" PRÉSERVER LA VIE PRIVÉE DES INDIVIDUS GRÂCE AUX SYSTÈMES PERSONNELS DE GESTION DES DONNÉES » (PRESERVING INDIVIDUAL PRIVACY WITH PERSONAL DATA MANAGEMENT SYSTEMS)" PAR IULIAN SANDU POPA

Discipline :INFORMATIQUE

Résumé :
Surfant sur la vague des initiatives de divulgation restreinte de données et des nouvelles réglementations en matière de protection de la vie privée, le paradigme du Cloud Personnel émerge à travers une myriade de solutions proposées aux utilisateurs leur permettant de rassembler et de gérer l'ensemble de leur vie numérique. Du côté positif, cela ouvre la voie à de nouveaux services à valeur ajoutée lors du croisement de plusieurs sources de données d'un individu ou du croisement des données de plusieurs personnes. Cependant, ce changement de paradigme vers la responsabilisation de l'utilisateur soulève des questions fondamentales quant à l'adéquation des fonctionnalités et des techniques de gestion et de protection des données proposées par les solutions

existantes aux utilisateurs lambda. Notre travail aborde ces questions à trois niveaux. Tout d'abord, nous passons en revue, comparons et analysons les alternatives de cloud personnel au niveau des fonctionnalités fournies et des modèles de menaces ciblés. De cette analyse, nous déduisons un ensemble général d'exigences en matière de fonctionnalité et de sécurité que tout système personnel de gestion des données (PDMS) devrait prendre en compte. Nous identifions ensuite les défis liés à la mise en œuvre d'un tel PDMS et proposons une conception préliminaire pour une architecture PDMS étendue et sécurisée de référence répondant aux exigences considérées. Ensuite, nous nous concentrons sur les calculs personnels pour une instance matérielle spécifique du PDMS (à savoir, un dispositif personnel sécurisé avec un stockage de masse de type NAND Flash). Dans ce contexte, nous proposons un moteur de recherche plein texte embarqué et évolutif pour indexer de grandes collections de documents et gérer des politiques de contrôle d'accès basées sur des étiquettes. Troisièmement, nous abordons le problème des calculs collectifs dans une architecture entièrement distribuée de PDMS. Nous discutons des exigences d'architectures système et de sécurité et proposons des protocoles pour permettre le traitement distribué des requêtes avec de fortes garanties de sécurité contre un attaquant maîtrisant de nombreux nœuds corrompus.

Abstract:

Riding the wave of smart disclosure initiatives and new privacy-protection regulations, the Personal Cloud paradigm is emerging through a myriad of solutions offered to users to let them gather and manage their whole digital life. On the bright side, this opens the way to novel value-added services when crossing multiple sources of data of a given person or crossing the data of multiple people. Yet this paradigm shift towards user empowerment raises fundamental questions with regards to the appropriateness of the functionalities and the data management and protection techniques which are offered by existing solutions to laymen users. Our work addresses these questions on three levels. First, we review, compare and analyze personal cloud alternatives in terms of the functionalities they provide and the threat models they target. From this analysis, we derive a general set of functionality and security requirements that any Personal Data Management System (PDMS) should consider. We then identify the challenges of implementing such a PDMS and propose a preliminary design for an extensive and secure PDMS reference architecture satisfying the considered requirements. Second, we focus on personal computations for a specific hardware PDMS instance (i.e., secure token with mass storage of NAND Flash). In this context, we propose a scalable embedded full-text search engine to index large document collections and manage tag-based access control policies. Third, we address the problem of collective computations in a fully-distributed architecture of PDMSs. We discuss the system and security requirements and propose

protocols to enable distributed query processing with strong security guarantees against an attacker mastering many colluding corrupted nodes.

INFORMATIONS COMPLÉMENTAIRES

M. Amr El Abbadi Professeur, University of California Santa Barbara (rapporteur)
M. Luc Bouganim Directeur de Recherche, Inria Saclay-Ile-de-France (tuteur)
M. Sébastien Gambs Professeur, Université du Québec à Montréal (examinateur)
Mme Esther Pacitti Professeur, Université Montpellier 2 (examinatrice)
Mme Indrakshi Ray Professeur, Colorado State University (rapporteuse)
M. Vincent Roca Chargé de Recherche, HDR, Inria Rhône-Alpes (rapporteur)
Mme Karine Zeitouni Professeur, UVSQ (examinatrice)

Contact : DSR - Service FED : theses@uvsq.fr