cercana al 40% para las aplicaciones móviles de rastreo de contactos, y sólo 5 países superan el 20%. Por el contrario, la penetración de Facebook supera el 50% en todos los países excepto Alemania (45,5%). Del mismo modo, la penetración de Android es superior al 40% en todos los países excepto EE.UU. (32%) y Suiza (39%). Nótese que la penetración de Android sólo representa un límite inferior de la penetración de Google. Google tiene otras aplicaciones muy populares, como Gmail y Google Maps, que son muy utilizadas por los usuarios de iOS.

Precisión: Las grandes empresas tecnológicas utilizan sofisticadas técnicas que combinan señales de GPS, WiFi y redes celulares para geolocalizar a los usuarios con gran precisión tanto en exteriores como en interiores (GPS.gov, 2017; Google, 2020). Google afirma ser capaz de geolocalizar a los usuarios con una precisión de 1 a 2 metros utilizando algoritmos de multilateración basados en la señal Wifi de 3 puntos de acceso (Google, 2020).

Por lo tanto, las altas tasas de penetración y precisión de localización de las BigTechs las convierten en una fuente de datos que puede ser suficiente para implementar soluciones eficientes de rastreo de contactos. Trabajos de investigación recientes, que utilizan datos de LPs con una penetración mucho menor que FB o Google, también respaldan esta hipótesis (Aleta et al., 2020).

Tabla 1. Penetración en porcentaje de smartphones, Android, Facebook, e instalaciones de aplicaciones de traceo de contactos y número de usuarios activos estimados en 18 países. La población de cada país para calcular la penetración se ha obtenido de la base de datos del Banco Mundial (Data World Bank, 2020).

Países	Smartphone	Android	Facebook	BT apps moviles	
				Instalaciones	Usuarios activos estimados
Alemania	90	61	45.50	34.5	21.7
Australia	105	44	71.42	27.6	17.4
Austria	117	78	50.25	9	5.7
Bélgica	68	41	65.00	12.2	7.7
Croacia	71	59	50.84	2	1,3
Dinamarca	115	55	71.03	34.8	21.9
España	90	71	62.05	11.5	7.2
Estados Unidos	81	32	69.90	2.5	1.6
Finlandia	140	97	59.65	45.3	28.5
Francia	79	51	58.35	9.5	6
Holanda	82	48	63.09	25	15.8
Irlanda	78	42	65.54	40.5	25.5
Italia	84	62	57.80	21.1	13.3
Letonia	96	69	52.45	9.1	5.7
Portugal	104	78	67.47	1	0.6
Reino Unido	85	40	66.64	36.05 *	21.7*
Rep. Checa	84	66	53.32	14	8.8
Suiza	97	39	52.38	33.4	21.1

* El número de usuarios activos en la aplicación móvil de rastreo de contactos para el caso de Reino Unido corresponde sólo a Inglaterra y Gales.

Otros beneficios

La solución propuesta permite supervisar el rendimiento de la misma. Además, las ubicaciones geográficas pueden asociarse a categorías específicas denominadas puntos de interés (Point of Interest o POIs por sus siglas en inglés). Por ejemplo, una ubicación determinada puede asociarse a un restaurante, una estación de tren o un hospital. Nuestra solución aprovecha esto para proporcionar una distribución estadística de los POIs visitados por los usuarios infectados frente a los POIs visitados por la población general. La comparación de estas distribuciones puede ayudar a identificar sesgos estadísticos en los POIs más visitados habitualmente por los usuarios infectados, que podrían ser focos de infección.

Requisitos de privacidad

Por un lado, los expertos en privacidad y las Autoridades de Protección de Datos (DPAs por sus siglas en inglés) han mostrado su preocupación por el uso de información de geolocalización para el rastreo digital de contactos. Básicamente argumentan que puede facilitar a los gobiernos, a través de sus agencias de seguridad, la aplicación de una vigilancia masiva debido a la escalabilidad que ofrecen las tecnologías digitales. Por lo tanto, nuestra solución debería limitar la capacidad de las autoridades sanitarias para deducir masivamente la información del grafo de contactos de las personas utilizando los datos recibidos de los LP. Además, debería proporcionar disposiciones de privacidad para permitir revelar los ataques selectivos dispuestos a inferir el grafo de contactos de individuos concretos.

Por otro lado, las empresas BigTech disponen de medios para inferir la identidad de los individuos infectados. Pueden aprovechar los datos de geolocalización, pero también otras fuentes de información como correos electrónicos, publicaciones en redes sociales o consultas en motores de búsqueda de su propiedad. Por ejemplo, pueden detectar a un usuario que visitó un centro de pruebas después de visitar su sitio web y luego permanece en su casa durante un periodo similar a una cuarentena obligatoria. Por lo tanto, creemos que las propuestas, como la nuestra, que aprovechan los datos de geolocalización de las empresas BigTech no suponen ningún riesgo adicional para la privacidad de los usuarios infectados porque las empresas BigTechs ya cuentan con las capacidades necesarias para inferir con alta probabilidad cuando un usuario ha sido infectado. A pesar de ello, deben ofrecerse garantías de privacidad adecuadas. En particular, nuestra solución no debería proporcionar a los LPs información explicita sobre la identidad de los usuarios infectados. También debería limitar la capacidad de los LPs para inferir tales identidades a partir de la información recibida de las HAs.

Cumpliendo con los requisitos de privacidad

Para cumplir los requisitos de privacidad definidos, aprovechamos los siguientes principios: K-anonymity, criptografía básica y auditoría basada en no repudio.

K-anonymity: En nuestra solución, la HA envía una lista de IDs de usuario al LP, y éste responde con los contactos de riesgo de dichos IDs de usuario. Aprovechando los principios del K-anonymity, la HA mezcla en su solicitud M IDs de usuarios infectados y N IDs aleatorios reales (es decir, números de teléfono móvil aleatorios asociados a usuarios reales) donde M <<< N. Esto sirve para anonimizar la identidad de los usuarios infectados y dificultar la capacidad de los LPs para inferir fácilmente los ID pertenecientes a los usuarios infectados. Los IDs aleatorios utilizados por la HA son proporcionados por un proveedor de identidades (IDP) para garantizar que se trata de ID existentes. En nuestra solución, los IDP están representados por operadores de redes móviles.

Además, la HA debe agregar los IDs en grupos. Hay dos tipos de grupos: Los grupos infectados incluyen exclusivamente IDs de usuarios infectados; los grupos aleatorios incluyen IDs de usuarios aleatorios o una mezcla de usuarios aleatorios e infectados. Los mensajes de la HA al LP incluyen K grupos de los cuales sólo L son grupos infectados, donde L <<< K. Tras la recepción de un mensaje de solicitud de la HA, el LP calcula los contactos de riesgo de cada ID de usuario. A continuación, agrega en la respuesta los contactos de riesgo de todos los identificadores de usuario en un único grupo. Este proceso de agregación se basa en el concepto de K anonymity para evitar que la HA relacione los IDs de contactos de riesgo recibidos con un individuo concreto. Obsérvese que cuanto mayor sea el tamaño de los grupos, mayores serán las garantías de privacidad.

Criptografía: Una HA honesta sólo está interesada en los IDs de contactos de riesgo asociados a los grupos infectados. Para impedir que las HAs accedan a los ID de contacto de grupos aleatorios, el LP cifra la lista de contactos de cada grupo (incluida en la respuesta al HA) utilizando una clave diferente por grupo. Por lo tanto, la HA recibe los IDss de contactos de todos los grupos cifrados. Para recuperar las claves de los grupos infectados, la HA tiene que enviar una solicitud a un intermediario al que denominamos Autoridad Independiente de Terceros (ITPA por sus siglas en inglés). En esta solicitud, la HA indica el número total de grupos en la consulta, así como el ID de los grupos infectados. A su vez, la ITPA solicita las claves de todos los grupos al LP y reenvía a la HA sólo las claves asociadas a los grupos infectados. Por último, utilizando las claves recibidas, la HA obtiene los IDs de los contactos de riesgo asociados únicamente a los grupos infectados, completando así el procedimiento de rastreo de contactos.

Auditoría basada en no repudio: Nuestra solución se basa en el concepto de responsabilidad civil para garantizar los derechos de privacidad de los usuarios. Obsérvese que se trata de un planteamiento ampliamente adoptado en el ordenamiento jurídico de las democracias avanzadas. Por ejemplo, un Estado no puede impedir que alguien conduzca por encima del límite de velocidad, pero quien lo haga es responsable de ello. En el caso de la privacidad, un Estado no puede impedir que una empresa BigTech aplique prácticas intrusivas en la privacidad, pero sí castigarla en caso de que un proceso de auditoría revele el uso de esas prácticas. Por lo tanto, una HA o un LP que utilice los datos que recibe para fines distintos del rastreo de contactos será responsable de ello. Por ejemplo, una HA malintencionada puede llevar a cabo un ataque selectivo (véase la sección Ataques Potenciales y Contramedidas) para desvelar el grafo de contactos de un individuo y filtrarlo a otros poderes públicos. Esto sería un delito equivalente a filtrar el historial médico de un individuo objetivo a otras ramas del gobierno. Nuestra solución recoge las pruebas de no repudio necesarias para que la entidad auditora correspondiente las utilice para desvelar cualquier posible ataque por parte de una HA.

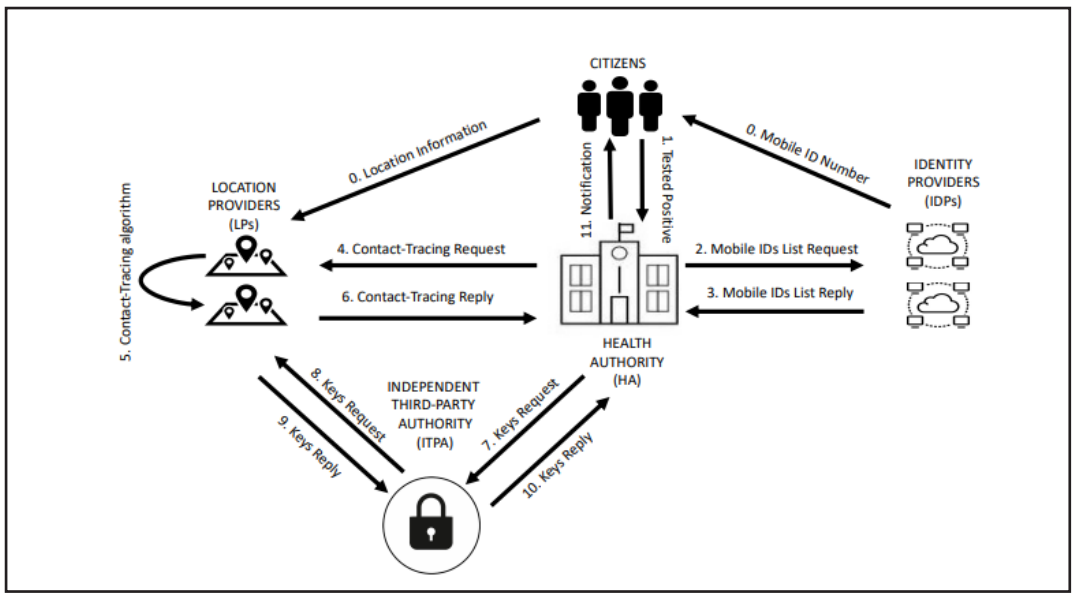


Figura 1. Propuesta de protocolo para rastreo de contactos y arquitectura.

