IN PARTNERSHIP WITH:
Université Versailles Saint-Quentin

Activity Report 2019

Project-Team PETRUS

PErsonal & TRUSted cloud

RESEARCH CENTER
Saclay - Île-de-France

THEME
Data and Knowledge Representation and Processing

Table of contents

Project-Team PETRUS

Creation of the Team: 2016 December 01, updated into Project-Team: 2017 July 01

Keywords:

Computer Science and Digital Science:

A1.1.8. - Security of architectures
A1.4. - Ubiquitous Systems
A3.1.2. - Data management, quering and storage
A3.1.3. - Distributed data
A3.1.5. - Control access, privacy
A3.1.6. - Query optimization
A3.1.8. - Big data (production, storage, transfer)
A3.1.9. - Database
A4.3. - Cryptography
A4.5. - Formal methods for security
A4.7. - Access control
A4.8. - Privacy-enhancing technologies

Other Research Topics and Application Domains:

B2.5.3. - Assistance for elderly
B6.4. - Internet of things
B6.6. - Embedded systems
B9.10. - Privacy

1. Team, Visitors, External Collaborators

Research Scientists

Nicolas Anciaux [Team leader, Inria, Senior Researcher, HDR]
Luc Bouganim [Inria, Senior Researcher, HDR]

Faculty Members

Guillaume Scerri [Univ de Versailles Saint-Quentin-en-Yvelines, Associate Professor]
Philippe Pucheral [Univ de Versailles Saint-Quentin-en-Yvelines, Professor, HDR]
Iulian Sandu Popa [Univ de Versailles Saint-Quentin-en-Yvelines, Associate Professor]

Post-Doctoral Fellow

Julien Loudet [Inria, Post-Doctoral Fellow, from Nov 2019]

PhD Students

Robin Carpentier [Univ de Versailles Saint-Quentin-en-Yvelines, PhD Student]
Riad Ladjel [Inria until Sept 2019, UVSQ since Sept 2019, PhD Student]
Julien Loudet [CozyCloud, PhD Student, until Sep 2019, granted by CIFRE]
Axel Michel [INSA CVL, PhD Student, until Apr 2019]
Dimitrios Tsolovos [Inria, PhD Student]

Technical staff

Aydogan Ersoz [Inria, Engineer, until Aug 2019]
Laurent Schneider [Inria, Engineer]

Interns and Apprentices

Ludovic Javet [Inria, intern, from Sep 2019 to Dec 2019]
Julien Mirval [Inria, intern, since Apr 2019]
Syed Moeen Ali Naqvi [Inria, intern, from Apr to Dec 2019]
Loen Boban [Inria, intern, from May 2019 until Aug 2019]

Administrative Assistants

Adeline Lochet [Inria, Administrative Assistant, until May 2019]
Emmanuelle Perrot [Inria, Administrative Assistant]

External Collaborator

Benjamin Nguyen [INSA CVL, Professor, HDR]

2. Overall Objectives

2.1. Overall Objectives

We are witnessing an exponential accumulation of personal data on central servers: data automatically gathered by administrations and companies but also data produced by individuals themselves (e.g., photos, agendas, data produced by smart appliances and quantified-self devices) and deliberately stored in the cloud for convenience. The net effect is, on the one hand, an unprecedented threat on data privacy due to abusive usage and attacks and, on the other hand, difficulties in providing powerful user-centric services (e.g. personal big data) which require crossing data stored today in isolated silos. The Personal Cloud paradigm holds the promise of a Privacy-by-Design storage and computing platform, where each individual can gather her complete digital environment in one place and share it with applications and users, while preserving her control. However, this paradigm leaves the privacy and security issues in user's hands, which leads to a paradox if we consider the weaknesses of individuals' autonomy in terms of computer security, ability and willingness to administer sharing policies. The challenge is however paramount in a society where emerging economic models are all based - directly or indirectly - on exploiting personal data.

While many research works tackle the organization of the user's workspace, the semantic unification of personal information, the personal data analytics problems, the objective of the PETRUS project-team is to tackle the privacy and security challenges from an architectural point of view. More precisely, our objective is to help providing a technical solution to the personal cloud paradox. More precisely, our goals are (i) to propose new architectures (encompassing both software and hardware aspects) for secure personal cloud data management and formally prove important bricks of the architecture, (ii) propose new data administration models reaching the main requirements of a personal cloud (decentralized access and usage control models, data sharing, data collection and retention models, etc.) and study the enforcement of the resulting privacy policies based on secure hardware and formally proven architectural components, (iii) propose new secure distributed database indexing models, privacy preserving query processing strategies and data anonymization techniques for the personal cloud.

