Sistema para la gestión automática de las políticas de privacidad y uso de las cookies

Cristòfol Daudén-Esmel, Jordi Castellà-Roca and Alexandre Viejo
Universitat Rovira i Virgili, Departament d'Enginyeria Informàtica i Matemàtiques, CYBERCAT
Av. Països Catalans 26, E-43007 Tarragona, Spain
{critofol.dauden, jordi.castella, alexandre.viejo}@urv.cat

***Resumen*—El incremento en el uso de Internet implica que cada vez más usuarios compartan información sensible sin darse cuenta de que se exponen a riesgos innecesarios. Para ello, la UE propuso el Reglamento General de Protección de Datos (RGPD), según el cual el consentimiento para la obtención y procesamiento de los datos personales de los usuarios debe darse de forma clara e inequívoca. Un claro ejemplo donde esto se lleva a cabo, son los pop-ups que aparecen mientras navegamos por internet. Sin embargo, una correcta configuración del consentimiento requiere de un esfuerzo para el usuario, llevándolo en la mayoría de casos a la aceptación todas las condiciones sin siquiera leerlas. Así, en este proyecto realizamos una propuesta de marco para la gestión automática de las políticas de privacidad y uso de las cookies de los usuarios, mediante el uso de contratos inteligentes y la tecnología blockchain.**

***Index Terms*—RGPD, criptología, seguridad de la información, blockchain, contratos inteligentes**

I. Introducción

El uso de las tecnologías de información y comunicación (TIC) ha seguido crecido en los últimos años[1]. La popularidad de las redes sociales y la digitalización de las gestiones online [2] han contribuido significativamente a ello. No obstante, uno de los efectos colaterales de esta situación es que los usuarios comparten información sensible por Internet sin darse cuenta de que puede afectar a su seguridad, es decir, sus datos personales les exponen a riesgos innecesarios [1].

Para que los usuarios sean sensibles a esta exposición y puedan prevenirla es importante que sepan en que consiste su privacidad de datos, cómo protegerla y proporcionarles herramientas con las que puedan ejercer este derecho.

En este sentido, una de las claves es el consentimiento de datos, regulado por el Reglamento General de Protección de Datos (RGPD)[2]. Según esta normativa, el consentimiento para la obtención y procesamiento de los datos personales de los usuarios debe darse de forma clara e inequívoca por parte del usuario interesado, el cual debe haber recibido información detallada acerca de la gestión de sus datos por parte del servicio o página online.

Un claro ejemplo, en donde se pide un consentimiento para la recaudación y uso de datos, son los pop-ups que aparecen mientras navegamos por internet[3]. En ellos se informa al usuario del uso que hacen los proveedores de servicio sobre los datos que recaban mientras se navega por sus páginas. Con el acuerdo de los usuarios, estos proveedores de servicio y sus socios, usan cookies o tecnologías similares para almacenar, acceder y procesar datos personales como: almacenar o acceder a información en un dispositivo, anuncios y contenido personalizados, medición de anuncios y del contenido, información sobre el público y desarrollo de productos, datos de localización geográfica precisa e identificación mediante las características de dispositivos, uso de cookies técnicas o de preferencias, etc.

De acuerdo con la legislación previamente mencionada, el usuario puede retirar su consentimiento u oponerse al procesamiento de datos basado en intereses legítimos en cualquier momento. Sin embargo, tal como se menciona en estos mismos pup-ups, esto puede provocar un incorrecto funcionamiento de ciertos servicios e incluso el no acceso a la plataforma web.

En este proceso de aceptación de las condiciones para la recolección y uso de datos, los usuarios, por norma general, pueden aceptar todos los usos con un solo clic u optar por una configuración de usos más personalizada, rechazando algunos de estos. La segunda opción, sin embargo, requiere de un esfuerzo extra para el usuario, ya que debe leer detenidamente cada uno de estos usos y aceptar y/o rechazar cada uno de ellos individualmente. De este modo, en la mayoría de casos, los usuarios aceptan todas las condiciones sin siquiera leerlas[4].