Protocolo para el rastreo de contactos utilizando información de proveedores de localización

En esta sección, describimos los pasos del protocolo de comunicación, incluida la secuencia de mensajes intercambiados por los cuatro actores implicados en nuestra solución: Autoridad Sanitaria (AS), Proveedor de Localización (LP), Proveedor de Identidad (IDP) y una Autoridad Independiente de Terceros (ITPA).

• Paso 0: Este paso se refiere al contexto básico en el que se basa nuestra solución. Por un lado, los LPs registran información histórica sobre la ubicación de los usuarios que ejecutan su sistema operativo, aplicaciones móviles, etc. También almacenan el número de teléfono móvil de una parte importante de los usuarios. Por otro lado, los IDPs, es decir, los operadores de telefonía móvil, proporcionan a los usuarios números de teléfono móvil que sirven como IDs de usuario en nuestra solución.

• Paso 1: La HA obtiene los IDd de los usuarios que han dado positivo en una ventana de tiempo determinada (por ejemplo, un día).

• Paso 2: La HA activa el proceso de rastreo de contactos solicitando al IDP una lista de N IDs de usuario (es decir, números de teléfono móvil reales). El valor de N lo decide la HA y puede variar de una solicitud a otra.

Hay algunas observaciones a tener en cuenta: (1) Este mensaje incluye un identificador único denominado *Transaction ID* que se incluirá en todos los mensajes restantes del proceso; (2) El mensaje se firma con la clave privada de la HA. Obsérvese que en el resto del proceso todas las entidades firman con su clave privada los mensajes que envían.

• Paso 3: El IDP responde a la petición de la HA con una lista de N IDs de usuario aleatorios.

• Paso 4: La HA crea K grupos. Como se ha explicado anteriormente, sólo L de estos grupos son grupos infectados y K L son grupos aleatorios. Los grupos resultantes se incluyen en un mensaje *Contact-Tracing Request* que se envía al LP. Es importante señalar que los ID de usuario incluidos en un grupo infectado no pueden estar presentes en otros grupos infectados en esta solicitud ni en solicitudes pasadas o futuras.

• Paso 5: Tras la recepción de la solicitud de rastreo de contactos, el LP ejecuta el algoritmo de rastreo de contactos para identificar los IDs de contactos de riesgo de cada ID de usuario incluido en la solicitud. Los IDs de contacto de riesgo de todos los usuarios de un grupo se agregan para eliminar cualquier vinculo entre un ID de usuario y un ID de contacto de riesgo.

Además, el LP recopila los POIs visitados por cada ID de usuario en una ventana temporal definida en el pasado (por ejemplo, los últimos 10 días). A continuación, calcula la distribución de los tipos de POIs visitados por los ID de usuario incluidos en cada grupo, así como la distribución global de los tipos de POIs visitados por todos los ID de usuario incluidos en la solicitud.

La información asociada a cada grupo, es decir, la lista de IDs de contactos de riesgo y la distribución de tipos de POI, se cifra con una clave independiente por grupo.

Por último, el LP agrega la información cifrada por grupo junto con la distribución de tipos de POI para todos los IDs de usuario y crea un mensaje *Contact-Tracing Reply* que se envía a la HA.

Tres observaciones importantes a tener en cuenta son: (1) El LP debe mantener un registro de la clave utilizada para cifrar cada grupo; (2) El algoritmo de rastreo de contactos implementado por el LP así como el número de días para la identificación de los POIs visitados debe ser definido por los epidemiólogos y está fuera del objetivo de este trabajo; (3) el LP almacena todos los mensajes *Contact-Tracing Request* recibidos con fines de auditoría.

• Paso 6: Tras la recepción del *Contact-Tracing Reply* la HA necesita desencriptar la información asociada a los grupos infectados, es decir, la lista de contactos de riesgo y el tipo de distribución de POIs. Para ello, envía un mensaje *Keys Request* a la ITPA incluyendo el número total de grupos incluidos en la *Contact-Tracing Request* y los identificadores de los grupos infectados.

• Paso 7: La ITPA envía al LP el mensaje *Keys Request* pero sólo incluye el *Transaction ID*.

• Paso 8: Tras la recepción del mensaje *Keys Request*, el LP envía al ITPA un mensaje *Keys Reply* que incluye las claves de todos los grupos.

• Paso 9: El ITPA comprueba si el número de claves de la respuesta recibida coincide con el número real de grupos comunicados por la HA. Si los números coinciden, el ITPA genera un mensaje *Keys Reply* para la HA que sólo incluye las claves de los grupos infectados. En caso contrario, el mensaje *Keys Reply* incluye un error indicando que el número de grupos comunicado no coincide con el número de claves facilitado por el LP.

• Paso 10: Tras la recepción del mensaje *Keys Reply*, la HA desencripta la información sobre los contactos de riesgo y el tipo de distribución de POIs incluida en el mensaje *Contact-Tracing Reply* para los grupos de usuarios infectados.

• Paso 11: La HA se pone en contacto con los contactos de riesgo.

Ataques potenciales y contramedidas

Como se ha explicado anteriormente, nuestra solución está diseñada para impedir que tanto los LPs como las HAs se comporten de manera inadecuada y accedan a información que no están autorizadas a obtener.

A continuación, explicamos en detalle las contramedidas que ofrece nuestra solución para evitar: 1) que los LPs intenten deducir los IDs asociados a los individuos infectados; y, 2) que las HAs intenten obtener el grafo de contactos de los ciudadanos.

Inferencia de la identidad de los usuarios infectados por parte del LP

Un LP malicioso podría intentar desvelar la identidad de los usuarios infectados basándose en la información recibida en los mensajes *Contact-Tracing Request*, lo que se conoce como ataque de reidentificación. Para ello, podrían utilizar una obtener la única solicitud o combinar solicitudes posteriores para identidad de los usuarios infectados.

Para evitar los ataques de re-identificación, la HA tiene que reutilizar los IDs que ya han sido utilizados incluyéndolos en grupos aleatorios de peticiones posteriores. De lo contrario, si los ID aleatorios sólo se utilizan una vez y se descartan, el LP podría inferir con una probabilidad muy alta que los IDd repetidos en diferentes consultas pertenecen a individuos infectados.

Además de la reutilización de IDs, nuestra solución se basa en el principio de K-anonymity. El número de IDs aleatorios, N, en los mensajes de solicitud es varias veces mayor que el número de IDs de usuarios infectados, M. La complejidad para realizar un ataque de reidentificación crece con el cociente N . Además, nuestra solución permite introducir un alto nivel de aleatoriedad en los mensajes de petición para evitar que los LPs puedan inferir patrones que permitan identificar grupos que incluyan IDs de usuarios infectados: 1) el número de IDs de usuarios infectados y aleatorios difiere de mensaje a mensaje; 2) el número de grupos en un mensaje difiere de mensaje a mensaje; y, 3) la longitud de los diferentes grupos dentro del mismo mensaje también debería diferir. Además, la HA podría enviar de vez en cuando mensajes que no incluyan ninguna identificación de usuario infectado.

Más allá de las medidas técnicas, el principal argumento para apoyar nuestra solución es que los LPs potentes como Google o Facebook dispuestas a identificar a los ciudadanos infectados ya pueden hacerlo fácilmente con la información que poseen. Por lo tanto, las medidas de privacidad adoptadas en nuestra solución ofrecen garantía suficientes para evitar que aumente el riesgo de un posible ataque de reidentificación por parte de los LP con respecto a ataques que pueden implementar a día de hoy.

Inferencia por parte de la HA del grafo de contactos de un usuario-id

Nuestra solución no puede evitar de antemano que una HA maliciosa obtenga el grafo de contactos de un individuo concreto. Por ejemplo, una HA puede realizar un ataque dirigido utilizando dos veces el mismo ID en dos grupos infectados diferentes. Los contactos de riesgo comunes en los dos grupos pueden revelar el grafo de contactos del individuo objetivo. Una persona podría volver a infectarse y aparecer en dos solicitudes de rastreo de contactos diferentes de la misma HA, aunque estas solicitudes no deberían producirse en un corto periodo de tiempo. La segunda solicitud debería aparecer al menos unas semanas o meses después de la primera solicitud de rastreo de contactos que contenga el ID de esta persona.

Una opción eficiente para evitar que la HA pueda obtener el grafo de contactos de usuarios re-infectados, es obligar a la HA a eliminar la información de los grupos de contacto descifrados al cabo de un periodo de tiempo en el cuál es altamente improbable que un usuario vuelva a reinfectarse. Por ejemplo, cada semana o cada dos semanas. De esta forma, la HA no podrá obtener el grafo de una persona que se reinfecta pasados unos meses.

Además, nuestra solución conserva las pruebas de no repudio necesarias para demostrar que se ha producido un ataque de este tipo. La entidad auditora sólo tiene que comprobar si el HA ha utilizado el mismo ID dos veces (o más) en grupos de usuarios infectados en el mismo mensaje o en mensajes diferentes durante la ventana temporal previa al borrado de datos. La entidad auditora puede recuperar todos los mensajes *Contact-Tracing Request* del LP. Del mismo modo, la entidad auditora recupera de la ITPA, para cada mensaje *Contact-Tracing Request*, cuáles son los grupos infectados declarados por la HA. Con esa información, la entidad auditora podría identificar los ataques de la HA. La capacidad de auditoría descrita proporciona garantías de privacidad basadas en la responsabilidad innegable, una técnica muy utilizada en las democracias desarrolladas.

Por último, nuestra recomendación es ejecutar el proceso de auditoría descrito una vez al día para detectar cualquier HA maliciosa poco después de que haya implementado un ataque.

Implementación

El protocolo que forma parte de la solución descrita se implementa sobre HTTPS, en concreto, los dos proveedores: Proveedor de Identidad (IDP) y Proveedor de Localización (LP), y también la Autoridad Independiente de Terceros (ITPA) se desarrollan como servidores HTTPS que reciben peticiones POSTs de la Autoridad Sanitaria (HA), o de los otros servidores. El uso de HTTPS proporcionará cifrado de extremo a extremo de los datos transmitidos, los clientes también comprobarán la autenticidad de los certificados de los servidores. Además, todos los mensajes son firmados y comprobados por todas las partes implicadas.

El repositorio del código está disponible en https://github.com/fcaravaca/DigitalContactTracing.

Estructura

Los servidores de la implementación (IDP, LP e ITPA) son contenedores Docker que contienen el propio servidor (será un servidor Express) y una base de datos MySQL. El fichero de configuración permite la posibilidad de lanzar varios contenedores docker de cada tipo de servidor.

Encriptación de contactos

Los contactos de los grupos se envían a la Autoridad Sanitaria cifrados, en concreto con AES-256 (CBC como modo de funcionamiento). El Proveedor de Localización cifrará cada uno de los grupos por separado, con diferentes Claves y Vectores de Inicialización (IVs) generados aleatoriamente. Estas Claves e IVs se almacenan en la base de datos del Proveedor de Localización y sólo se enviarán a una Autoridad Independiente de Terceros (ITPA). La ITPA recibirá el número de grupos y sólo enviará las claves e IVs de los grupos infectados a la Autoridad Sanitaria.

Firmas

Cada uno de los actores involucrados en el protocolo tendrá que firmar sus mensajes para permitir que el otro extremo verifique la autenticidad de los mensajes enviados. Esto se hace con un par de claves Privada y Pública, el emisor utilizará su clave privada para firmar la información, y el receptor la verificará utilizando la clave pública del emisor.

Esta solución utiliza RSA con SHA256. La información se convertirá en una cadena base64, a la que se aplicará el hash SHA256. Esta información se cifrará utilizando la clave privada del remitente. El receptor calculará el hash

SHA256 de la información recibida y descifrará la firma utilizando la clave pública del remitente. A continuación, el receptor comprobará si la firma y la información son equivalentes, validando así la autenticidad del remitente. La firma también puede utilizarse con fines de no repudio.