3. Research Program

3.1. Research Program

To tackle the challenge introduced above, we identify three main lines of research:

- (Axis 1) Personal cloud server architectures. Based on the intuition that user control, security and privacy are key properties in the definition of trusted personal cloud solutions, our objective is to propose new architectures (encompassing both software and hardware aspects) for secure personal cloud data management and formally prove important bricks of the architecture. We also focus in this axis on administration models and their enforcement in relation to the architecture of the system, so that the exclusive control of a non expert individual can be ensured.

- (Axis 2) Global query evaluation. The goal of this line of research is to provide capabilities for crossing data belonging to multiple individuals (e.g., performing statistical queries over personal data, computing queries on social graphs or organizing participatory data collection) in a fully decentralized setting while providing strong and personalized privacy guarantees. This means proposing new secure distributed database indexing models and query processing strategies. In addition, we concentrate on locally ensuring to each participant the good behaviour of the processing, such that no collective results can be produced if privacy conditions are not respected by other participants.
- (Axis 3) Economic, legal and societal issues. This research axis is more transverse and entails multidisciplinary research, addressing the links between economic, legal, societal and technological aspects. We will follow here a multi-disciplinary approach based on a 3-step methodology: i) identifying important common issues related to privacy and to the exploitation of personal data; ii) characterizing their dimensions in all relevant disciplines and jointly study their entanglement; iii) validating the proposed analysis, models and trade-offs thanks to in vivo experiments.

These contributions will also rely on tools (algorithms, protocols, proofs, etc.) from other communities, namely security (cryptography, secure multiparty computations, formal methods, differential privacy, etc.) and distributed systems (distributed hash tables, gossip protocols, etc.). Beyond the research actions, we structure our software activity around a single common platform (rather than isolated demonstrators), integrating our main research contributions, called PlugDB. This platform is the cornerstone to help validating our research results through accurate performance measurements on a real platform, a common practice in the DB community, and target the best conferences. It is also a strong vector to federate the team, simplify the bootstrapping of new PhD or master students, conduct multi-disciplinary research and open the way to industrial collaborations and technological transfers.

4. Application Domains

4.1. Personal cloud, home care, IoT, sensing, surveys

As stated in the software section, the Petrus research strategy aims at materializing its scientific contributions in an advanced hardware/software platform with the expectation to produce a real societal impact. Hence, our software activity is structured around a common Secure Personal Cloud platform rather than several isolated demonstrators. This platform will serve as the foundation to develop a few emblematic applications. Several privacy-preserving applications can actually be targeted by a Personal Cloud platform, like: (i) smart disclosure applications allowing the individual to recover her personal data from external sources (e.g., bank, online shopping activity, insurance, etc.), integrate them and cross them to perform personal big data tasks (e.g., to improve her budget management) ; (ii) management of personal medical records for care coordination and well-being improvement; (iii) privacy-aware data management for the IoT (e.g., in sensors, quantified-self devices, smart meters); (iv) community-based sensing and community data sharing; (v) privacy-preserving studies (e.g., cohorts, public surveys, privacy-preserving data publishing). Such applications overlap with all the research axes described above but each of them also presents its own specificities. For instance, the smart disclosure applications will focus primarily on sharing models and enforcement, the IoT applications require to look with priority at the embedded data management and sustainability issues, while community-based sensing and privacy-preserving studies demand to study secure and efficient global query processing. Among these applications domains, one is already receiving a particular attention from our team. Indeed, we gained a strong expertise in the management and protection of healthcare data through our past DMSP (Dossier Medico-Social Partagé) experiment in the field. This expertise is being exploited to develop a dedicated healthcare and well-being personal cloud platform. We are currently deploying 10000 boxes equipped with PlugDB in the context of the DomYcile project. In this context, we are currently setting up an Inria Innovation Lab with the Hippocad company to industrialize this platform and deploy it at large scale (see Section the bilateral contract OwnCare II-Lab).

5. New Software and Platforms

5.1. PLUG-DB ENGINE

KEYWORDS: Databases - Personal information - Privacy - Hardware and Software Platform

FUNCTIONAL DESCRIPTION: en PlugDB is a complete platform dedicated to a secure and ubiquitous management of personal data. It aims at providing an alternative to a systematic centralization of personal data. The PlugDB engine is a personal database server capable of storing data (tuples and documents) in tables and BLOBs, indexing them, querying them in SQL, sharing them through assertional access control policies and enforcing transactional properties (atomicity, integrity, durability).

