IN PARTNERSHIP WITH:
Université Versailles Saint-Quentin

Activity Report 2018

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

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

PhD Students

Robin Carpentier [Univ de Versailles Saint-Quentin-en-Yvelines]
Dimitrios Tsolovos [Inria]
Riad Ladjel [Inria]
Julien Loudet [CozyCloud]
Axel Michel [INSA CVL]
Paul Tran Van [CozyCloud]

Technical staff

Aydogan Ersoz [Inria]
Laurent Schneider [Inria]

Interns

Robin Carpentier [Inria, from Apr 2018 until Sep 2018]

Baptiste Crepin [Inria, from Apr 2018 until Sep 2018]
Lindia Vanessa Kamtchogom Kenmegne [Inria, from Jun 2018 until Aug 2018]
Yiqun Liu [Inria, from Apr 2018 until Jun 2018]

Administrative Assistants

Adeline Lochet [Inria, from Jun 2018]
Emmanuelle Perrot [Inria]

External Collaborator

Benjamin Nguyen [INSA Centre Val-de-Loire, 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 four 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.

- (Axis 2) Privacy preserving administration models and enforcement. This research axis is devoted to the definition of sharing rules that are easily manageable for the individual and enforced by default (i.e., secure implementation). Complementary to the definition of sharing policies, it is mandatory to help the average user regulate the complete lifecycle of her data, from its capture, to its dissemination and up to its deletion. Our objective is to 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.
- (Axis 3) 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, privacy preserving query processing strategies and data anonymization techniques for the personal cloud.
- (Axis 4) Economic, legal and societal issues. This research axis is more transversal 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. Highlights of the Year

5.1. Highlights of the Year

Creation of the Inria Innovation Lab 'OwnCare'

PETRUS has set up the OwnCare Inria Innovation Lab (IILab) with UVSQ and the Hippocad company in January 2018. The objective of this IILab is to industrialize PlugDB, a flagship software/hardware platform initiated in the SMIS team and today pursued in PETRUS, and deploy it in the medical/social field. A first deployment over 10.000 patients is planned in the Yvelines district (see Section 8.1.1 for details).

6. New Software and Platforms

6.1. 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/

7. New Results

7.1. Extensive and Secure PDMS Architecture (Axis 1)

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

The Personal Cloud paradigm is emerging through a myriad of solutions offered to users to let them gather and manage their whole digital life. This paradigm shift towards user empowerment raises fundamental questions with regards to the appropriateness of the data management functionalities and protection techniques which are offered by existing solutions to laymen users. This year, we reviewed, compared and analyzed personal cloud alternatives in terms of the functionalities they provide and the threat models they target. From this analysis, we derived a general set of security requirements that any Personal Data Management System (PDMS) should consider. We then identified the challenges of implementing such a PDMS and proposed a preliminary design for an extensive and secure PDMS reference architecture satisfying the considered requirements. Finally, we discussed several important research challenges remaining to be addressed to achieve a mature PDMS ecosystem. A first paper making the functionality and security standpoint in PDMS solutions, proposing five security goals and a preliminary architecture to fulfill these goal based on Trusted Execution Environments was published at IS'19 [12], and preliminary results on the case of a crowdsensing architecture was presented at Middleware'18 [15] and BDA'18 [18].

7.2. Data sharing model for the Personal Cloud (Axis 2)

Participants: Nicolas Anciaux [correspondent], Philippe Pucheral, Guillaume Scerri, Paul Tran Van, Baptiste Crepin.

In the PDMS context, new sharing models are needed to help end-users controlling the sharing policies under use. We proposed an architecture to produce authorizations satisfying users' sharing desires without having to trust the underlying producing these authorizations in the PhD thesis of Paul Tran-Van [11] and we demonstrated the solution at EDBT'18 [14]. We currently investigate the case of a data sharing system producing what we call 'zero-knowledge permissions', i.e., a set of authorizations produced by an untrusted sharing model which is supposed to reveal no information at all about a given subset of documents in the user space.

7.3. SEP2P: Secure and Efficient P2P Personal Data Processing (Axis 3)

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? We studied the feasibility of such a pure P2P personal data management system and provide efficient and scalable mechanisms to reduce the data leakage to its minimum with covert adversaries. In particular, we showed that data processing tasks can be assigned to nodes in a verifiable random way, which cannot be influenced by malicious colluding nodes. We proposed a generic solution which largely minimizes the verification cost. Our experimental evaluation shows that the proposed protocols lead to minimal private information leakage, while the cost of the security mechanisms remains very low even with a large number of colluding corrupted nodes. We illustrated our generic protocol proposal on three data-oriented use-cases, namely, participatory sensing, targeted data diffusion and more general distributed aggregate queries. The full protocol was simulated and evaluated. A first paper focusing on imposed randomness was published at EDBT'19 [13].