Cada uno de los servicios tendrá acceso a su clave privada, y a las claves públicas de los otros sistemas, para firmar y validar las firmas respectivamente.

Formato de los mensajes

Los mensajes entre los servicios siguen la misma estructura básica, en forma de JSON:

```
{
    "información Base64(información),
    "firma": Base64(RSA(SHA256(Base64(información)), privateKey)),
    "id": remitente
}
```

La información es un JSON, cuyo formato varía entre cada mensaje, si bien, en cada uno de los mensajes siempre hay un campo que corresponde al *id transaction*. La información se envía calculando su representación Base64, esto es debido a que la representación del objeto JSON puede variar de extremo a extremo, por lo que es más seguro firmar y enviar la información codificada en Base64, aunque los datos transmitidos aumentarán.

Auditoría

La auditoría se puede realizar con la información guardada en las Bases de Datos de las ITPAs, LPs e IDPs. Estas tablas incluyen los IDs de las transacciones, la HA que solicita la transacción y algunos de los parámetros relacionados con las mismas. La entidad auditora debería solicitar la información a los LP, IDP e ITPA, para después comprobar el estado de cada una de las bases de datos y ver las solicitudes realizadas desde un HA específico, ver la frecuencia de las solicitudes, o comprobar si el HA solicita información a un IDP cada vez que realiza una solicitud a un LP.

Podrían utilizarse otros datos de auditoría, guardando los datos brutos de las solicitudes realizadas desde la HA al LP. Esta información podría combinarse con la base de datos ITPA, para ver entonces si un identificador de un usuario se utiliza en varios grupos infectados, ya que la HA podría estar intentando inferir el gráfico de contactos de un usuario.

Mensajes de transacciones completas

En esta sección mostramos el contenido de los mensajes compartidos entre las partes implicadas en una simulación sencilla, para comprobar los contactos de 10 personas infectadas. La HA incluirá 10 teléfonos por cada uno de los teléfonos infectados, por lo que enviará 110 contactos en diferentes grupos. En particular, esta HA decide hacer 2 grupos para los teléfonos infectados, por lo tanto esto significa que en promedio los grupos deben tener una longitud de 5 teléfonos, y habrá 20 grupos de teléfonos al azar. Por lo tanto, un total de 22 grupos serán enviados al Proveedor de Localización.

Aquí mostramos el contenido de las peticiones y respuestas decodificando el base64 del campo info.

Resumen de los parámetros de simulación:

```
Phones infected (M = 10) = +34 600 000 001, +34 600 000 002, +34 600 000 003,
    +34 600 000 004, +34 600 000 005, +34 600 000 006, +34 600 000 007, +34
    600 000 008, +34 600 000 009 , +34 600 000 010

L = 2
N/M = 10 -> N = 10
K = 22 as K - L = 20, to maintain the same group size in all K groups
```

La HA estabelce un nuevo *transaction ID* con el valor cc92e749-4480-4f1d-9db6-978efcd46523, y envía un mensage al IDP solicitando 100 números de telefono aleatorios.


```
{
 "id":"HA",
 "info":{
  "transaction_ID":"cc92e749-4480-4f1d-9db6-978efcd46523",
  "amount":100
 },
 "signature":"I7e7zF7Dwi/u20YqQu8CSdWLZm3mdH0gxTIVKeZGTks/v5XNBqOvH3BO
 6GrB1HKcKNYJmY4mgz5NEHJfNimRdDcY/Y5RsLq41DDH1SMuY6K9uCCGGpkiW3fekfdIv
 n1+7bwp3zLoEvfOdFIOY2RBhTfa3TDRvkE26I7WlyqI9RtVBytdduYTGCATVPmWaek/5i
 tw6CWPkLelOaf9lbzhRRiZAyJ3L7M6D6FWNOLYMJDdIdFMRzTq7NyhFQlQ6mdjg1gUJeb
 gWSJxclylzl0hcJGpkyRVTQDQsfzDovQ5conImUcY9UAi/ZNBvQeqzmQVC3ILKGeijMJC
 R1pSQq6wGQ=="
}
```


Respuesta de IDP a HA, que devuelve los 100 telefonos aleatorios.


```
{
  "info":{
    "transaction_ID":"cc92e749-4480-4f1d-9db6-978efcd46523",
    "amount":100,
    "ids":[
           "+34 653 788 444", "+34 648 411 356", "+34 603 539 920", "+34 649
               785 675", "+34 663 729 249", "+34 696 432 331", "+34 603 278
               344", "+34 682 887 384", "+34 605 283 029", "+34 650 437 443",
               "+34 623 465 678", "+34 603 997 526", "+34 685 327 541", "+34
               632 726 211", "+34 611 010 619", "+34 669 470 430", "+34 601
               175 472", "+34 683 395 773", "+34 650 757 568", "+34 651 397
               644", "+34 662 262 889", "+34 650 545 033", "+34 677 323 626",
               "+34 673 550 058", "+34 630 476 478", "+34 617 817 103", "+34
               672 261 416", "+34 666 891 280", "+34 628 257 589", "+34 670
               695 441", "+34 648 951 489", "+34 643 088 158", "+34 632 070
               640", "+34 614 093 031", "+34 640 922 608", "+34 640 439 978",
               "+34 684 187 530", "+34 613 848 622", "+34 600 669 193", "+34
               614 035 237", "+34 673 195 847", "+34 617 674 407", "+34 698
               818 999", "+34 658 500 365", "+34 648 217 882", "+34 680 477
               943", "+34 672 391 058", "+34 685 116 085", "+34 604 456 764",
               "+34 634 022 350", "+34 663 709 522", "+34 639 383 419", "+34
               686 091 747", "+34 637 293 314", "+34 688 197 010", "+34 639
               884 733", "+34 629 404 805", "+34 618 506 098", "+34 635 722
               271", "+34 648 088 325", "+34 621 851 577", "+34 614 437 919",
               "+34 696 116 590", "+34 692 536 429", "+34 691 483 831", "+34
               602 657 187", "+34 657 763 786", "+34 677 778 487", "+34 668
               296 886", "+34 631 319 526", "+34 633 183 965", "+34 646 668
               115", "+34 662 066 763", "+34 692 687 369", "+34 656 674 921",
               "+34 628 398 123", "+34 663 186 294", "+34 663 953 368", "+34
               674 459 789", "+34 668 683 752", "+34 649 132 555", "+34 682
               772 220", "+34 639 669 893", "+34 646 046 481", "+34 665 777
               823", "+34 640 628 251", "+34 658 464 281", "+34 681 813 791",
               "+34 626 986 647", "+34 691 164 273", "+34 637 169 576", "+34
               635 382 402", "+34 634 279 625", "+34 658 723 255", "+34 643
               013 653", "+34 663 884 025", "+34 679 732 955", "+34 600 346
               094", "+34 657 118 433", "+34 667 194 644"
    ]
  },
  "id":"IDP",
  "signature":"W4uZzTh9DAuON8w+R8qobHrrtUib0FcKezIGbfvpa7ajUDPlGaRB9hm2
qo8hDOteDsGviSjMBJ7c104PoiMeOY3Iw3D88lp6wAZf1j2L34YfqFpQJHfXUyjJNSJKX
lcd/LsWiC4mWS3yXDoDtm455gBs2EInTFe8/yso5Qhxpx020heosa4YQS0i/PRywKIP9h
45geSVvSniKoq7K0Q9r+pKa5yBigV8plEJKtQ85h+HOdkx7UGX/c67XdK+pOcYv/bA11o
wISApiUKRGZ5c5IpMhvsFQ61ApoRcCwz85zHqb4PhZ33ia5t/ijoZNc6PJkek8h0KisnC
2CEonuki9A=="
```

```
}
```

Tras recibir los telefonos, la HA genera los grupos y asigna a cada uno de ellos un ID de grupo aleatorio. El tamano medio de los grupos es de 5, pero la cantidad en cada grupo será aleatoria. Los IDs de los grupos iinfectados son 1e85ada3-bc1e-4442-bbd4-20e3b2e20691 y 2c43ac0e-f072-4aad-aeae-6988671b5746, con longitudes de 7 y 3 respectivamente.


```
{
  "id":"HA",
  "info":{
    "transaction_ID":"cc92e749-4480-4f1d-9db6-978efcd46523",
    "groups":[
      {
        "group_id":"6c62ab11-8866-4dfc-9c66-5459b68d722e",
        "ids":[ "+34 650 757 568", "+34 600 669 193", "+34 663 709 522", "+34
            674 459 789"
        ]
      },
      {
        "group_id":"607ac506-588e-4a0d-ac8f-c6118fa608f5",
        "ids":[ "+34 605 283 029", "+34 628 257 589", "+34 648 217 882", "+34
            635 722 271", "+34 633 183 965", "+34 668 683 752"
        ]
      },
      {
        "group_id":"6513caa1-86e7-4d3d-8f4a-e18090be2606",
        "ids":[ "+34 603 278 344", "+34 672 261 416", "+34 662 066 763", "+34
            682 772 220", "+34 640 628 251", "+34 600 346 094"
        ]
      },
      {
        "group_id":"f21c85eb-319f-4934-8053-b0f873893223",
        "ids":[ "+34 683 395 773", "+34 613 848 622", "+34 673 195 847", "+34
            634 022 350", "+34 686 091 747", "+34 688 197 010", "+34 649 132
            555", "+34 658 464 281", "+34 626 986 647"
        ]
      },
      {
        "group_id":"100a569f-2137-4711-b74c-7e25ae53dabb",
        "ids":[ "+34 649 785 675", "+34 673 550 058", "+34 614 437 919", "+34
            691 483 831", "+34 643 013 653"
        ]
      },
      {
        "group_id":"7749d184-c758-4b1d-935b-cfc3016bac7e",
        "ids":[ "+34 648 411 356", "+34 650 545 033", "+34 672 391 058", "+34
            629 404 805", "+34 602 657 187"
        ]
      },
```

```
{
  "group_id":"03fbc052-5134-4703-be20-c407c0835e9a",
  "ids":[ "+34 651 397 644", "+34 614 035 237", "+34 668 296 886", "+34
      631 319 526", "+34 646 668 115", "+34 663 953 368", "+34 657 118
      433"
  ]
},
{
  "group_id":"8303b685-f91d-4e1d-b110-9e799c175a4c",
  "ids":[ "+34 650 437 443", "+34 670 695 441", "+34 680 477 943", "+34
      618 506 098", "+34 692 687 369"
  ]
},
{
  "group_id":"19d4189a-a579-4634-b413-8a7e4f3e2468",
  "ids":[ "+34 696 432 331", "+34 617 817 103", "+34 639 884 733", "+34
      639 669 893"
  ]
},
{
  "group_id":"d2691a90-012d-40f9-91f2-6abf79f01443",
  "ids":[ "+34 603 539 920", "+34 677 323 626", "+34 696 116 590", "+34
      677 778 487", "+34 658 723 255"
  ]
},
{
  "group_id":"01e71438-d681-440f-9ebe-2f719157e08a",
  "ids":[ "+34 682 887 384", "+34 666 891 280", "+34 646 046 481"
  ]
},
{
  "group_id":"cac5d3ed-d5e1-4ca4-9d97-c57ea390ba99",
  "ids":[ "+34 601 175 472", "+34 684 187 530", "+34 658 500 365", "+34
      604 456 764", "+34 657 763 786"
  ]
},
{
  "group_id":"1e85ada3-bc1e-4442-bbd4-20e3b2e20691",
  "ids":[ "+34 600 000 002", "+34 600 000 004", "+34 600 000 005", "+34
      600 000 006", "+34 600 000 008", "+34 600 000 009", "+34 600 000
      010"
  ]
},
{
  "group_id":"54b5d3e4-5c4c-497c-98c2-fd880a0aa04b",
  "ids":[ "+34 663 729 249", "+34 630 476 478", "+34 698 818 999", "+34
      663 186 294", "+34 665 777 823", "+34 637 169 576"
  ]
},
```

```
    {
      "group_id":"2c43ac0e-f072-4aad-aeae-6988671b5746",
      "ids":[ "+34 600 000 001", "+34 600 000 003", "+34 600 000 007"
      ]
    },
    {
      "group_id":"26debb37-f758-4f0c-af1f-ecb8c29d5b27",
      "ids":[ "+34 603 997 526", "+34 643 088 158", "+34 639 383 419", "+34
          692 536 429", "+34 635 382 402", "+34 667 194 644"
      ]
    },
    {
      "group_id":"85cdf393-613b-41bf-92fe-046318523af0",
      "ids":[ "+34 632 726 211", "+34 614 093 031", "+34 656 674 921", "+34
          681 813 791", "+34 663 884 025"
      ]
    },
    {
      "group_id":"cf3b88bc-5961-49c6-a6e4-f925491e3f7e",
      "ids":[ "+34 653 788 444", "+34 662 262 889"
      ]
    },
    {
      "group_id":"e960bb6e-660b-4ff6-8e0f-a840ce01a260",
      "ids":[ "+34 669 470 430", "+34 640 439 978", "+34 617 674 407", "+34
          621 851 577", "+34 628 398 123"
      ]
    },
    {
      "group_id":"a61a1144-08d7-4a95-9306-96918e0be333",
      "ids":[ "+34 623 465 678", "+34 648 951 489", "+34 685 116 085", "+34
          637 293 314"
      ]
    },
    {
      "group_id":"5960a1a5-db1a-42bd-bb67-adfcff3f85c9",
      "ids":[ "+34 611 010 619", "+34 640 922 608", "+34 648 088 325", "+34
          634 279 625"
      ]
    },
    {
      "group_id":"daf8579e-a23e-4fa7-9b46-885158930741",
      "ids":[ "+34 685 327 541", "+34 632 070 640", "+34 691 164 273", "+34
          679 732 955"
      ]
    }
  ]
 },
"signature":"FviNsY6T+jauxiC/hcKOjpoH6WTiKfIyFhCIT6LENDL+IglMB3PxzAPT
```

```
DeBe1WHTv1NMQVEew+0okHW8QbOBbQZZOlPSrUljwwLGlLmnrhYdgdbqlAuMP29Sovs2Z
PUBPrf77OkHH2qXvpt8HOxZd1Y5LBOd58XXMW2Isn7qIJ6cnf3PsVHJZ/c8SvN1ntM6yQ
X10Mtr3rekPy3knkAbObo0GlK3FMo/gNSoLryEYJGtmKlP5copdZOgrszam4PUJSbz2zn
n8cGRxPny2sBcFu6j4CXVC/ZPyInYxEB0e0FmHiopeSqEmp9PCka845khOShDvpBtxPOW
YEhmGA/xyw=="
}
```