The PlugDB engine is embedded in a tamper-resistant hardware device combining the security of smartcard with the storage capacity of NAND Flash. The personal database is hosted encrypted in NAND Flash and the PlugDB engine code runs in the microcontroller. Complementary modules allow to pre-compile SQL queries for the applications, communicate with the DBMS from a remote Java program, synchronize local data with remote servers (typically used for recovering the database in the case of a broken or lost devices) and participate in distributed computation (e.g., global queries). PlugDB runs both on secure devices provided by Gemalto and on specific secure devices designed by PETRUS and assembled by electronic SMEs. Mastering the hardware platform opens up new research and experiment opportunities (e.g., support for wireless communication, secure authentication, sensing capabilities, battery powered ...). PlugDB engine has been registered first at APP (Agence de Protection des Programmes) in 2009 - a new version being registered every two years - and the hardware datasheets in 2015.

PlugDB has been experimented in the field, notably in the healthcare domain. We also recently set up an educational platform on top of PlugDB, named SIPD (Système d'Information Privacy-by-Design) and used at ENSIIE, INSA CVL and UVSQ through the Versailles Sciences Lab fablab, to raise students awareness of privacy protection problems and embedded programming. As a conclusion, PlugDB combines several research contributions from the team, at the crossroads of flash data management, embedded data processing and secure distributed computations. It then strongly federates all members of our team (permanent members, PhD students and engineers). It is also a vector of visibility, technological transfer and dissemination and gives us the opportunity to collaborate with researchers from other disciplines around a concrete privacy-enhancing platform.

PlugDB is now being industrialized in the context of the OwnCare Inria Innovation Lab (II-Lab). In OwnCare, PlugDB acts as a secure personal cloud to manage medical/social data for people receiving care at home. It should be deployed over 10.000 patient in the Yvelines district. The industrialization process covers the development of a complete testing environment, the writing of a detailed documentation and the development of additional features (e.g., embedded ODBC driver, TPM support, flexible access control model and embedded code upgrade notably). It has also required the design of a new hardware platform equipped with a battery power supply, introducing new energy consumption issues for the embedded software.

- Participants: Aydogan Ersoz, Laurent Schneider, Luc Bouganim, Nicolas Anciaux and Philippe Pucheral
- Contact: Nicolas Anciaux
- URL: https://project.inria.fr/plugdb/

6. New Results

6.1. The Security Properties of a PDMS (Axis 1)

Participants: Nicolas Anciaux [correspondent], Luc Bouganim, Philippe Pucheral, Iulian Sandu Popa, Guillaume Scerri.

Different Personal Data Management Systems (PDMS) solutions are emerging in both academia and industry. In terms of functionality and security properties, PDMS solutions differ significantly from traditional Data Base Management Systems (DBMS). In a journal article published in Information Systems this year [3], we take stock of the functionality and security of PDMS solutions, propose five very specific security properties to be achieved and provide a preliminary architecture to meet them based on secure hardware [3]. We also presented as a tutorial at VLDB'19 [4] and a keynote at APVP'19 a review of the literature on database and security on data management issues for secure hardware and new research directions for privacy preserving management of personal data.

6.2. SEP2P and DISPERS (Axis 2)

Participants: Luc Bouganim [correspondent], Julien Loudet, Iulian Sandu Popa.

Personal Data Management Systems (PDMS) arrive at a rapid pace allowing us to integrate all our personal data in a single place and use it for our benefit and for the benefit of the community. This leads to a significant paradigm shift since personal data become massively distributed and opens an important question: how can users/applications execute queries and computations over this massively distributed data in a secure and efficient way, relying exclusively on peer-to-peer (P2P) interactions despite covert adversaries which could be executing the query? We first proposed a Secure and Efficient Peer-to-Peer protocol (SEP2P) to randomly select the nodes that will execute the query. This protocol leverages properties of distributed hash tables (DHT) to select nodes in a way that is, at the same time, secure, random and efficient. The security and randomness stem from the fact that we know, with a very high probability, that at least one honest node contributed to the creation and attestation of this list of nodes; while the efficiency stems from the fact that very few nodes are involved in this process. Building on top of SEP2P, we designed DISPERS, a protocol that applies three design rules: (D1) imposed randomness, enforced by SEP2P, (D2) knowledge dispersion, and (D3) task compartmentalization: Each user provides profile information to indexing nodes, chosen randomly thanks to the DHT (D1). Shamir secret-sharing techniques are used to avoid that any indexing node has a full knowledge of indexed nodes (D2). Then, for each query, a set of random nodes is selected (SEP2P) to coordinate the research for query targets using the indexing nodes. Each of these random nodes learns a part of the query targets IP address but does not know the query (D2, D3). Another set of random nodes is chosen to compute of the final answer based on partial local results from targets. These nodes learn part of the results but do not know the targets, thanks to proxies, nor the meaning of these results (D2, D3). These results are the core of Julien Loudet's thesis [1]. SEP2P was published at EDBT'19 [9] while a demonstration of DISPERS was published at VLDB'19 [8].Both works were also exposed/demonstrated at BDA'19 [13] [12] and APVP'19 [14] for the French research community in databases and security and privacy.