Como ya hemos comentado, este proceso se debe llevar a cabo cada vez que un usuario quiera acceder a un nuevo sitio web, por lo que resulta muy complicado para este, tener conocimiento/recordar de todos aquellos lugares donde ha dado su consentimiento y de que tipo es este (ha aceptado todas las condiciones, las ha rechazado o ha optado por una configuración personalizada). Además, estos sistemas de gestión de consentimientos siguen una estrategia centralizada guardando estos permisos en los servidores de los proveedores de servicios, de forma que el usuario debe confiar en que dicho proveedor es honesto en lo referente a sus preferencias.

Con todo lo que hemos mencionado podemos extraer una serie de necesidades:

i) Se requiere de una herramienta que de forma automática y transparente gestione las preferencias del uso de las cookies y del nivel de privacidad que desea cada usuario. De este modo, se evitará el "Aceptar Todo" al cual hacen uso la mayoría de los usuarios para acceder al contenido web deseado con la mayor brevedad posible.

ii) Se requiere de una alternativa a esta centralización de la gestión del consentimiento en los servidores de

[1]Individuals - internet use [ISOC_CI_IFP_IU] https://ec.europa.eu/eurostat/databrowser/bookmark/1614ab44-2592-48ee-99b1-01237e038e78

[2]Individuals - internet activities [ISOC_CI_AC_I] https://ec.europa.eu/eurostat/databrowser/bookmark/0a0bfe7e-85a1-4a0c-84d6-fc2f5bf006ab

[3]Didomi https://www.didomi.io/

[4]76 % Ignore Cookie Banners https://www.advance-metrics.com/en/blog/76-ignore-cookie-banners-the-user-behavior-after-30-days-of-gdpr/

los proveedores de servicio. Como alternativa, algunos trabajos ([3], [4], [5], [6], [7], [8], [9], [10], [11]) sugieren descentralizar estos consentimientos mediante su inclusión en Contratos Inteligentes (SCs), los cuales son ejecutados en una blockchain (se realiza el "*deploy*" del contrato inteligente).

Cabe mencionar, que para realizar el *deploy* de un SC en una blockchain se requiere de una pareja de claves (una clave pública y una privada) para calcular una firma digital. El problema está en que si un usuario usa siempre la misma pareja de claves para firmar cada uno de los SCs sobre el consentimiento de uso de sus datos personales, un adversario podría re-identificar al usuario al cual pertenece una clave pública concreta. Esto se llevaría a cabo mediante el análisis de todas las plataformas web a las que ha accedido. Además, una vez identificado el usuario, se puede extraer información sensible del mismo, analizando las mismas páginas web a las que ha accedido.
Teniendo esto en cuenta, las propuestas previamente mencionadas no consideran o no presentan ninguna solución para la protección de la privacidad de los usuarios, en lo referente al uso de la misma pareja de claves para realizar el *deploy* de los SCs.

Para evitar esta situación, proponemos el uso de una nueva pareja de claves cada vez que se genera un nuevo SC entre un usuario y un nuevo proveedor de servicio. Así, se requiere de un sistema que permita la generación y gestión de todas estas parejas de claves de forma automática y transparente al usuario. Este sistema debe ser multi-plataforma, de modo que permita al usuario hacer uso de estas claves desde cualquier equipo para gestionar los SCs que contienen estos/sus consentimientos sobre el uso de sus datos personales por los proveedores de servicio.

I-A. Contribución

En este trabajo realizamos una propuesta de marco para la gestión automática de las políticas de privacidad y uso de las cookies de los usuarios. De acuerdo con las necesidades mencionadas anteriormente, este marco:

a) gestiona de forma **automática** y **transparente** la aceptación de políticas y uso de las cookies en cuanto el usuario navega por internet;
b) registra de forma **descentraliza** estas políticas aceptadas mediante el uso de contratos inteligentes y la tecnología blockchain, y;
c) protege la **privacidad** del usuario en el caso de que un atacante pretendiese identificarlo y extraer información sensible sobre el mismo.

En cuanto al punto a), existen plug-ins que se encargan de la automática aceptación de las cookies en navegadores web [5] [6] [7]. Estos, sin embargo, se limitan a la simple interacción con el "*pop-up*"de la web. Del mismo modo, como ya hemos mencionado, respecto al punto b), también existen propuestas para la gestión del consentimiento de un usuario a proveedores de servicio mediante SCs.