El proveedor local ejecuta el algoritmo de deteccion de contactos estrechos y envía los contactos de cada grupo cifrados.


```
{
  "id":"LP1",
  "info":{
    "transaction_ID":"cc92e749-4480-4f1d-9db6-978efcd46523",
    "groups":[
      {
        "group_id":"6c62ab11-8866-4dfc-9c66-5459b68d722e",
        "contact_ids":"sUUPEK+NeCbPZLHTNim9oy8JcJZRyZ4m7mq1wGMlVd3udsla
        Zeyk9YWZtSOsyYHJv0zAqjGWzcNBDuO0qbs+yyuVNE5b/Yu8owY8lkQL6GIHTIW
        d3SKOoFhM0Y24fiXMOrX31uZwiZB7YHb85Ty7fZpG80fjxjp/aTCQ/vX2SLsv6Q
        uuKXtehCfdPRQMfeI+M4CRh7wjHZ6n22pHp4yKZ3VE3XM2N09n5IUKgbtAmki7O
        ACGa8R3znGmtwcfykNU"
      },
      {
        "group_id":"607ac506-588e-4a0d-ac8f-c6118fa608f5",
        "contact_ids":"UA2guYJVDDXQclP8r5uq4A0WRqgJQmLHVW4EV+VPmacv0Z5K
        eA+IlLewtyOCHyEcZ4DooQlPznyWB8pTDpTzT6SyonAjaLTcTKShHNAFHFqr0tb
        8LVdjoGtU0/nzetuDZtuaLMsC0FuojDFRE6ZE/A=="
      },
      {
        "group_id":"6513caa1-86e7-4d3d-8f4a-e18090be2606",
        "contact_ids":"ZwofGVVARyBzrRBZTvDlYcYZbr8QFV8nssU/+lmnrIJZ41ca
        6hPQ9h5Tgl4pcbqo7lp43LdDyPKK1ng8rPGYmdKQIRsRAZSeCunOaZ/HYwuIUuz
        Fvc5/R5VgIvlwp75SiTP0Be3Qfq1GsC4ZJ5UhtvlJJKUkn8k8qpd389j3HS4IB2
        V81Uqts/CX8BmWCnrp8alr1ANV+syoCN8fAGyiucYP1Xmg/Gq/L3ZuyN2ufG54W
        MTS4KebQ6EOq38nud3HHivMO9fxkSVrsVT8216ESA=="
      },
      {
        "group_id":"f21c85eb-319f-4934-8053-b0f873893223",
        "contact_ids":"InjL6sLDyjyv9DcoRJROnQSijYErNhKQHIUf2XgXh8nk4vs2
        uOAFk3DaG4PRIIZ1diEDf4cgsdt5f6wqXyXHhN7xfXvD8QFAdJHR/F3MEgj03KB
        Lji9Opk6Nf8QUn9DEk8mutrMnxr5FW90+yfNQeCcHA7TxMxagnB6M8exPae1zkj
        OGBbZ9jH7R7b6ID1wIbSon99LUrtySQekPAISZWRsVHyPHcui81FRCkqZBcVlDf
        bFOBA+NXZSjHyU+6j5OdE6yfxUXTU0s4ii8gRoGLAaZDuahywpbAfJH4juXSiM3
        Bo/LkaOmSZqchtHuwaFR9Bt1jXhFafrFbypMknCdsuHOzpLlHF7wvxEDdpAmUwp
        DF9pCDrnPrFwir9A0O1NqU5Fi5Ft+JHf9cvTWBKSobfUJVSbiQSNPurkuzkmps9
        v2OcrmctYg0+bkkYsRBGgKuv91z9E4TMLaw2UHiDo0zCMxd8J2IkDntDmyQ/2wo
        ccl+F0b8vR3kJVsfH0vJSFVO2DPmZC5nruhhF8c8pMp4txQ3yUr7NlkMkWlcTdq
        gAbEV0Tfmfu7HG190mQwKgANHVOOqIDup3Qn7RATOIzKtA=="
      }
```

```
  },
  {
    "group_id":"100a569f-2137-4711-b74c-7e25ae53dabb",
    "contact_ids":"hRLwG5I+xLtDBOg+Me0cxH/gQ5FxSBT4/bpLSiol575Sp5oK
    dNqFxwFkTaGG9yajwCHoptU+tVW0Lp/rxmwtSLV2unzdT3inodGIIs9mbfxuhU6
    7z7nbPwaZ2wvXSBbrudusQakbTHx7NfoqeDGWGOB7KSZZEO1RAzjnakjfAI6fg1
    bRZL22TE4ymyVneSXZOMbVmslqBvb1PjVNbflAipkpPl25MRMpmnanQOhSw1oLn
    HF96xuvHfiAvcj7ooGFn/TUxuIkRrfV9Vh4VsC9qg=="
  },
  {
    "group_id":"7749d184-c758-4b1d-935b-cfc3016bac7e",
    "contact_ids":"RzNuT90hIXX6iB7BvVWMwNv9Ma4uIGl+92MkAFKHM/ln7ub7
    +cy30tWZeGCt8ocgaqyeA7VukDhZBScwAQt4N//2XWeiAMjykBnOlhosxAutsXO
    10oBvDmu1yATgILb8va4mOGUeIXTWAkBuo5lBeSvXYy7mzbgrsP0l3fhVrS0kb3
    cqlupE1/Z+4nqSJYq+qg6UNY9jFMLTTmc5dPyt+Kwe2Szg88blhDmpCzxoan0="
  },
  {
    "group_id":"03fbc052-5134-4703-be20-c407c0835e9a",
    "contact_ids":"WNY+YPvgn4Ed/1A/XxOOH0LUkQSKfWI1hQ7rv8nq2bCHXGR7
    6BfQUpNcCKtuD3IBslgjPW5U1tU8DDgKBFSQGcCZPGsn1DtbXt8oqvHgHHw0UUL
    UXkDqTbzRoL7zkXQkiBbeLqz0x6wrVaeEDn48MTIngEQ04bPe0P/mbk71X8mwDB
    xm8VL+/P0nsAmRh1S1DeZ/r+Ut83nmuxA2XRimkQFGYLV7WB3BUI3/zceD6WrSU
    L4dhvJJoVRuEsYuuzyy"
  },
  {
    "group_id":"8303b685-f91d-4e1d-b110-9e799c175a4c",
    "contact_ids":"S4qXjgbXGtTfTRKDbXI9PiktosJ9D59FIGE3rgv1sC6Sp6hf
    XbkfA1zGUDAR00nACpsLEEj+fvUAXE2BIxSA7Qm3OFSbx86IAvsBlMMBRA9qUFy
    8GcXBC3NRy96gCfYEUwPvc5saTYgMX8b/MQU1rskPLBshqYLEC8iSuSUFm6n9in
    n9nbaQtqxAUCMOU9/+I5K8tdrEXw32rl41e02ENO5hinzOMuImh9+Mkp5ymeXJQ
    h1Fpp92EkDgnQO3EKXV"
  },
  {
    "group_id":"19d4189a-a579-4634-b413-8a7e4f3e2468",
    "contact_ids":"FSv+GtwB1tyy+1YuYKc+pW2DLOsWqpEhXpAYtwQrz7ySNnjM
    K5wCP3qjYQ+JH8wKHIr62AjS8aPDoMkkL+LJMznxA6gNRf0YdkQYcNQ0Ro5dXSh
    pT7OPE3MsnB4LcZ4tsUQhz9A39WawxmyTg1LSmw=="
  },
  {
    "group_id":"d2691a90-012d-40f9-91f2-6abf79f01443",
    "contact_ids":"fH80TsqZ2MYqV/FRMyB5CRf77ShprDZYbciUmY5qNVRD0SjC
    EpM+UpKWzCZDMtu21znvlDaSjv3sBhMZmRlpuhm0BqDx8mxn1bH/Klkj8zvwZo1
    qk2qlmo86alyqEfSFVIVG6rSIXqGReCf0X+ADGDEaxCuh7j4enETQx49/qMvPAs
    O+I9M1ebKL9RhkFWl3LCixghsDbQ29G+bItyBcq4YKWOBVLK4o3HRi6r2AxG0kA
    +KDxqOaTw9FzxQVgyt5ZpGYyzhmG4X1kBWx2RrAvg=="
  },
  {
    "group_id":"01e71438-d681-440f-9ebe-2f719157e08a",
    "contact_ids":"O7GUI8Un3bsYm6fM+jPZFL2RhqaE0oUcmErEnYknIbT/OZVR
```

```
    i+yRWaR4v4/EbcIUjQQQG9yIiHX3KOOCyYRrOJvUpYmwXfJedDYyV6PZnTDSr3q
    PFxaxfHVq+qHYfEfyZcl9cAqXGV9giF4ldWn3oR18OymYlGp5YueBPeX7o9Los9
    loSO40SNAuFvi2Iw4Qa71MUAH2OJaaDBwksTG/yp48o7f/g98eBvv6en4mh2U="

  },
  {
    "group_id":"cac5d3ed-d5e1-4ca4-9d97-c57ea390ba99",
    "contact_ids":"UWD2qCZWG4RA766BHa8ZiXe1foxk0NsxcbUf4leYrHUPQXql
    v96CauQW9NoSng/iDFsvAFd9F7zbVViwYdVJMEQFANypvsnfGegpGpKktZKDZ9N
    YCX9CSUMRHe/TISk0Qjzr3zLNZKeD2JzvG9ZsGipCqv/B/fvAnr1A5w9nz8iv6E
    1L+ll8jXlm+AWujLtGe10s5HlkvQ4trPL1qc9x9sg9fgyI1seX47h87PCbMYpor
    2KRRKAp3wzPL8q4OS2+yFgE5vnuhPnfaxxGWlh1xA=="
  },
  {
    "group_id":"1e85ada3-bc1e-4442-bbd4-20e3b2e20691",
    "contact_ids":"F/00zIj7tKxjGlVYOJaUfjLJmZ6+kr0wHbMWzgHz6KWV82tG
    VkW+zoUB1p1Ctpclo7yud49wUdUlY8sg+QMNZ84tAYCzWNbT6vjLwi7fL3h7woO
    cPoVOZibsnq/osD6999Zns3kVHPBXfV2W8hvg5lUAdP/9PLa8G9yeXUMn4o3IBZ
    8vCg0gIcEb87rgszIHiftQfdcSiclMiPi/8wCWYi2eAHigQP8pLEoKN8yUdBTzS
    CdJr7HETgkuw+D6G5kGCw1xNTulGem2i/jhcfbT/sJHWhzLPXrtJ/0kg38rwbRS
    ISmnK4vLXhVcOigGCGUTaDBVvYI7bHlFgCK3qWsFYQfQwpSLyn45JYJ4eysHNrg
    ="
  },
  {
    "group_id":"54b5d3e4-5c4c-497c-98c2-fd880a0aa04b",
    "contact_ids":"D60jicPbCrzIq8Vo9wZ/WjTypIv2xxMbPQhCRR1/GSAqTvj9
    R4vT1fNB0iI0BBpG5IOEWBFK9eyBq9aQ9a6rQrG/TtjvyIpjLaZ2XWK5ppIcvLU
    qq76MQyN5f0OvSec11lTDik2nxAcU7yTjn32P+t/wDzENy5NoO2nGFJvLjwkXbN
    bz1uncazLoszv1hG0+MzE21hsYSTeVJjSsYn9M+OqNYMQ9RfI2cpZ5gPQJ/DWzE
    4LSvLpUCr+DNC0/eGJ+FwFYiViWZzzkNaIhPh3WlVINsS0XPHDY9HUuJopW6f7c
    xUcGLG8Bh+BYlHPb9EYR1of8kgvNZ9LeRNTIuRSqMQ=="
  },
  {
    "group_id":"2c43ac0e-f072-4aad-aeae-6988671b5746",
    "contact_ids":"qej+knFvl7LAtPrA2IzBDFbF69qcZ2r65Bz+NTMEHl5dbu++
    +eYTUqykvRg51gie3h3lkRpa/f0FTiTsQTPzJqwLfy88ajxq0mfx9Ap2EgpMswV
    d3CPGZLWTk1JBWgksDaJaIZW8mksdQPZE41Z9mg=="
  },
  {
    "group_id":"26debb37-f758-4f0c-af1f-ecb8c29d5b27",
    "contact_ids":"cBU2kBmObS3Ot6X35hQczki6xKNO5lIqoFjXUJCpk8nTdiyy
    FOmAM+0tnpZa2JDe1pZh+K/Hb0tpQDpwfQyQL4g3rHFiZRjdOTcZNRQWpB1e2aw
    xSMhHMOb5ly2iMb56pSJJ5rpjA16jRik4j96KqOTtTtdYgvPTCD4QtnHSQu4Kq6
    igUyue0A+M5phK5qXkvD+hz5/M1kAyaaXe6zRkTHyL+4+32XuyfJ2UbnJzK6096
    7A6Lm05ULQHBLXYirdUyAUoIfhDH7V+KdJnDCmVr7Hrv/pAovUaI82tgEAAaXGd
    Ji3Qcy7Jm+3imMs/NCbd"
  },
  {
    "group_id":"85cdf393-613b-41bf-92fe-046318523af0",
```

```
      "contact_ids":"SZO5OyUALZuwE8ELq8Uc6nmaiAKU2cogIXj3ZYWF8KVn5bx4
      UPKH108AImJ0mkm5QKEunn2w1kp61J+EUUjVGWWCe1PmyPpvOXWOp1dBj9AKSr+
      LkrmY2lWk0zkZlZAxXFuoTKd1OpzH/teKRjboy/SDSyvwfY1d69l9M5zkFnpPEN
      5qP/V2LvlQYfiANu+ZQzTRvexd2qNng33e3JWM0+5D5xy43UH+X78uRba0lu0yn
      c5Gywev3+Jj3CZHNGE3"
    },
    {
      "group_id":"cf3b88bc-5961-49c6-a6e4-f925491e3f7e",
      "contact_ids":"G9etHXY4n4dmci6NMJi9D/jAiTRmz6rrJkvbU1UKtN11s1Mw
      7vpk3A/kVnt3+b3dCfqSvnJ0u2EIgeYHUIUZPnh8iVMm9eWJbUf7WRcISVPcdrr
      kcqgb7I3pB5YtRvUZ4KdRsbx2OYY745HHDnN+zA=="
    },
    {
      "group_id":"e960bb6e-660b-4ff6-8e0f-a840ce01a260",
      "contact_ids":"NW1A8Qw22LLziJaoMqjJaOf277WxytGM/3VPXlOcQ1O/+TXl
      LgUzIZZod7WI+RHGZSDVa7x29cXyfmr5JPyUVDLVYKhc+KmOlTJR+yxzm1Cu0xQ
      WY1W7ZehDlLqt0UgXhXGQ5hzmkDsq5TISNC3Jq9+mO0oY3ZA6gfkXAAmt+udh5Z
      tcbb2IKwVx4oAzyR4WiQOiKgZ7UjrjDxn5y+IyTgyDPPiJ0DOSYPIh18GYXLf5L
      YI2EmbAxVwEXZ8vvWUba0jFo1YHKVoGzSidhkipBQ=="
    },
    {
      "group_id":"a61a1144-08d7-4a95-9306-96918e0be333",
      "contact_ids":"6woWdnRrnJcAtoHnbQ0wSkPjIFqN+zYkWMJjEjBuyM8nMovl
      vEJ8JT6fKA2CLnaM2jvseMA2VyF6lixusvm7tD+IrpcXenAUFUhXju/h3/Xj/xj
      3v6b+o3bQ1dQMjLpAJXpH+9m/2KSVtL7Ps+mOyw=="
    },
    {
      "group_id":"5960a1a5-db1a-42bd-bb67-adfcff3f85c9",
      "contact_ids":"Ve983FBn/05TfV89sI6Pq4V2xFc9+pvuhwB586Io3FEBwPMk
      x21szaDRwSTYqrMSaupyoeXNiqn/mYiAekMes+QUa6u1ZcFavM1lgM6/nXw="
    },
    {
      "group_id":"daf8579e-a23e-4fa7-9b46-885158930741",
      "contact_ids":"YNHYyzbLXgm44Tn+WAXAZYv8zLhTSo2uRF4SM8uCVpwHi476
      j5MB76U7CrP71L6Iiy8uCKGkkqa/mvfSNzcH43jZ0T2sXps062Mm065NNpLznE7
      p0L+r40a0oGniPjq3cKPfV+jL3azFnxoVgGXGY2E6HboXPyuDmBzniZageFBNE4
      M0wyLCdx3LYpsbTERoIoNo3mfvJl2ykacwhKFzyGj+NJO7OZhNTNta53R5ZbU="
    }
  ]
},
"signature":"PKUx4vVALPBWF5Gn7tWBO1dMMAWVDuyKQxumgPcjZH1qgEqXqZs30k+K
NdlwmoDecmYyxkoSuet8z+K5Y6XM7ODdgHGwwIIJVJwnmd17C3JUM+jyHMVikPlhLQgFP
SXOoZHJBBK7frSQo9I4vavnNnLujQG9ZcrZy/Ap7JMimligNit5Yw/EBlmiIYVIblvip1
EvqA7/kBpXF2OtfgKlma9uMR5fA3+bzYDcjDiMyJ0qGVchtk4yFQ709mwVk8CFlh8HFor
IsvH70Nu7V9r8JJMYiI7YWgdprMxGZ/vcTYM+dFg02RVFSspybUVAh8Z1iPvRDVHlXNqW
u0QEzEAfrA=="
}
```