6.3. Manifest-based Framework for Secure Decentralized Queries (Axis 2)

Participants: Riad Ladjel [correspondent], Nicolas Anciaux, Philippe Pucheral, Guillaume Scerri.

The PDMS context calls for a new decentralized way of handling processing. The challenge is to allow generic treatment of large populations of PDMS, with a double objective: to preserve the mutual trust of individuals in their PDMS, and to guarantee an honest result (calculated on the right data, with the right code). To achieve this goal, our approach introduces a computational 'manifest', stipulating its execution plan and the privacy clauses (e.g., collection rules) to be guaranteed at runtime, based on trusted hardware (e.g., Intel SGX processor). Our contributions consist of (1) a protocol for randomly assigning compute tasks to participants to prevent targeted attacks, (2) a mechanism guaranteeing global compute integrity through local-only checks (without centralized trusted third party) and (3) database countermeasures limiting the impact of hidden channel attacks from corrupted participants. These contributions resulted in articles in TrustCom'19 [7] and ISD'19 [6]. Our approach guarantees confidentiality and processing integrity, it is generic and scalable, and goes far beyond existing approaches (e.g., secure multiparty computing or differential privacy).

6.4. Mobile Participatory Sensing with Strong Privacy Guarantees (Axis 2)

Participant: Iulian Sandu Popa [correspondent].

Mobile participatory sensing (MPS) could benefit many application domains. A major domain is smart transportation, with applications such as vehicular traffic monitoring, vehicle routing, or driving behavior analysis. However, MPS's success depends on finding a solution for querying large numbers of smart phones or vehicular systems, which protects user location privacy and works in real-time. This work proposes PAMPAS, a privacy-aware mobile distributed system for efficient data aggregation in MPS. In PAMPAS, mobile devices enhanced with secure hardware, called secure probes (SPs), perform distributed query processing, while preventing users from accessing other users' data. A supporting server infrastructure (SSI) coordinates the inter-SP communication and the computation tasks executed on SPs. PAMPAS ensures that SSI cannot link the location reported by SPs to the user identities even if SSI has additional background information. Moreover, an enhanced version of the protocol, named PAMPAS$^+$, makes the system robust even against advanced hardware attacks on the SPs. Hence, the risk of user location privacy leakage remains very low even for an attacker controlling the SSI and a few corrupted SPs. Our experimental results demonstrate that these protocols work efficiently on resource constrained SPs being able to collect the data, aggregate them, and share statistics or derive models in real-time. This work has been accomplished in collaboration with NJIT and DePaul University and has been recently accepted as a journal paper (an 'Online first' version is available at https://link.springer.com/article/10.1007/s10707-019-00389-4).

6.5. Empowerment and Big Data on Personal Data: from Portability to Agency (Axis 3)

Participants: Nicolas Anciaux [correspondent], Riad Ladjel, Philippe Pucheral, Guillaume Scerri.

The current highly centralised model of personal data management is based on established business practices that have led to widespread adoption, in contrast to user-centric and privacy-oriented systems such as PDMS, which therefore need to be studied in terms of technical, economic and legal feasibility and adoptability with researchers from other disciplines. In the context of the DATAIA GDP-ERE project, we are analyzing the technical and legal conditions under which individuals can exercise their right to data portability. Over the period, we have jointly studied a new notion that characterizes the true power of the individual over his or her personal data: agency. In particular, we have shown how the notion of agency, which comes from the social sciences, can be transposed and used to our context to measure the empowerment of individuals in Big Data applications. This study led to two joint publications with law researchers over the period, in particular in the journal Dalloz IP/IT [5], as well as several international panels (see in Section Popularization, e.g., panel at BDVA forum organized in Helsinky with the European Commission, at the Annual Forum of Trans Europ Expert, etc.)

6.6. OwnCare Inria Inovation Lab

Participants: Philippe Pucheral [correspondent], Nicolas Anciaux, Luc Bouganim, Laurent Schneider.