[5]Ninja Cookie https://addons.mozilla.org/es/firefox/addon/ninja-cookie/
[6]Super Agent https://addons.mozilla.org/es/firefox/addon/super-agent/
[7]Auto Cookie Optout https://addons.mozilla.org/es/firefox/addon/auto-cookie-optout/

Así, en este trabajo combinamos tecnologías existentes que abordan los puntos a) y b), y nos centramos en el diseño de un protocolo para la generación y gestión de las parejas de claves necesarias para completar el proceso de firma digital para el desarrollo de los contratos inteligentes en la blockchain. De este modo mantenemos la privacidad de los usuarios, en un marco para la automática gestión de las políticas de privacidad y uso de las cookies de los usuarios, en cuanto estos navegan por internet.

El resto del trabajo está organizado de la siguiente forma: en la sección II se muestra el marco propuesto y se explica el protocolo para la gestión de claves diseñado; en la sección III se analiza la propuesta presentada y; finalmente, se concluye el trabajo en la sección IV.

II. PROPUESTA

En esta sección presentamos nuestro marco para la gestión automática de las políticas de privacidad y uso de las cookies de los usuarios. Primero, mostramos una visión general del marco y como funciona y, después, detallamos el protocolo desarrollado para la creación y gestión de las claves criptográficas.

II-A. Visión general del marco

Una visión general de la arquitectura propuesta se muestra en la Figura 1. Como se puede observar, el usuario tiene dos puntos de acceso al sistema propuesto. Por un lado, un plug-in que se debe instalar en el navegador web. Este se encarga de la gestión de las políticas y el uso de las cookies, y de la generación de los contratos inteligentes donde estas quedan registradas. Por otro lado, una aplicación móvil desde la cual los usuarios tienen el control sobre los proveedores de servicio a los que han dado su consentimiento para el procesamiento de datos, cuáles son estos permisos y gestionar los contratos inteligentes generados por el plug-in (e.j. restringiendo el uso de los datos).
Otro componente esencial del sistema es el *Key Storage*, donde se guardan todas las parejas de claves generadas por el plug-in para poder realizar el *deploy* de los SCs en la blockchain. Este *Key Storage* consiste en una Base de Datos Personal Online (Personal Online Database - POD) la cual permite el almacenaje seguro y gestión de dichas claves mediante el protocolo diseñado.
Finalmente, el último componente es la blockchain sobre la que se llevará a cabo el *deploy* de los contratos inteligentes.

II-B. Protocolo

El protocolo propuesto se divide en tres fases: i) fase de inicialización o set-up, donde se instala la aplicación móvil y el plug-in en el navegador; ii) fase de navegación, donde el usuario visita distintos sitios web y; iii) fase de control, donde el usuario puede consultar en que sitios web ha dado su consentimiento para el procesamiento de sus datos, de que tipo es este y revocar dicho permiso en el caso que lo crea oportuno. Una visión más general de este protocolo se puede observar en la Figura 2.

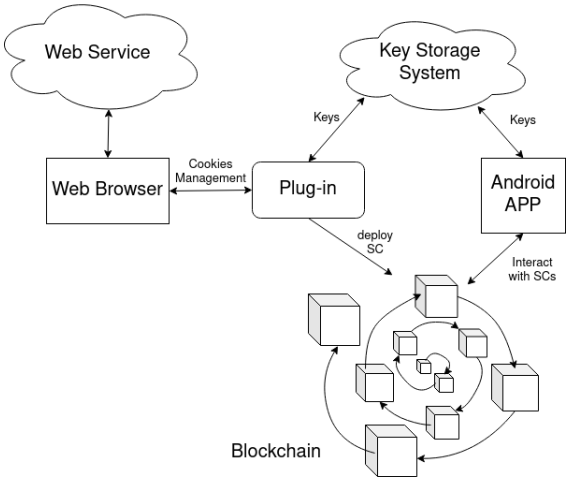


Figura 1. Framework

II-B1. Fase de Set-up: En esta primera fase, el usuario debe realizar una serie de tareas para poder usar el sistema propuesto:

1. Instalar y configurar en un dispositivo móvil (smartphone) la aplicación provista. Este proceso de configuración consta a su vez de distintos pasos:
   a) Generar un login seguro para el acceso a la aplicación mediante usuario y contraseña. Se ofrece al usuario la posibilidad de usar un Segundo Factor de Autenticación (2AF) para mejorar la seguridad de acceso.
   b) Sincronizar la aplicación con una POD. La aplicación provee al usuario de una POD gratuita; sin embargo, se le permite a este cambiarla.
   c) Generar una pareja de claves de criptografía asimétrica mediante un generador (clave pública PK_0 y clave privada SK_0). Este generador utilizará 12 palabras aleatorias como semilla para la generación de dichas claves. El usuario debe anotar y guardar estas palabras para restaurar el sistema en caso de que haya algún problema con el dispositivo móvil.
   d) Guardar la clave privada (SK_0) en el *Secure Storage* del dispositivo móvil.
   e) Guardar la clave pública (PK_0) en la POD, la cual ha sido previamente sincronizada con la aplicación.
2. Instalar y configurar el plug-in provisto en los navegadores que el usuario vaya a usar para navegar por internet. Este proceso, a su vez, también requiere de algunos pasos:
   a) Sincronizar el plug-in con la POD previamente escogida.
   b) Configurar el nivel de privacidad deseado por parte del usuario. Aquí, se le pregunta al usuario que nivel de privacidad desea, del 0 al 3, siendo el 0 en el que se aceptan todas las políticas y uso de las cookies y el 3 donde se rechazan todas.
   c) Descargar y almacenar en memoria la clave pública generada por la aplicación móvil (PK_0).

II-B2. Fase de Navegación: Una vez completada la fase de set-up, el usuario ya puede empezar a navegar por internet, de modo que todo el proceso de aceptación de políticas de privacidad y del uso de las cookies se realizará de forma automática y transparente mediante el plug-in instalado en el navegador. De este modo, cada vez que el usuario acceda a una nueva web donde se le requiera un consentimiento previo, el sistema realizará los siguientes pasos:

1. Generar una nueva pareja de claves asimétricas(PK_i y SK_i).
2. Aceptar las políticas y cookies en función del nivel de privacidad especificado por el usuario.
3. Exportar las políticas aceptadas a un contrato inteligente.
4. *Deploy* del contrato inteligente en la blockchain mediante la clave privada previamente generada (SK_i).
5. Generar una clave simétrica (K_i).
6. Cifrar la pareja de claves generada (PK_i y SK_i) usando la clave simétrica K_i ($Enc_{K_i}(PK_i, SK_i)$).
7. Cifrar la clave simétrica (K_i) usando la clave pública obtenida de la POD (($Enc_{PK_0}(K_i)$)).
8. Guardar la pareja de claves, cifradas con la clave simétrica ($Enc_{K_i}(PK_i, SK_i)$); y la clave simétrica, también cifrada con la clave pública PK_0 ($Enc_{PK_0}(K_i)$), en la POD.

II-B3. Fase de Control: En cualquier momento, el usuario debe tener acceso a todos aquellos sitios en los que ha dado su consentimiento y poder modificar o retirar dicho consentimiento de acuerdo con sus derechos sobre sus datos personales. Esto se lleva a cabo a través de la aplicación móvil provista. Así, en esta fase se explica el funcionamiento del sistema en cuanto un usuario quiera tener acceso y o modificar dichos permisos:

1. Descargar el bloque cifrado ($Enc_{K_i}(PK_i, SK_i)$, $Enc_{PK_0}(K_i)$).
2. Descifrar la clave simétrica (K_i) mediante la clave privada almacenada en el *secure storage* del dispositivo móvil (SK_0): $Dec_{SK_0}(K_i)$.
3. Descifrar la pareja de claves asimétricas ((PK_i y SK_i)) mediante la clave simétrica previamente obtenida (K_i): $Dec_{K_i}(PK_i, SK_i)$.
4. Obtener el contrato inteligente que contiene el acuerdo aceptado por el usuario sobre las políticas de privacidad y el uso de las cookies, mediante la clave pública obtenida anteriormente (PK_i).
5. Modificar el acuerdo en el contrato inteligente mediante una transacción firmada con la clave privada obtenida anteriormente (SK_i).