La HA envía una petición de clave a la ITPA, especificando el ID de la transacción, el número total de grupos, cuales son los grupos infectados, y cuál era el ID del LP que se consultó.


```
{
  "id":"HA",
  "info":{
    "transaction_ID":"cc92e749-4480-4f1d-9db6-978efcd46523",
    "total_groups":22,
    "infected_groups":[
      "2c43ac0e-f072-4aad-aeae-6988671b5746",
      "1e85ada3-bc1e-4442-bbd4-20e3b2e20691"
    ],
    "LP_ID":"LP1"
  },
  "signature":"azOpxZlXkLUwx6lqW/HEJeGvQIHCeGKuc5gmOS3r2/Xuft8nbKTZnl6/
  Pbbxdl5XdJBxarigMVCshWxUn8SC+oRaMUEg+nKJzFO3lLa+RljNq/xWLf7JU3yLZFR6l
  jHCZJJueg1QgO/hIqnbYpEay6dDLgFw9CeuQfs3qkohWbds6WAOxbtnCvLJrT0ekcteCl
  12ZT1M6qui2zZpBItWsCS8OSqkRmxPyBKNkXQ2TLvvwLuSIyGq+wEIcJlKXPsSEXc1tdY
  dmIrmV9iWcIymqc7pzFMA6x/Np0514XEOfbpmDotrQZpiW3nERMayRPMq6ejXD2sJZAQW
  L6DyShmZpQ=="
}
```


Recibida la informacion, la ITPA solicitará al LP las claves para desencriptar los contactos.


```
{
  "info":{
    "id":"ITPA",
    "transaction_ID":"cc92e749-4480-4f1d-9db6-978efcd46523"
  },
  "signature":"wlOdseb8LDJgfuQZWUQ1fumb7UD0k5KvDwp4P2ZYNXATDQxRnmK9UNK8
  WSc5uaf5viRcoJ7TnLdyH1ILrUeOahZxf+KOghUz98PMyTALW095buXwgxTShhylmT/r6
  pZY+0A8nczH7kP22t5SrcYppAH88nN52oUrTQoodY92Riy2pmIlX1ARhXfhp5EDBfdTpv
  yvPKM3J9x/j6DSZ7MSvnqmm6bIjqTdrDcyk4J+7rA3wqowPtQGwBnNqLSP+WLZ49hxRaw
  P4g8bkQs9g3UIL9ktdagmhme7bHrkn9pnKtaBX4d+N1bugbtsnWAUtoxpmQdIwRbg8Uho
  6uR1/uVN9w==",
  "id":"ITPA"
}
```