The OwnCare IILab was created in January 2018 (see section: Bilateral Contracts with Industry) and involves the Hippocad SME and the PETRUS team around the management of medical-social data at patient's home. The objective is to build a fully decentralized and highly secure personal medical-social folder based on PlugDB, and deploy it at large scale. Besides this industrial objective, the goal is also to leverage and validate the PETRUS research contributions related to secured Personal Cloud architectures. Before the creation of the OwnCare IILab initiative, PlugDB was an advanced research prototype. It is now evolving towards a transferable product. To reach this state, a considerable effort has been made in terms of development, testing platform, validation procedures and documentation. PlugDB engine is regularly registered at APP (Agence de Protection des Programmes), for both the PlugDB hardware datasheets and the code of the PlugDB-engine. The next PlugDB code registration will cover all functionalities added since the beginning of the IILab, notably: dynamic upgrade of the embedded code, TPM-based secure boot, ad-hoc embedded stored procedures, RBAC-style access control model, aggregate computation, SSL certificate management, event/error logging mechanism. Some of these developments are highly challenging considering the embedded context and the energy consumption constraints we have to face (the current device hosting PlugDB is based on two microcontrollers – MCU – powered by small batteries). Typically, we had to implement the first coupling between a TPM and a STM MCU, a lightweight version of SSL that accommodates MCU resources and energy-saving synchronization protocols between 2 MCU.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. OwnCare II-Lab (Jul 2017 - Dec 2020)

Partners: PETRUS (Inria-UVSQ), Hippocad (SME)
End 2016, the Yvelines district lauched a public call for tender to deploy an industrial solution aiming at covering the whole distinct (10.000 patients). The Hippocad company, in partnership with Inria, won this call for tender with a solution called DomYcile in May 2017 and the project was launched in July 2017. DomYcile is based on a home box combining the PlugDB hardware/software technology developed by the Petus team and a communication layer based on SigFox. Hippocad and Petrus then decided to launch a joint II-Lab (Inria Innovation Lab) named OwnCare. The objective is threefold: (1) build an industrial solution based on PlugDB and deploy it in the Yvelines district in the short-term, (2) use this Yvelines testbed to improve the solution and try to deploy it at the national/international level in the medium-term and (3) design flexible/secure/mobile personal medical folder solutions targeting individual uses rather than professional uses in the long-term. The DomYcile project with the Yvelines district has started in July 2017 and the II-Lab was officially created in January 2018.

7.2. Bilateral Grants with Industry

7.2.1. Cozy Cloud CIFRE - Loudet contract (Apr 2016 - Apr 2019)

Partners: Cozy Cloud, PETRUS
In relation with the bilateral contract mentioned above, a second CIFRE PhD thesis has been started by Julien Loudet. The objective is to allow for a secure execution of distributed queries on a set of personal clouds associated to users, depending on social links, user's localization or user's profile. The general idea is to build secure indexes, distributed on the users' personal clouds and to devise a secure execution protocol revealing solely the query result to the querier. Such highly distributed secure queries potentially enable new (social) applications fed by user's personal data which could be developed on the Cozy-PlugDB platform.

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. ANR PerSoCloud (Jan 2017 - Dec 2020)

Partners: Orange Labs (coordinator), PETRUS (Inria-UVSQ), Cozy Cloud, U. of Versailles.
The objective of PerSoCloud is to design, implement and validate a full-fledged Privacy-by-Design Personal Cloud Sharing Platform. One of the major difficulties linked to the concept of personal cloud lies in organizing and enforcing the security of the data sharing while the data is no longer under the control of a central server. We identify three dimensions to this problem. Devices-sharing: assuming that the primary copy of user U1's personal data is hosted in a secure place, how to share and synchronize it with U1's multiple (mobile) devices without compromising security? Peers-sharing: how user U1 could exchange a subset of his-her data with an identified user U2 while providing to U1 tangible guarantees about the usage made by U2 of this data? Community-sharing: how user U1 could exchange a subset of his-her data with a large community of users and contribute to personal big data analytics while providing to U1 tangible guarantees about the preservation of his-her anonymity? In addition to tackling these three scientific and technical issues, a legal analysis will guarantee compliance of this platform with the security and privacy French and UE regulation, which firmly promotes the Privacy by Design principle, including the current reforms of personal data regulation.

8.1.2. GDP-ERE, DATA-IA project (Sept. 2018 - Jan. 2022)

Partners: DANTE (U. of Versailles), PETRUS (Inria-UVSQ).
The role of individuals and the control of their data is a central issue in the new European regulation (GDPR) enforced on 25th May 2018. Data portability is a new right provided under those regulations. It allows citizens to retrieve their personal data from the companies and governmental agencies that collected them, in an interoperable digital format. The goals are to enable the individual to get out of a captive ecosystem, and to favor the development of innovative personal data services beyond the existing monopolistic positions. The consequence of this new right is the design and deployment of technical platforms, commonly known as Personal Cloud. But personal cloud architectures are very diverse, ranging from cloud based solutions where millions of personal cloud are managed centrally, to self-hosting solutions. These diversity is not neutral both in terms of security and from the point of view of the chain of liabilities. The GDP-ERE project tends to study those issues in an interdisciplinary approach by the involvement of jurists and computers scientists. The two main objectives are (i) to analyze the effects of the personal cloud architectures on legal liabilities, enlightened by the analysis of the rules provided under the GDPR and (ii) to propose legal and technological evolutions to highlight the share of liability between each relevant party and create adapted tools to endorse those liabilities. http://dataia.eu/actualites/linstitut-dataia-vous-presente-le-projet-gdp-ere-rgpd-et-cloud-personnel-de-lempowerment

