Partage de documents sécurisé entre Cloud personnels

Paul Tran-Van, Philippe Pucheral, Nicolas Anciaux, Benjamin André

Partage de documents sécurisé entre Cloud personnels

Paul Tran-Van[1,2,3] , Philippe Pucheral[1,2], Nicolas Anciaux[1,2], Benjamin André[3]

[1]INRIA Paris-Rocquencourt
France
Fname.Lname@inria.fr

[2]U. Versailles St-Quentin-En-Yvelines
France
Fname.Lname@uvsq.fr

[3]Cozy Cloud
France
{paul, ben}@cozycloud.cc

MOTIVATION

Nous sommes aujourd'hui témoins d'une accumulation exponentielle de données personnelles sur les serveurs : données stockées par les administrations, les hôpitaux, les assurances; données captées automatiquement par les sites web visités, données issues de capteurs (smart meters et plus généralement la multitude d'objets intelligents formant l'Internet des objets), ceci sans oublier les données numériques possédées ou créées par les individus eux-mêmes (e.g. photos, agendas, publications sociales, etc).

La plupart de ces données aboutissent sur les serveurs des majors de l'internet, faisant ainsi perdre tout contrôle des utilisateurs sur leurs propres données personnelles, devenues le *nouveau pétrole* du XXIe siècle. Ces serveurs centralisés totalement opaques sont organisés en gigantesques silos de données, posant des problèmes évidents de respect de la vie privée, que ce soit par malveillance, négligence, ou usage abusif. De plus, aucune collaboration entre services n'est rendue possible, restreignant drastiquement les utilisateurs dans l'utilisation de leurs données qui se retrouvent dispersées et isolées dans ces silos.
Face à cette situation, le World Economic Forum a formulé le besoin de voir émerger des plateformes de gestion de données personnelles permettant à chaque individu de collecter, gérer et partager ses données dans différents contextes avec de réelles garanties de protection de la vie privée [WEF12]. Cette vision a été renforcée par l'affaire PRISM dévoilée par Edward Snowden. Pour répondre à ces critiques, de multiples solutions décentralisées émergent [NTB+12]. Cependant, ces solutions sacrifient généralement la fonctionnalité et les perspectives de services innovants sur l'autel de la protection de la confidentialité. Soit les données sont gérées en silos isolés empêchant tout rapprochement, croisement et analyse de données, soit le partage de données est réalisé sur la seule base de la confiance entre individus, sans garantie tangible de sécurité[1].

SOLUTION DU CLOUD PERSONNEL

Face à cette situation, l'utilisation d'une plateforme de « Personal Cloud » [AAK15] *user-centric*, associée à un hardware sécurisé ouvre une nouvelle voie dans la protection, la gestion et le partage des données personnelles. Cozy[2] est un « Personal Cloud » permettant aux utilisateurs de stocker leurs données personnelles sur un serveur qu'ils contrôlent, tout en fournissant les couches logicielles et des applications permettant de gérer ces données de façon simple, intuitive et innovante. L'ensemble de la plateforme est open-source, afin de garantir la transparence auprès des utilisateurs et de permettre à la communauté d'auditer le code et d'y contribuer, que ce soit par de nouvelles applications ou directement dans le cœur logiciel.