El LP responderá con la Clave y el IV.


```
{
  "info":{
    "transaction_ID":"cc92e749-4480-4f1d-9db6-978efcd46523",
    "keys":[
      {
        "group_id":"01e71438-d681-440f-9ebe-2f719157e08a",
        "aes_key":"dbf0d880a8d8de24d09eff2d3359c8416286aacb9f666f93cf33
            d46158899a06",
        "iv":"96b0874c1806d8dd441fcaa8f4491ff6"
      },
      {
```

```
  "group_id":"03fbc052-5134-4703-be20-c407c0835e9a",
  "aes_key":"c7646cb2117fd29a73871a9cfa80f8020d02ee414c79bf783cbe
      ccaba4a2e6ba",
  "iv":"764cc4012f81d90738cb5fb3df110af4"
},
{
  "group_id":"100a569f-2137-4711-b74c-7e25ae53dabb",
  "aes_key":"92fb488e762acde51d0d5ce9cf68c3e862e07db0e25d235e4074
      74739abaa9ba",
  "iv":"b764f39f9966ab02e839a819d3c8e5b2"
},
{
  "group_id":"19d4189a-a579-4634-b413-8a7e4f3e2468",
  "aes_key":"c0c40b5f5f0a350eeedd10a8856082ab0df3a069fa7474401ef5
      feb425773215",
  "iv":"defa401a2a175c7f7a6604b43aa03eba"
},
{
  "group_id":"1e85ada3-bc1e-4442-bbd4-20e3b2e20691",
  "aes_key":"2068c64ee3a05c3661afbe97747e44169785de604cf6503cc65b
      0ea0b0777a27",
  "iv":"63a07db34447eeca94f111955a10f85a"
},
{
  "group_id":"26debb37-f758-4f0c-af1f-ecb8c29d5b27",
  "aes_key":"541f1f0d9051c8d4f1a3ba140a4142c014d1409b09a2cbe6cf38
      e42d679bee14",
  "iv":"e1a2db8b1c67b9554cb609fbf5a5189a"
},
{
  "group_id":"2c43ac0e-f072-4aad-aeae-6988671b5746",
  "aes_key":"be463056c7ce14fcd3dce92b274c97893f2b669726024aa2a484
      1bfa64a3122a",
  "iv":"b2c3856d2afd93eb3b4e98f657abbb80"
},
{
  "group_id":"54b5d3e4-5c4c-497c-98c2-fd880a0aa04b",
  "aes_key":"fd42f6d85edc941550905bd7cdd32c67e3a42f408a2d1549d26d
      2b3635895809",
  "iv":"a30c6d0098f7217ccf9e7269e7a07c56"
},
{
  "group_id":"5960a1a5-db1a-42bd-bb67-adfcff3f85c9",
  "aes_key":"03f633c90ed401585d0a014456da123c200768c1ff0cdc399fd4
      aeb8783810a7",
  "iv":"be614bb14a3cd5fab10620c32ff1d61a"
},
{
  "group_id":"607ac506-588e-4a0d-ac8f-c6118fa608f5",
```

```
    "aes_key":"9f86747f3327e4e86c4544f682d83b0e949b6e4ad437913aa779
        603096cd9806",
    "iv":"0df4ec0fc5fe5077ccb7a18fe6bd6a35"
  },
  {
    "group_id":"6513caa1-86e7-4d3d-8f4a-e18090be2606",
    "aes_key":"0355f32bbe5ab055a90db35329c82012f9e89aa6c66bb0473c8c
        93c411e3276f",
    "iv":"1b42acdbef8fe02d1f537b431698d495"
  },
  {
    "group_id":"6c62ab11-8866-4dfc-9c66-5459b68d722e",
    "aes_key":"1e0e465138a67734b9adde87204a398e00ea5133afc2ade34feb
        3713c5493a5e",
    "iv":"13b7b1a65a76a1dd2fa54f9483328373"
  },
  {
    "group_id":"7749d184-c758-4b1d-935b-cfc3016bac7e",
    "aes_key":"ca7e03095a81e63256f77f0d90b6b0ee54956492978138988805
        d852faa2e0a1",
    "iv":"7ea6c1272ffbe1a5676e2cd9bc277f62"
  },
  {
    "group_id":"8303b685-f91d-4e1d-b110-9e799c175a4c",
    "aes_key":"249a64a7c553422a67310a8b5f0130b38eeb4333f705402bd6e8
        e6de228fbd7a",
    "iv":"44640c138e3d9f27b1880b129a01a480"
  },
  {
    "group_id":"85cdf393-613b-41bf-92fe-046318523af0",
    "aes_key":"e3e5278ff69a25bec2af00c1f69120ac72f37da45270656b977f
        45457499e18e",
    "iv":"ed79a52af5f9400fdca5210d45cd0064"
  },
  {
    "group_id":"a61a1144-08d7-4a95-9306-96918e0be333",
    "aes_key":"8e76896d4f453a45d11d667460d7d6bdadaaa08a48d90f9caf85
        7cfb5d2ef727",
    "iv":"7d0c8a508afbb240626c53aecca6f7bf"
  },
  {
    "group_id":"cac5d3ed-d5e1-4ca4-9d97-c57ea390ba99",
    "aes_key":"4f271c40151d5982e7958947c44ab3dbb8c503572f88213b5eee
        84d80b4acc2a",
    "iv":"65b72d8c1fff5d9b2b46ccad7769fc71"
  },
  {
    "group_id":"cf3b88bc-5961-49c6-a6e4-f925491e3f7e",
    "aes_key":"0ece50f67905f47f850273562af971b5c24ad04fb5766f7170dd
```

```
            66aea4c0e170",
        "iv":"bbb3920f27327b543ddfd8fc9e4169de"
      },
      {
        "group_id":"d2691a90-012d-40f9-91f2-6abf79f01443",
        "aes_key":"aacf4153249b2da7d5c6f98374b47118e5f28e6ac4a34a5092c0
            eb0d1b767285",
        "iv":"eb81d0420dfccc435b38bf67ac00fca2"
      },
      {
        "group_id":"daf8579e-a23e-4fa7-9b46-885158930741",
        "aes_key":"894220016aab3e1d77abade8e2fddc1ab7f3044f8cbfa56303f9
            82157995479e",
        "iv":"58ea2a0f7e0ddc1c4b9ffceca6253e88"
      },
      {
        "group_id":"e960bb6e-660b-4ff6-8e0f-a840ce01a260",
        "aes_key":"2890ac60629f156055fac9aa6cf2da21301e5660e156564f8b36
            c1a72fd44a26",
        "iv":"313f5e5cedfb4466ec8cfb363a788ba6"
      },
      {
        "group_id":"f21c85eb-319f-4934-8053-b0f873893223",
        "aes_key":"3ec64b5c8b62770f76e98916ec41128462f7b7a26a5c9a12653c
            df924cf02726",
        "iv":"33445f835d1612f0fe5925b076288a32"
      }
    ]
  },
  "id":"LP1",
  "signature":"lKY4EsbTX3nX7rtMNXWTQbTWB35ameUTerHEHs9VB9TGtQ83btCCH9yL
  AHx4ePgVewm+olIhP2oVxfQPr7lc420p9dODryS74UTiRl0f72PD4kZLpinH3y75QuVej
  AeQO40z9pcI8HI7Owu8oTcT/wEEe67Q5EIxnqrEA+YVXdeicf4D90nrihIuLsLDRwk5bZ
  nXTWMs1DZlqW8rH2W8jDPJYZX6e0K7rFXRGZ2TZqbnsN/3YFBDOyKeSjiC1TtvAIpx9IZ
  JAKeiLcaLE4wwGoX+cjkSvH8RKwSk5EZPXpoT/WcJYu0eIDGRL8IhgGSTNAg4AJl6TRqJ
  cEVSVDDfow=="
}
```


La ITPA comprobará que el número de grupos coincide, y devolverá sólo las claves para desencriptar la información de los grupos infectados.


```
{
  "info":{
    "transaction_ID":"cc92e749-4480-4f1d-9db6-978efcd46523",
    "keys":[
      {
        "group_id":"1e85ada3-bc1e-4442-bbd4-20e3b2e20691",
        "aes_key":"2068c64ee3a05c3661afbe97747e44169785de604cf6503cc65b
            0ea0b0777a27",
```

```
        "iv":"63a07db34447eeca94f111955a10f85a"
      },
      {
        "group_id":"2c43ac0e-f072-4aad-aeae-6988671b5746",
        "aes_key":"be463056c7ce14fcd3dce92b274c97893f2b669726024aa2a484
            1bfa64a3122a",
        "iv":"b2c3856d2afd93eb3b4e98f657abbb80"
      }
    ]
  },
  "id":"ITPA",
  "signature":"HA469U9kYE+PadUL4Ofnei2kD6gzrYc61bDXid6Su9C4WX+L3n6xiUJu
  WIMRAE2T8w4CNRh3k5ZtrJ7TzLP23Fhka0/QCxtSV0Z5qDXukFHRehzVgr/FQnIDE14qx
  V8Jjk2Fcay5BiRrUfaGPeztAoiCm6tagd1W0pJ4RjXWk92g6wchOvkzlJkicfEE/m1ngF
  YPT6KpK/Oxkx2ShX23ZIY4xCRPkpmYJzY0faqIOQgd6DwxPO9wkBnoh5H2CY7f4fOP/cD
  bxuhAE2Z46dFmLDFUgJEqKrih1mKPrFOIekoE1u65eTyYGw23ReHxzo1qy7mshbCeqrXE
  Y2ei1XSvUA=="
}
```


Una vez que la Autoridad Sanitaria reciba las claves de los grupos infectados, podrá descifrarlas.

Las tablas 2, 3 y 4 muestran el estado de las tablas de la transacción cc92e749-4480-4f1d-9db6-978efcd46523.