8.1.3. Postdoc DIM RFSI, Ile-de-France Region (2019 - 2020)

Partners: Inria (PETRUS).
This project is a continuation of Julien Loudet's Phd thesis. Julien finalized a CIFRE thesis defended in October 2019. This thesis is the result of a solid collaboration (another CIFRE thesis was defended in 2018) between the PETRUS team and the startup Cozy Cloud, which is also working on the personal cloud issue. The project finances 8 months of postdoc for Julien. The objective is to enforce the collaboration with Cozy Cloud by allowing the postdoc (i) to submit an extended journal paper on his last results (DISPERS protocol), (ii) to realize a detailed specification of the distributed protocols developed during his PhD for their implementation in the Cozy Cloud platform and (iii) to collaborate with a future PhD candidate of a new thesis in collaboration with Cozy Cloud exploring decentralized automatic learning techniques in the personal cloud context.

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events: Organisation

9.1.1.1. Member of the Organizing Committees

- Luc Bouganim: Co-organizer of Ecole thématique BDA Masses de Données Distribuées, Aussois, June 2020
- Iulian Sandu Popa: Colloque National Capteurs et Sciences Participatives (CASPA), Paris, 1-4 avril 2019

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

- Nicolas Anciaux: VLDB'19, SIGMOD'19
- Luc Bouganim: EDBT'2020
- Philippe Pucheral: DATA'19, MOBILITY'19, MEDES'19
- Iulian Sandu Popa: ICDE'20, SSDBM'19, IEEE MobileCloud'19, DATA'19, BDA'19 demo
- Guillaume Scerri: BDA'19

9.1.3. Journal

9.1.3.1. Member of the Editorial Boards

- Nicolas Anciaux: Associate Editor of the VLDB Journal

9.1.3.2. Reviewer - Reviewing Activities

- Iulian Sandu Popa: Journal of Internet Services and Applications
- Guillaume Scerri: ACM Transactions on Privacy and Security

9.1.4. Research Administration

- Philippe Pucheral: Member of the HDR committee of the STV doctoral school (UVSQ) since 2014
- Philippe Pucheral: Member of the steering committee of the ED STIC doctoral school of University Paris-Saclay, 'Data, Knowledge and Interactions' committee (about 250 PhD students) since 2014
- Philippe Pucheral: Member of the bureau of the DAVID lab board since 2016
- Nicolas Anciaux: Member of the Council of the Doctoral College of the University Paris-Saclay
- Nicolas Anciaux: Member of the "Bureau du comité des projets" at Inria saclay
- Nicolas Anciaux: Member of the DATAIA Convergence Institute Program Committee since 2018.
- Nicolas Anciaux: Correspondent for the Doctoral school ED STIC of University Paris-Saclay at Inria Saclay
- Nicolas Anciaux: Responsible for the 'Mission Jeunes Chercheurs' (MJC) at Inria Saclay
- Nicolas Anciaux: Responsible for the 'Formation par la Recherche' (FPR) at Inria Saclay
- Nicolas Anciaux: Member of the bureau of the DAVID lab board
- Luc Bouganim: Member of the Scientific Commission (CS) of Inria Saclay-IDF (Cordi-S, Post-Doc, Delegation)
- Luc Bouganim: Member of the Commission for Technological Development (CDT) of Inria Saclay-IDF
- Luc Bouganim: Member of the admission committee for DR2 at Inria
- Luc Bouganim: Member of the recruitment committee for CRCN at Inria
- Luc Bouganim: Member of the recruitment committee of associate professor at ITU Copenhagen
- Iulian Sandu Popa: Member of the Commission for Technological Development (CDT) of Inria Saclay-IDF
- Iulian Sandu Popa: Member of the recruitment committee for an MCF (Maître de Conférences) position at CNAM
- Iulian Sandu Popa: PhD thesis referent for the ED STIC doctoral school of University Paris-Saclay
- Guillaume Scerri: PhD thesis referent for the ED STIC doctoral school of University Paris-Saclay