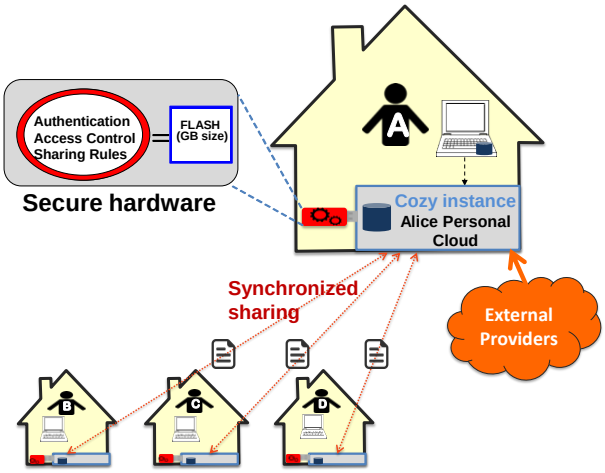

Figure 1 : Architecture

Des applications classiques sont disponibles, d'agenda, contacts, mails, photos, fichiers, etc, mais également des connecteurs permettant d'importer des données externes dans son Cozy et de disposer ainsi de son espace personnel réunissant toutes ses données. Ainsi les factures, relevés bancaires, données d'objet connectés ou encore publications sur des réseaux sociaux peuvent être réunies au même endroit, évitant la dispersion des données et permettant des usages innovants en croisant ces données, par exemple pour faire du quantified-self.
Un « Personal Cloud » tel que Cozy se doit d'être irréprochable en matière de sécurité. Dans [ABB+13], est décrite la vision d'un *Personal Data Server* (PDS) dont l'objectif est de construire une alternative crédible à la centralisation systématique des données personnelles sur des serveurs. Un PDS tire sa sécurité du composant matériel sécurisé dans lequel il est embarqué. S'il existe une grande variété de tels composants sécurisés (mass storage SIM card, clé USB sécurisée, secure token, smart dongle, etc), tous peuvent être abstraits par (1) un Environnement d'Exécution de Confiance et (2) un grand espace de stockage (potentiellement sans confiance, et donc devant contenir uniquement des données chiffrées). L'Environnement d'Exécution de Confiance est habituellement composé d'un microcontrôleur sécurisé qualifié de *tamper-resistant*

[1] Voir par exemple l'initiative FreedomBox (http://freedomboxfoundation.org/).
[2] http://cozy.io/en/

(résistant aux attaques physiques), tandis que l'espace de stockage est habituellement constitué d'une mémoire Flash externe (puce de Flash ou carte micro-SD).
La confiance qu'il est possible de porter à un PDS est due à une combinaison de facteurs: (1) le fait qu'un PDS porte les données d'un seul individu, qu'aucun code externe ne puisse être installé dessus et qu'il faille être en sa possession physique pour l'attaquer, (2) le microcontrôleur *tamper-resistant*, qui rend les attaques physiques ou par canaux cachés très difficiles, (2) l'auto-administration du PDS, qui évite les attaques internes par l'administrateur, et (4) le fait que le propriétaire du PDS lui-même ne peut pas accéder à toutes les données stockées, puisqu'il doit s'authentifier et accède aux données selon ses privilèges[3]. Un PDS supportant l'algèbre relationnelle a été conçu [ABP+14] et prototypé [LAS+15]. Ce prototype est embarqué dans un token USB sécurisé, d'où son nom PlugDB du fait qu'il est connectable/déconnectable à l'envie sur tout terminal. Une expérimentation terrain a été menée, permettant à PlugDB d'atteindre un fort niveau de maturité [AAB+10].
Un transfert technologique est actuellement en cours afin d'intégrer PlugDB dans l'architecture Cozy, qui déléguera ainsi les parties critiques de sécurité, à savoir le contrôle d'accès et la gestion des clés de chiffrement.
Le modèle initial simple suivant est envisagé : (1) le granule de contrôle d'accès est le document, (2) des méta-données sont associées aux documents et peuvent être utilisées pour définir des règles de contrôle d'accès (ex: autoriser l'accès de tel document à tel utilisateur ou rôle en fonction du sujet, de l'auteur, du type de document, etc), (3) les documents sensibles sont stockés chiffrés dans le DataSystem de Cozy Cloud (i.e., CouchDB), (4) les clés de chiffrement et les règles de contrôle d'accès sont stockées et évaluées dans PlugDB, (5) quand une demande de document est envoyée par une App à Cozy Cloud, celui-ci route la requête vers PlugDB qui évalue la ou les règles de contrôle d'accès associées et renvoie la clé permettant de déchiffrer le document dans le cas positif, (6) Cozy Cloud peut alors déchiffrer le document stocké dans son DataSystem et le renvoyer à l'App. Si le débit du composant sécurisé le permet, il sera envisagé de faire déchiffrer le document directement par PlugDB afin qu'aucune clé de chiffrement ne soit jamais exposée.
En parallèle de cette intégration, PlugDB peut être utilisé pour stocker et évaluer des règles de partage. Lorsqu'un utilisateur souhaite partager des documents avec une ou plusieurs personnes disposant d'un « Personal Cloud » distant, une règle de partage est stockée dans PlugDB, contenant les identifiants des documents, les destinataires, les permissions, le mode d'authentification, etc. Si l'utilisateur souhaite chiffrer ces documents, les clés seront également stockées dans PlugDB. Les destinataires du partage peuvent utiliser leur propre PlugDB pour stocker et appliquer ces règles, tandis que Cozy gère la synchronisation des documents entre les utilisateurs (si cela a été spécifié par l'initiateur du partage), permettant ainsi la propagation des modifications en pair à pair. N'importe quel type de donnée peut être partagé ; Cozy utilise une base NoSQL CouchDB[4] où les données sont représentées sous la forme de documents JSON, identifiés et versionnés de façon unique.