Tabla 2. Base de datos del IDP.

transaction_id	health_authority	phones_requested	creation_date
cc92e749-4480-4f1d-9db6-978efcd46523	HA	100	2022-10-03 09:32:45

Tabla 3. Base de datos del ITPA.

transaction_id	ha	lp	transaction_timestamp	total_groups	infected_groups	result
cc92e749-4480...	HA	LP1	2022-10-03 09:32:45	22	2	Transaction OK

Tabla 4. Base de datos del Proveedor de Localización.

transaction id	ha	group id	aes key	iv	creation date
cc92e749-4480...	HA	01e71438-d681-440f-9ebe-2f719157e08a	dbf0d88...	96b0874...	2022-10-03 09:32:45
cc92e749-4480...	HA	03fbc052-5134-4703-be20-c407c0835e9a	c7646cb...	764cc40...	2022-10-03 09:32:45
cc92e749-4480...	HA	100a569f-2137-4711-b74c-7e25ae53dabb	92fb488...	b764f39...	2022-10-03 09:32:45
cc92e749-4480...	HA	19d4189a-a579-4634-b413-8a7e4f3e2468	c0c40b5...	defa401...	2022-10-03 09:32:45
cc92e749-4480...	HA	1e85ada3-bc1e-4442-bbd4-20e3b2e20691	2068c64...	63a07db...	2022-10-03 09:32:45
cc92e749-4480...	HA	26debb37-f758-4f0c-af1f-ecb8c29d5b27	541f1f0...	e1a2db8...	2022-10-03 09:32:45
cc92e749-4480...	HA	2c43ac0e-f072-4aad-aeae-6988671b5746	be46305...	b2c3856...	2022-10-03 09:32:45
cc92e749-4480...	HA	54b5d3e4-5c4c-497c-98c2-fd880a0aa04b	fd42f6d...	a30c6d0...	2022-10-03 09:32:45
cc92e749-4480...	HA	5960a1a5-db1a-42bd-bb67-adfcff3f85c9	03f633c...	be614bb...	2022-10-03 09:32:45
cc92e749-4480...	HA	607ac506-588e-4a0d-ac8f-c6118fa608f5	9f86747...	0df4ec0...	2022-10-03 09:32:45
cc92e749-4480...	HA	6513caa1-86e7-4d3d-8f4a-e18090be2606	0355f32...	1b42acd...	2022-10-03 09:32:45
cc92e749-4480...	HA	6c62ab11-8866-4dfc-9c66-5459b68d722e	1e0e465...	13b7b1a...	2022-10-03 09:32:45
cc92e749-4480...	HA	7749d184-c758-4b1d-935b-cfc3016bac7e	ca7e030...	7ea6c12...	2022-10-03 09:32:45
cc92e749-4480...	HA	8303b685-f91d-4e1d-b110-9e799c175a4c	249a64a...	44640c1...	2022-10-03 09:32:45
cc92e749-4480...	HA	85cdf393-613b-41bf-92fe-046318523af0	e3e5278...	ed79a52...	2022-10-03 09:32:45
cc92e749-4480...	HA	a61a1144-08d7-4a95-9306-96918e0be333	8e76896...	7d0c8a5...	2022-10-03 09:32:45
cc92e749-4480...	HA	cac5d3ed-d5e1-4ca4-9d97-c57ea390ba99	4f271c4...	65b72d8...	2022-10-03 09:32:45
cc92e749-4480...	HA	cf3b88bc-5961-49c6-a6e4-f925491e3f7e	0ece50f...	bbb3920...	2022-10-03 09:32:45
cc92e749-4480...	HA	d2691a90-012d-40f9-91f2-6abf79f01443	aacf415...	eb81d04...	2022-10-03 09:32:45
cc92e749-4480...	HA	daf8579e-a23e-4fa7-9b46-885158930741	8942200...	58ea2a0...	2022-10-03 09:32:45
cc92e749-4480...	HA	e960bb6e-660b-4ff6-8e0f-a840ce01a260	2890ac6...	313f5e5...	2022-10-03 09:32:45
cc92e749-4480...	HA	f21c85eb-319f-4934-8053-b0f873893223	3ec64b5...	33445f8...	2022-10-03 09:32:45

Análisis de rendimiento de la solución propuesta

Nuestra solución requiere que su implementación pueda escalar a un número elevado de teléfonos. Por ello se ha ejecutado la simulación con diferentes parámetros para comprobar si el sistema puede escalar, es decir, cuánto tarda la ejecución del algoritmo en diferentes circunstancias. Para cada uno de los escenarios, ejecutamos el sistema y registramos el tiempo varias veces, y luego calculamos el tiempo medio de ejecución.

En realidad, el Rastreo Digital de Contactos llevará más tiempo, ya que estas simulaciones no incluyen el tiempo necesario para realizar el rastreo real de contactos en los proveedores de localización: obtener los contactos cercanos asociados a cada uno de los teléfonos. Por lo tanto, el tiempo total necesario para ejecutar este sistema es el siguiente:

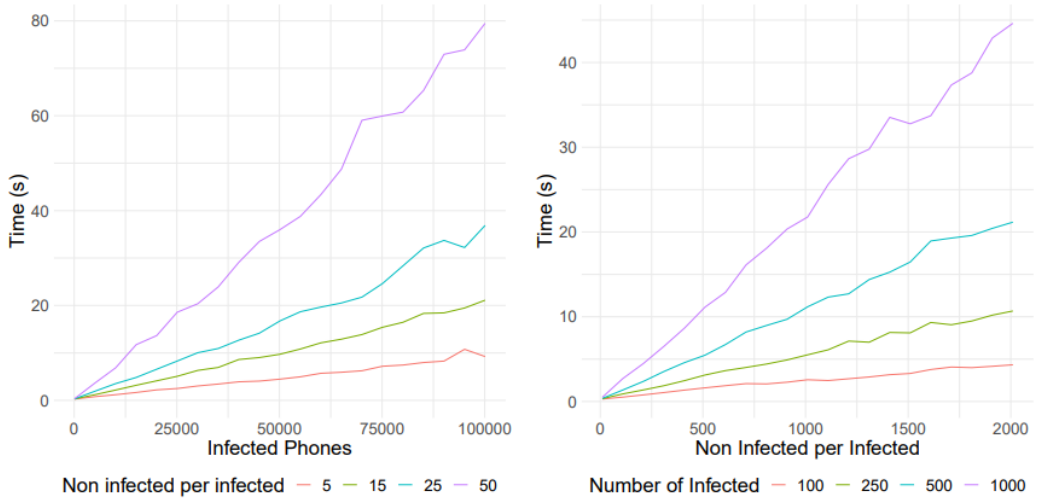
$$TiempoTotal = t_0 + CTR_{(M+N)} + IDR_N + NetworkDelays \quad (1)$$

Donde $t0$ representa el tiempo que necesitan los sistemas para preparar, enviar y procesar las diferentes solicitudes del sistema, a excepción de la Solicitud de Rastreo de Contactos, de $M + N$ teléfonos en el Proveedor Local, y el tiempo que necesita el IDP para recuperar N teléfonos reales. Este tiempo cambiará en función del estado de la red ($Network\ Delays$). Por lo tanto, el tiempo representado en los siguientes escenarios es el $t0$, a excepción del escenario C que también incluye los $Network\ Delays$. Aunque el $t0$ cambiará dependiendo de las capacidades del dispositivo que ejecute cada uno de los servicios.

Para simplificar las mediciones sólo hay un IDP y un LP que la HA puede contactar. En un entorno real, sería mejor consultar a varios LPs.

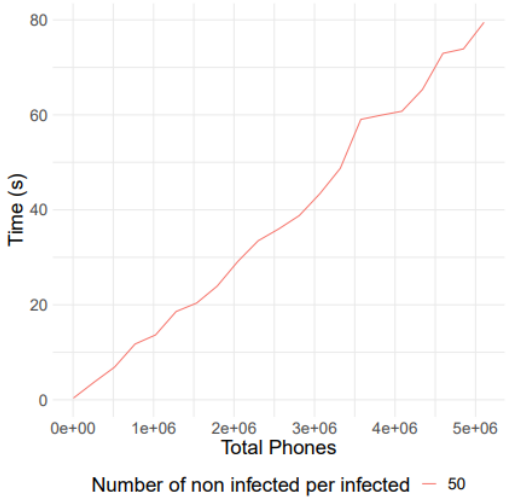
Número de contactos a rastrear

La figura 2 muestra diferentes escenarios. El primero (2a) muestra cómo el tiempo necesario para ejecutar el algoritmo aumenta el número de teléfonos infectados, con diferentes números de N / M. La figura 2c representa el mismo escenario cuando N / M = 50 para mostrar el número total de teléfonos: se tardarán 80 segundos en procesar una solicitud de 100000 personas infectadas con más de 50000000 teléfonos solicitados a un Proveedor de Localización.



(a) Tiempo de respuesta de la solución con un número creciente de infectados

(b) Tiempo de respuesta de la solución con un número creciente de no infectados por infectado



(c) Tiempo de respuesta de la solución con un incremento del número total de teléfonos (IDs)

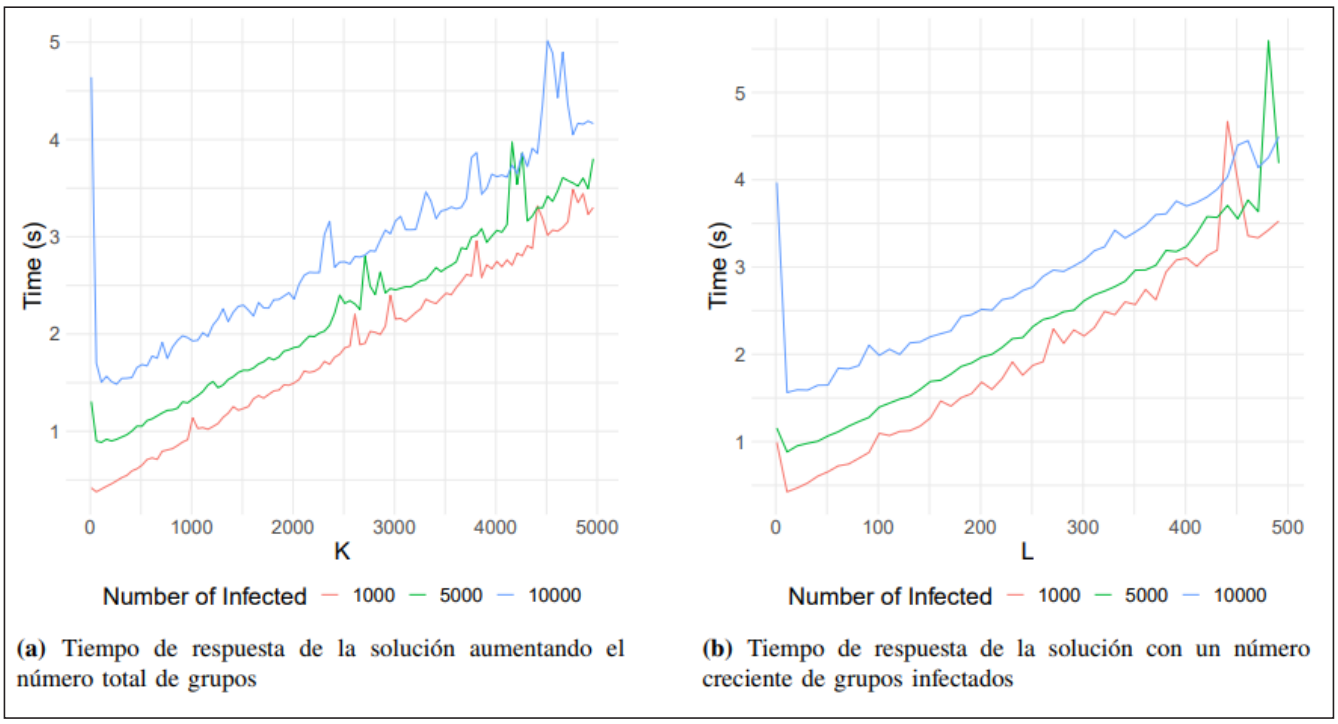
Figura 2. Evaluacion de rendimiento de las solución propuesta.

Número de grupos

Ejecutamos diferentes simulaciones, con diferentes valores de M (1000, 5000, 10000), y N = 10 M para ver el efecto en el rendimiento. Las figuras 3a y 3b muestran cómo el aumento de la cantidad de grupos se traduce en un mayor tiempo de ejecución de los valores.

La figura 3a varía entre K = 2 y K = 5000, mientras que la figura 3b va desde L = 1 hasta cerca de L = 500.

Como se observa en las figuras, al aumentar el número de grupos se tarda más en procesar las solicitudes, con la excepción de sólo dos grupos en total.



(a) Tiempo de respuesta de la solución aumentando el número total de grupos

(b) Tiempo de respuesta de la solución con un número creciente de grupos infectados

Figura 3. Rendimiento con diferente número de grupos para N = 10 · M.