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

- Licence : Iulian Sandu Popa, Bases de données (niveau L3), 96, UVSQ, France. Guillaume Scerri, Initiation aux bases de données (niveau L2), 63, UVSQ, France. Guillaume Scerri, Fondements de l'informatique (niveau L1), 36, UVSQ, France. Guillaume Scerri, Théorie des Langages (niveau L2), 45, UVSQ, France.
- Master : Iulian Sandu Popa, Bases de données relationnelles (niveau M1), Gestion des données spatiotemporelles (niveau M2), Sécurité des bases de données (niveau M2), 96, UVSQ, France. Philippe Pucheral, responsible of the DataScale master, courses in M1 and M2 in databases and in security, introductory courses for jurists,UVSQ, France. Guillaume Scerri, Bases de données relationnelles (niveau M1), 36, UVSQ, France. Guillaume Scerri, Sécurité et bases de données pour juristes, 4.5, UVSQ, France. Guillaume Scerri, Sécurité, 18, UVSQ, France.

- Engineers school : Nicolas Anciaux, courses on Databases (module IN206, niveau M1), 21, and Advanced databases (module ASI13, niveau M2), 24, at ENSTA ParisTech. Nicolas Anciaux, Systèmes d'Information "privacy by design" (niveau M1), 30, at ENSIIE Evry, France. Luc Bouganim, Systèmes d'Information "privacy by design" (niveau M1), 42, ENSIIE Evry, France. Luc Bouganim, Bases de données relationnelles (niveau M1), 32, ENSTA, France.

9.2.2. Supervision

- PhD : Julien Loudet, Distributed and Privacy-Preserving Personal Queries on Personal Clouds, UVSQ, October 2019, Luc Bouganim and Iulian Sandu Popa
- PhD: Axel Michel, Secure Distributed Computations, INSA CVL, April 8, 2019, Benjamin Nguyen and Philippe Pucheral
- PhD in progress: Riad Ladjel, Secure Distributed Computation for the Personal Cloud, October 2016, Nicolas Anciaux, Philippe Pucheral and Guillaume Scerri
- PhD in progress: Dimitris Tsoulovos, Privacy-by-design Middleware for Urban-scale Mobile Crowdsensing, April 2017, Nicolas Anciaux and Valérie Issarny (Inria Mimove)
- PhD in progress: Robin Carpentier, Secure and efficient data processing in trusted execution environments for the personal cloud, October 2018, Nicolas Anciaux, Iulian Sandu Popa and Guillaume Scerri

9.2.3. Juries

- Nicolas Anciaux : Jury Member of the PhD of Rémy Delanaux (University Lyon I)
- Philippe Pucheral : President of the PhD jury of Karima RAFES (Paris-Saclay University, 25/01/2019)
- Philippe Pucheral : President of the PhD jury of Duc CAO (Paris-Saclay University, 26/09/2019)

9.3. Popularization

- Nicolas Anciaux: "Sécurité des données personnelles, démonstration de la box 'DomYcile' développée par PETRUS et Hippocad pour le département des Yvelines, Journées du Patrimoine 2019 à l'Inria Rocquencourt, Sept. 2019.
- Nicolas Anciaux: Demonstration of the 'DomYcile' home-box, Inria stand, European Big Data Value Forum (EBDVF19), organized by BDVA in collaboration of the European Commission, Oct. 2019.
- Round table on "Personal Dataspaces" at European Big Data Value Forum (EBDVF19), organized by BDVA in collaboration of the European Commission, Oct. 2019. The round table is chaired by Marko Turpeinen (Director EIT Digital Finland). Intervention of N. Anciaux about "Empowerment and Big Data on personal data: from data portability to personal agency".
- Nicolas Anciaux: séminaire LINC à la CNIL. "Solutions de cloud personnel : sécurité, vie privée, et perspectives", Nov. 2019.
- Nicolas Anciaux: "PETRUS : Cloud personnel de confiance et gestion de nos données", Café des Sciences d'Inria, site de Rocquencourt, 11 juin 2019
- N. Anciaux: Panel on "European Data Protection Law", 10th Annual Forum of Trans Europ Expert 'Le droit de l'Union européenne vu d'ailleurs', Conseil Suprérieur du Notariat, Paris. April 2019. Round table chaired by J. Sénéchal (Dir. pôle "Droit des contrats" at TEE) and N. Martial-Braz (Dir. pôle "Droit de la propriété intellectuelle at TEE), with B. Amaudric du Chaffaut (Deputy General Counsel at Google France) on GDPR evolution in Europe, F. Nicola (Prof. at Washington College of Law) on the echo of GDPR in California and N. Anciaux (researcher at Inria) on technical-juridical challenges of the GDPR.