SCENARIO DE LA DEMONSTRATION

Dans cette démonstration, nous présentons de façon séparée Cozy et PlugDB, puis un cas d'usage de partage synchronisé et décentralisé entre Cozy distants intégrant PlugDB. Ce dernier est responsable de l'authentification et de la gestion des méta-données associées au partage. La possibilité de coupler PlugDB et Cozy est illustrée sur l'exemple de deux utilisateurs partageant une liste de documents. Une fois la liste définie, toute mise à jour sur un document est synchronisée immédiatement de part et d'autre.

TRAVAUX FUTURS

Le travail en cours cherche à créer des règles de partage simples et expressives, permettant aux utilisateurs de partager des contenus dynamiques entre instances Cozy. L'accès à ces règles et leur application sont réalisés via PlugDB, également responsable des clés de chiffrement et de l'authentification des utilisateurs distants.
Un travail est également mené[5] afin de rendre ce partage interopérable avec d'autres plateformes de « Personal Cloud ».

BIBLIOGRAPHIE

[AAB+10] Allard, T., Anciaux, N., Bouganim, L., Pucheral, P., & Thion, R. (2010). Seamless access to healthcare folders with strong privacy guarantees. *Healthcare Delivery Reform and New Technologies: Organizational Initiatives: Organizational Initiatives*.

[AAK15] S. Abiteboul, B. André, D. Kaplan. 'Managing your digital life with a Personal information management system'. Communications of the ACM, 2015, 58 (5), pp.32-35.

[ABB+13] N. Anciaux, P. Bonnet, L. Bouganim, B. Nguyen, I. S. Popa, P. Pucheral, 'Trusted Cells: A Sea Change for Personal Data Services'. CIDR 2013.

[ABP+14] N. Anciaux, L. Bouganim, P. Pucheral, Y. Guo, L. Le Folgoc, S. Yin, 'MILo-DB: a personal, secure and portable database machine'. Distributed and Parallel Databases 32(1): 37-63 (2014).

[LAS+15] S. Lallali, N. Anciaux, I. Sandu Popa, P. Pucheral, 'A Secure Search Engine for the Personal Cloud'. SIGMOD Conference 2015.

[NTB+12] A. Narayanan, V. Toubiana, S. Barocas, H. Nissenbaum, D. Boneh, 'A Critical Look at Decentralized Personal Data Architectures' in *Data Usage Management on the Web*, 2012.

[WEF12] The World Economic Forum. Rethinking Personal Data: Strengthening Trust. May 2012.

[3] Au même titre qu'un porteur de carte bancaire par exemple n'a pas accès aux secrets cryptographiques embarqués dans sa propre carte à puce.

[4] http://couchdb.apache.org/

[5] https://tools.ietf.org/html/draft-dejong-decentralized-sharing-00