Transacción en un entorno completo no contenido

Desplegamos el sistema: 1 LP, 1 IDP, y 1 ITPA en máquinas en diferentes redes y recursos limitados (por ejemplo, raspberry pi y VPS) para ver cómo se comporta el sistema en una situación real. Como se ve en la Figura 4, el sistema escala lo suficientemente bien incluso con varios millones de teléfonos en una sola transacción.

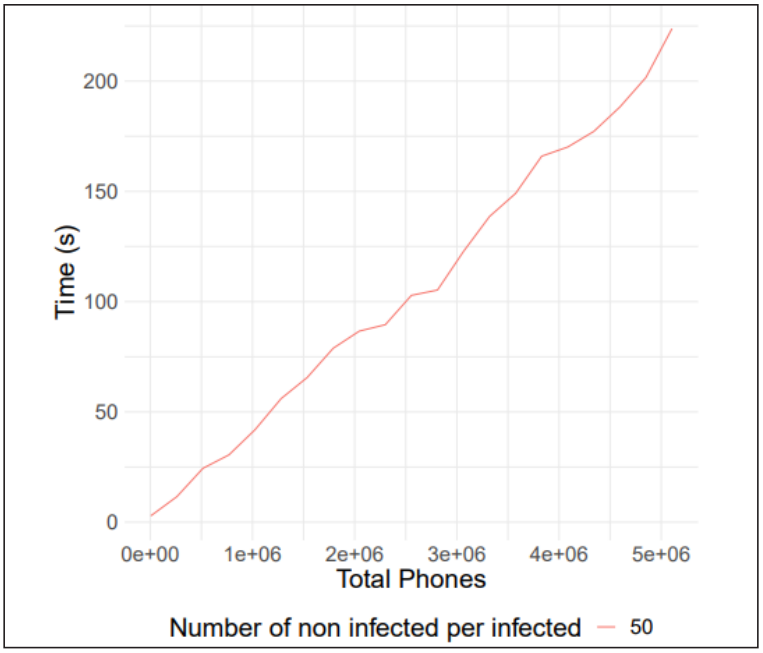


Figura 4. Tiempo de respuesta de la solución en un entorno real.

Los resultados sugieren que este sistema de comunicación aumenta linealmente con el número de teléfonos solicitados. Aunque el tiempo requerido podría considerarse muy alto, es necesario entender que el sistema no necesita tener un tiempo de ejecución muy bajo. Además, el tiempo para realizar el rastreo de contactos real en el LP podría requerir aún más tiempo.

Conclusiones

El único enfoque de rastreo digital de contactos utilizado para luchar contra la pandemia COVID-19 en la mayoría de países desarrollados consistió en la utilización de aplicaciones móviles que aprovechan la tecnología Bluetooth para identificar encuentros de proximidad. En este artículo, hemos destacado la principal limitación de este enfoque: la falta de una adopción suficiente de este tipo de aplicaciones móviles, lo que ha hecho fracasar todos los intentos en este sentido.

Debido a la importancia que pueden tener las soluciones digitales de rastreo de contactos para ayudar a combatir futuras pandemias, es obligación de los investigadores, las autoridades de salud pública y las empresas tecnológicas explorar alternativas para encontrar una solución eficaz de rastreo de contactos. Como ejemplo de este esfuerzo de exploración, en este artículo proponemos una primera solución alternativa prometedora para el rastreo de contactos que invita a las autoridades sanitarias y a las empresas BigTechs a cooperar juntas.

Proponemos utilizar datos de geolocalización escalables y precisos ya existentes, que probablemente sirvan para construir una solución digital eficiente de localización de contactos

Proponemos utilizar datos de geolocalización escalables y precisos ya existentes, que probablemente sirvan para construir una solución digital eficiente de localización de contactos. La alternativa presentada a las actuales aplicaciones de localización de contactos se basa en la alta tasa de adopción ya disponible de la información de localización en tiempo real procedente de miles de millones de ciudadanos de todo el mundo. Esta información se almacena en bases de datos de grandes empresas tecnológicas que ya cuentan con un enorme número de usuarios activos. Además, esta solución tiene en cuenta las ubicaciones interiores y exteriores, abordando también la transmisión aérea demostrada en el caso del COVID-19. Esta propuesta define una arquitectura que aprovecha tales datos y proporciona suficientes garantías de privacidad a los ciudadanos.

Por último, hemos implementado nuestra solución sobre HTTPS con el objetivo de ver si nuestra solución es escalable en términos de volumen de datos y tiempo de respuesta incluso en el caso de manejar peticiones incluyendo millones de identificadores. Esta implementación proporciona cifrado de extremo a extremo, así como autenticación, ya que todos los mensajes deben estar firmados. Este sistema de comunicación ha sido probado en un entorno real, en dispositivos con recursos muy limitados y situados en diferentes redes. Los resultados muestran que la solución propuesta escala de manera eficiente para su uso en el rastreo de contactos digital.

Contribuciones de los autores

Los autores participaron igualmente en la elaboración del manuscrito y aprobaron la versión final presentada.

Financiación

Este trabajo es parte del acuerdo entre la Comunidad de Madrid y la Universidad Carlos III de Madrid para la financiacion de proyectos de investigación del SARS-CoV-2 y la enfermedad COVID-19, para el proyecto «Multi-source and multi-method prediction to support COVID-19 policy decision making», que ha sido financiado con los fondos REACT-EU del fondo de desarrollo regional Europeo a «way of making Europe».

Declaración de disponibilidad de datos

El codigo usado para implementar la solución propuesta se encuentra disponible en https://github.com/fcaravaca/DigitalContactTracing

Conflicto de interés

Los autores declaran que no hay conflicto de interés.

Referencias bibliográficas

Aleta, A., Mart´ın-Corral, D., Bakker, M. A., Piontti, A. P. y., Ajelli, M., Litvinova, M., . . . Moro, E. (2020) Quantifying the importance and location of SARS-CoV-2 transmission events in large metropolitan areas. *medRxiv*. Retrieved from https://www.medrxiv.org/content/early/2020/12/17/2020.12.15.20248273 doi: 10.1101/2020.12.15.20248273

Apple and Google. (2021). *Exposure Notifications: Using technology to help public health authori- ties fight COVID-19.* (Accessed on: February 26, 2021. https://www.google.com/covid19/ exposurenotifications/)

Data World Bank. (2020). *Total Population.* (Accessed on: December 27, 2020 https://data.worldbank.org/indicator/SP.POP.TOTL)

Demographics of Mobile Device Ownership and Adoption in the United States. (2020, Jun). Pew Research Center. (Accessed on: December 27, 2020 https://www.pewresearch.org/internet/ fact-sheet/mobile/)

Dimoco. (2020, 04). *Market Insights.* (Accessed on: December 27, 2020 https://dimoco.eu/ carrierbilling/ coverage/)

EU. (2016). *Regulation (EU) 2016/679 of the European Parliament (General Data Protection Regulation)*. European Union. (Accessed on: April 22, 2020 http://eur-lex.europa.eu/eli/reg/2016/679/ oj)

Facebook. (2020). *Facebook Marketing API.* (Accessed on: December 27, 2020 https://developers.facebook.com/docs/marketing-apis)

FDVT. (2021, 02). *Contact tracing apps: number of downloads sources across countries.* (Accessed on: February 28, 2021 https://fdvt.org/files/COVID APPS SOURCES.pdf)

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Do¨rner, L., . . . Fraser, C. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*, *368*(6491). Retrieved from https://science.sciencemag.org/content/368/6491/eabb6936 doi: 10.1126/science.abb6936

Google. (2020, Mar). *Wi-Fi location: ranging with RTT.* (Accessed on: April 20, 2020 https:// developer.android.com/guide/topics/connectivity/wifi-rtt)

GPS.gov. (2017, Dec). *GPS Accuracy.* (Accessed on: April 20, 2020 https://www.gps.gov/systems/ gps/performance/accuracy/)

Hinch et al., R. (2020). Effective configurations of a digital contact tracing app: A report to NHSX. *GitHub*. (https://github.com/BDI-pathogens/covid-19 instant tracing/ blob/master/Report)

Lednicky, J. A., Lauzardo, M., Fan, Z. H., Jutla, A., Tilly, T. B., Gangwar, M., . . . Wu, C.-Y. (2020). Viable SARS-CoV-2 in the air of a hospital room with COVID-19 patients. *medRxiv*. Retrieved from https://www.medrxiv.org/content/early/2020/08/04/2020.08.03.20167395 doi: 10.1101/2020.08.03.20167395

Mokbel, M., Abbar, S., & Stanojevic, R. (2020, October). Contact Tracing: Beyond the Apps. *SIGSPATIAL Special*, *12*(2), 15–24. Retrieved from https://doi.org/10.1145/3431843.3431846 doi: 10.1145/3431843.3431846

Nakamoto, I., Wang, S., Guo, Y., & Zhuang, W. (2020). A QR Code–Based Contact Tracing Framework for Sustainable Containment of COVID-19: Evaluation of an Approach to Assist the Return to Normal Activity. *JMIR mHealth and uHealth*, *8*(9), e22321.

Prather, K. A., Marr, L. C., Schooley, R. T., McDiarmid, M. A., Wilson, M. E., & Milton, D. K. (2020). Airborne transmission of SARS-CoV-2. *Science*, *370*(6514), 303–304. Retrieved from https:// science.sciencemag.org/content/370/6514/303.2 doi: 10.1126/science.abf0521

Rahman, M. T., Khan, R. T., Khandaker, M. R., Sellathurai, M., & Salan, M. S. A. (2020). An automated contact tracing approach for controlling COVID-19 spread based on geolocation data from mobile cellular networks. *IEEE Access*, *8*, 213554–213565.

Reichert, L., Brack, S., & Scheuermann, B. (2020). Privacy-Preserving contact tracing of COVID-19 patients.*IACR Cryptol. ePrint Arch.*, *2020*, 375.

Rodríguez, P., Gran˜a, S., Alvarez-Leo´n, E. E., Battaglini, M., Darias, F. J., Herna´n, M. A., . . . others (2021). A population-based controlled experiment assessing the epidemiological impact of digital contact tracing. *Nature communications*, *12*(1), 1–6.

Salathé, M., Althaus, C. L., Anderegg, N., Antonioli, D., Ballouz, T., Bugnion, E., . . . von Wyl,V. (2020). Early Evidence of Effectiveness of Digital Contact Tracing for SARS-CoV-2 in Switzerland. *medRxiv*. Retrieved from https://www.medrxiv.org/content/early/2020/10/ 04/2020.09.07.20189274 doi: 10.1101/2020.09.07.20189274

Scientific Brief: SARS-CoV-2 and Potential Airborne Transmission. (2020, Oct). Centers for Disease Control and Prevention (CDC). (Accessed on: December 27, 2020 https://www.cdc.gov/coronavirus/ 2019-ncov/more/ scientific-brief-sars-cov-2.html)

StatCounter Global Stats. (2020). *Mobile Operating System Market Share Worldwide.* (Accessed on: December 27, 2020 https://gs.statcounter.com/os-market-share/mobile/)

StraitTimes. (2020, April). *Call for more people to use contact-tracing app.* (Accessed on: April 20, 2020 https://www.straitstimes.com/singapore/call-for-more-people-to-use-contact-tracing-app)

Swiss Federal Statistical Office. (2020). *Swiss Covid App Monitoring.* (Accessed on: December 27, 2020 https:// www.experimental.bfs.admin.ch/expstat/en/home/innovative-methods/ swisscovid-app-monitoring.assetdetail.13407769.html)

Wymant, C., Ferretti, L., Tsallis, D., Charalambides, M., Abeler-Do¨rner, L., Bonsall, D., . . . others (2021). The epidemiological impact of the NHS COVID-19 App. *Alan Turing Institute*.