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] J. LOUDET. *Distributed and Privacy-Preserving Personal Queries on Personal Clouds*, Université de Versailles Saint Quentin en Yvelines (UVSQ), October 2019, https://hal.inria.fr/tel-02376516

[2] A. MICHEL. *Personalizing Privacy Constraints in Generalization-based Anonymization Models*, INSA Centre Val de Loire, April 2019, https://hal.archives-ouvertes.fr/tel-02269565

Articles in International Peer-Reviewed Journals

[3] N. ANCIAUX, P. BONNET, L. BOUGANIM, B. NGUYEN, P. PUCHERAL, I. SANDU-POPA, G. SCERRI. *Personal Data Management Systems: The security and functionality standpoint*, in "Information Systems", 2019, vol. 80, pp. 13-35 [*DOI :* 10.1016/J.IS.2018.09.002], https://hal.archives-ouvertes.fr/hal-01898705

[4] N. ANCIAUX, L. BOUGANIM, P. PUCHERAL, I. S. POPA, G. SCERRI. *Personal Database Security and Trusted Execution Environments: A Tutorial at the Crossroads*, in "Proceedings of the VLDB Endowment (PVLDB)", August 2019, https://hal.inria.fr/hal-02269292

[5] N. ANCIAUX, C. ZOLYNSKI. *Empowerment and Big Data on personal data : from portability to agency*, in "Dalloz IP/IT", 2019, forthcoming, https://hal.inria.fr/hal-02349274

International Conferences with Proceedings

[6] R. LADJEL, N. ANCIAUX, P. PUCHERAL, G. SCERRI. *A manifest-based framework for organizing the management of personal data at the edge of the network*, in "ISD 2019 - 28th International Conference on Information Systems Development", Toulon, France, August 2019, https://hal.archives-ouvertes.fr/hal-02269203

[7] R. LADJEL, N. ANCIAUX, P. PUCHERAL, G. SCERRI. *Trustworthy Distributed Computations on Personal Data Using Trusted Execution Environments*, in "TrustCom 2019 - The 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications / BigDataSE 2019 - 13th IEEE International Conference on Big Data Science and Engineering", Rotorua, New Zealand, August 2019, https://hal.archives-ouvertes.fr/hal-02269207

[8] J. LOUDET, I. SANDU-POPA, L. BOUGANIM. *DISPERS: Securing Highly Distributed Queries on Personal Data Management Systems*, in "VLDB 2019 - 45th International Conference on Very Large Data Bases", Los Angeles, United States, Proceedings of the VLDB Endowment, August 2019, vol. 12, n^{o} 12, 4 p. , https://hal.inria.fr/hal-02269209

[9] J. LOUDET, I. SANDU-POPA, L. BOUGANIM. *SEP2P: Secure and Efficient P2P Personal Data Processing*, in "EDBT 2019 - 22nd International Conference on Extending Database Technology", Lisbon, Portugal, March 2019, https://hal.inria.fr/hal-01949641

Conferences without Proceedings

[10] R. LADJEL, N. ANCIAUX, P. PUCHERAL, G. SCERRI. *Trustworthy Distributed Computations on Personal Data Using Trusted Execution Environments*, in "APVP 2019 - Atelier sur la Protection de la Vie Privée", Cap Hornu, France, July 2019, https://hal.archives-ouvertes.fr/hal-02269200

[11] R. LADJEL, N. ANCIAUX, P. PUCHERAL, G. SCERRI. *Trustworthy Distributed Computations on Personal Data Using Trusted Execution Environments*, in "BDA 2019 - 35ème Conférence sur la Gestion de Données - Principes, Technologies et Applications", Lyon, France, October 2019, https://hal.archives-ouvertes.fr/hal-02269211

[12] J. LOUDET, I. SANDU-POPA, L. BOUGANIM. *DISPERS: Securing Highly Distributed Queries on Personal Data Management Systems*, in "BDA 2019 - 35ème Conférence sur la Gestion de Données - Principes, Technologies et Applications", Lyon, France, October 2019, https://hal.inria.fr/hal-02269201

[13] J. LOUDET, I. SANDU-POPA, L. BOUGANIM. *SEP2P: Secure and Efficient P2P Personal Data Processing*, in "BDA 2019 - 35ème Conférence sur la Gestion de Données - Principes, Technologies et Applications", Lyon, France, October 2019, https://hal.inria.fr/hal-02269222

[14] J. LOUDET, I. SANDU-POPA, L. BOUGANIM. *SEP2P: Secure and Efficient P2P Personal Data Processing*, in "APVP 2019 - Atelier sur la Protection de la Vie Privée", Cap Hornu, France, July 2019, https://hal.inria.fr/hal-02269216