Cabe destacar que el contenido de los contratos inteligentes se muestra de una forma clara e intuitiva a los usuarios, del mismo modo que cualquier modificación a realizar sobre los consentimientos almacenados en los mismos.

III. Discusión

En esta sección demostramos como el protocolo para la gestión de claves criptográficas permite mantener la privacidad de un usuario, en el caso de que un atacante intente reidentificarlo y obtener información sensible sobre él. Como no se guarda ningún tipo de información personal del usuario en

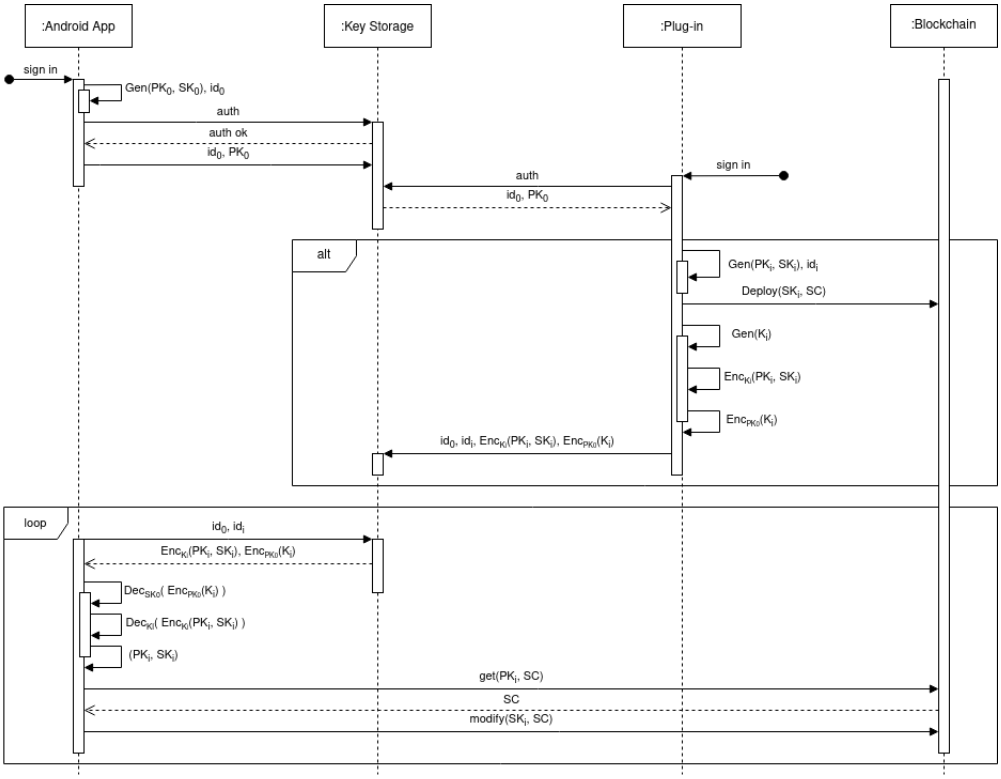


Figura 2. Protocol

los SCs, la única forma de que un atacante pueda re-identificar a dicho usuario es mediante el uso de casi-identificadores. En este caso, el atacante puede usar todas aquellas páginas web a las cuales el usuario ha accedido como estos casi-identificadores.

En una primera instancia, el atacante podría extraer de la BC todos los SCs asociados a una determinada clave pública y mediante ellos re-identificar al usuario. Para evitar este ataque, el sistema genera una nueva pareja de claves cada vez que el usuario acede a una nueva plataforma web, por lo que no habrá en la BC dos SCs asociados a una misma clave pública.