7.4. Mobile Participatory Sensing with Strong Privacy Guarantees (Axis 3)

Participant: Iulian Sandu Popa [correspondent].

Mobile participatory sensing could be used in many applications such as vehicular traffic monitoring, pollution tracking, or even health surveying. However, its 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 mobile participatory sensing. 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, we propose an enhanced version of the protocol, named PAMPAS$^+$, to make the system robust even against advanced hardware attacks on the SPs. Hence, the user location privacy leakage remains very low even for an attacker controlling the SSI and a few corrupted SPs. The leakage is proportional with the number of corrupted SPs and thus requires a massive SP corruption to break the system, which is extremely unlikely in practice. This work has been accomplished in collaboration with NJIT (see Section 9.2.1.1) and has been recently submitted as a journal paper.

7.5. Trustworthy Distributed Queries on Personal Data using TEEs (Axis 3)

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

The decentralized way of managing personal data in a PDMS provides a de facto protection against massive attacks usually performed on central servers. But this raises the question of how to preserve individuals' trust on their PDMS when performing global computations crossing data from multiple individuals? And how to guarantee the integrity of the final result when it has been computed by a myriad of collaborative but independent PDMSs? We study a secure decentralized computing framework where each participant gains the assurance that his data is only used for the purpose he consents to and that only the final result is disclosed. Conversely, the goal is to provides the querier with the guarantee that this result has been honesty computed, by the expected code on the expected data. A preliminary solution which capitalizes on the use of Trusted Execution Environments (TEE) at the edge of the network was presented at BDA'18 [19] and APVP'18 [20].

7.6. Performance of large scale data-oriented operations under TEE constraints (Axis 3)

Participants: Robin Carpentier [correspondent], Nicolas Anciaux, Iulian Sandu Popa, Guillaume Scerri.

The rise of Trusted Execution Environments like Intel SGX, and their more and more widespread use for data processing raises the question of their impact on performance, specifically for data oriented operations. While some works aim at embedding either the entirety of part of a database engine within a TEE, the direct impact of processing data with TEEs as opposed to more classical environment has not been studied yet. In particular, the cryptographic overhead of accessing persistent data outside the TEE enclave, the limited RAM amount of each TEE enclave, the cost of external function calls and memory access overheads, may slow the computing by orders of magnitude compared to a regular environment, and have to be taken into account. Preliminary results presenting both a benchmark of data operations within Intel SGX, together with optimisation of search algorithm dealing with the specific way of accessing external memory from inside SGX have been presented at BDA'18 [16].

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. 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.

8.2. Bilateral Grants with Industry

8.2.1. Cozy Cloud CIFRE - Tran Van contract (Oct 2014 -Feb 2018)

Partners: Cozy Cloud, PETRUS
Following a bilateral contract with Cozy Cloud (a French startup providing a personal Cloud platform), the CIFRE PhD thesis of Paul Tran Van capitalized on the Cozy-PlugDB platform to devise new access and usage control models to exchange data among devices of the same user (devices may have different levels of trustworthiness) and among different users thanks to a user-friendly sharing model [14].

8.2.2. 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.

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. 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.

9.1.2. PIA - PDP SECSi (May 2016 - Dec 2017)

Partners: Cozy Cloud (coordinator), Qwant, PETRUS (Inria-UVSQ), FING.
The objective of this PIA-PDP (Programme Investissement d'Avenir - Protection des Données Personnelles) SECSi project is to build a concrete Personal Cloud platform which can support a large scale deployment of Self Data services. Three major difficulties are identified and will be tackled in this project: (1) how to implement and enforce a fine control of the data flow when personal data are exploited by third party applications, (2) how to protect these same applications when processing is delegated to the personal cloud platform itself and (3) how to implement personalized search on the web without hurting user's privacy.