En una segunda instancia, el atacante podría obtener acceso a la POD donde se guardan todas estas parejas de claves generadas para la creación y gestión de los SCs. Para evitar que un atacante que ha obtenido acceso al POD pueda obtener acceso a las parejas de claves guardadas, estas son cifradas mediante criptografía simétrica (usando una nueva clave simétrica por cada pareja de claves asimétricas). Así mismo, estas claves simétricas son cifradas mediante una clave púbica, manteniéndose la clave privada asociada segura en el *secure storage* del dispositivo móvil donde se ha instalado la aplicación provista con el marco. Así, aunque un atacante pudiese acceder a la POD de un usuario concreto, este no podría acceder a las claves asimétricas y, por tanto, detectar cuáles son los SCs asociados a dicho usuario.

IV. Conclusiones

En este trabajo hemos presentado un marco para la gestión automática de las políticas de privacidad y uso de las cookies de los usuarios, centrándonos en el protocolo desarrollado para la creación y gestión de las claves criptográficas. Este protocolo permite el uso del sistema a la vez que permite mantener la privacidad del usuario en el caso de que un atacante intentase re-identificar a dicho usuario y obtener información sensible sobre él, como se ha demostrado en la sección III.

IV-A. Future work

Como trabajo futuro pretendemos añadir integridad en el almacenamiento de las parejas de claves asimétricas, de forma que un usuario pueda detectar si se ha llevado a cabo alguna modificación o se ha eliminado alguna de las claves.

Agradecimientos

Esta investigación cuenta con el apoyo del Fondo de Desarrollo Regional de la Unión Europea en el marco del Programa Operativo FEDER de Cataluña 2014-2020 con una subvención del 50 % del coste total subvencionable, en el marco del proyecto FEM-IOT [001-P-001682]; de la Comisión Europea (proyecto H2020-871042 ”SoBigData++”); y del Gobierno de España (proyecto RTI2018-095094-B-C21 Çonsentimiento”). El autor también cuenta con el apoyo del Gobierno español mediante una beca FPU (ref. FPU20/03254).

Referencias

[1] A. Esteve, “The business of personal data: Google, Facebook, and privacy issues in the EU and the USA,” *International Data Privacy Law*, vol. 7, no. 1, pp. 36–47, 03 2017. [Online]. Available: https://doi.org/10.1093/idpl/ipw026

[2] “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance),” *Official Journal of the European Union L 119*, vol. 59, p. 1–88, 5 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[3] C. Wirth and M. Kolain, "Privacy by blockchain design: A blockchain-enabled GDPR-compliant approach for handling personal data," in *Reports of the European Society for Socially Embedded Technologies (EUSSET)*, 2018.

[4] B. Faber, G. Michelet, N. Weidmann, R. R. Mukkamala, and R. Vatrapu, "BPDIMS: A blockchain-based personal data and identity management system," in *Conference: Hawaii International Conference on System Sciences*, January 2019.

[5] M. Zichichi, S. Ferretti, G. D'Angelo, and V. Rodríguez-Doncel, "Personal data access control through distributed authorization," in *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, Nov 2020, pp. 1–4.

[6] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "GDPR-compliant personal data management: A blockchain-based solution," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1746–1761, 2020.

[7] M. Davari and E. Bertino, "Access control model extensions to support data privacy protection based on GDPR," in *2019 IEEE International Conference on Big Data (Big Data)*, Dec 2019, pp. 4017–4024.

[8] M. Barati and O. Rana, "Tracking GDPR compliance in cloud-based service delivery," *IEEE Transactions on Services Computing*, pp. 1–1, 2020.

[9] M. M. Merlec, Y. K. Lee, S.-P. Hong, and H. P. In, "A smart contract-based dynamic consent management system for personal data usage under gdpr," *Sensors*, vol. 21, no. 23, 2021.

[10] S.-S. Jung, S.-J. Lee, and I.-C. Euom, "Delegation-based personal data processing request notarization framework for GDPR based on private blockchain," *Applied Sciences*, vol. 11, no. 22, 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/22/10574

[11] C. Daudén-Esmel, J. Castellà-Roca, A. Viejo, and J. Domingo-Ferrer, "Lightweight blockchain-based platform for GDPR-compliant personal data management," in *5th IEEE International Conference on Cryptography, Security and Privacy, CSP 2021, Zhuhai, China, January 8-10, 2021*, 2021, pp. 68–73.