9.1.3. CityLab@Inria, Inria Project Lab (May 2014 - Oct 2018)

Inria Partners: ARLES-MIMOVE, CLIME, DICE, FUN, MYRIADS, OAK, PETRUS, URBANET, WILLOW.
External partners: UC Berkeley.
CityLab@Inria studies ICT solutions toward smart cities that promote both social and environmental sustainability. A strong emphasis of the Lab is on the undertaking of a multi-disciplinary research program through the integration of relevant scientific and technology studies, from sensing up to analytics and advanced applications, so as to actually enact the foreseen smart city Systems of Systems. PETRUS contributes to Privacy-by-Design architectures for trusted smart objects so as to ensure privacy to citizens, which is critical for ensuring that urbanscale sensing contributes to social sustainability and does not become a threat. The PhD Thesis of Dimitris Tsoulovos, co-directed by MIMOVE and PETRUS, is funded by CityLab. http://citylab.inria.fr/

9.1.4. GDP-ERE, DATA-IA project (Sept. 2018 - Aug. 2021)

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

9.2. International Research Visitors

9.2.1. Visits to International Teams

9.2.1.1. Research Stays Abroad

Iulian Sandu Popa has visited the Computer Science department of NJIT (New Jersey Institute of Technology) for two months (Mars to April) during 2018. Iulian has a long history of collaboration with this department at NJIT, this being his second long stay since 2011. In particular, he collaborates at NJIT with Professor Vincent Oria on topics related to spatiotemporal data management and with Professor Cristian Borcea on topics such as privacy-preserving mobile computing for location-based applications [5] and secure and distributed crowd-sensing for smart city applications. For the latter topic, a joint journal paper has been recently submitted (see Section 7.4).

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organization

10.1.1.1. Member of the Organizing Committees

- Luc Bouganim: Co-organizer of Ecole thématique BDA Masses de Données Distribuées, Aussois, June 2018
- Iulian Sandu Popa: 34ème Conférence sur la Gestion de Données – Principes, Technologies et Applications (BDA 2018), Bucarest, 22-26 octobre 2018
- Iulian Sandu Popa: Colloque National Capteurs et Sciences Participatives (CASPA), Paris, 1-4 avril 2019

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

- Nicolas Anciaux: VLDB'18, VLDB'19, SIGMOD'19, DATA'18, BDA'18
- Luc Bouganim: Associate Editor for VLDB'18
- Philippe Pucheral: DATA'18, MOBILITY'18
- Iulian Sandu Popa: DATA'18, ICDE'19, IEEE MobileCloud'19

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Nicolas Anciaux: Associate Editor of the VLDB Journal

10.1.3.2. Reviewer - Reviewing Activities

- Iulian Sandu Popa: ACM Transactions on Spatial Algorithms and Systems, IEEE Transactions on Parallel and Distributed Systems, Geoinformatica

10.1.4. Invited Talks

- Iulian Sandu Popa: "Highly Distributed Queries on Personal Data Management Systems with Strong Privacy Guarantees", New Jersey Institute of Technology (NJIT), Newark, April 9, 2018. https://web.njit.edu/cs/CS_Seminar/abstract.php?id=391
- Célia Zolynski and Nicolas Anciaux: "L'avènement d'une gestion individuelle de nos données personnelles. Regards croisés sur certains enjeux de vie privée", Kick-Off of the DATAIA Institute, Fev. 2018. slides: http://petrus.inria.fr/~anciaux/papers/D36.pdf
- Philippe Pucheral: "Privacy-by-Obligation: Une réponse au paradoxe du Cloud Personnel ?", Inria Scientific days, June 28th, 2018.
- Célia Zolynski and Nicolas Anciaux: "GDPR and Personal Cloud: from Empowerment to Responsibility (GDP-ERE)", DATAIA-JST International Symposium on Data Science and AI, July 2018. Link: http://dataia.eu/actualites/dataia-jst-international-symposium-data-science-and-ai, slides: http://dataia.eu/sites/default/files/DATAIA_JST_International_Symposium/DATAIA-JST_SYMPOSIUM_Nicolas_Anciaux_Celia_Zolynski.pdf
- Philippe Pucheral: "Protection de la vie privée : potentiel et paradoxe du Cloud Personnel", SystemX seminar, October 18th, 2018. https://www.irt-systemx.fr/philippe-pucheral-animera-un-seminarsystemx-le-18-octobre/
- Nicolas Anciaux: "Personal Data Management Systems using Trusted Execution Environments", Zenith seminar, Inria / Univ. Montpellier, Nov. 2018. https://team.inria.fr/zenith/zenith-seminar-nicolas-anciaux-personal-data-management-systems-using-trusted-execution-environments-21-nov-2018/

10.1.5. 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: 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

10.2. Teaching - Supervision - Juries

10.2.1. 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. Luc Bouganim, Bases de données relationnelles et XML (niveau M1 et M2), 40, AFTI, 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 et INSA CVL, France.

10.2.2. Supervision

- PhD : Paul Tran Van, Partage de documents sécurisé dans le Cloud Personnel, UVSQ, April 3, 2018, Nicolas Anciaux and Philippe Pucheral
- PhD in progress: Axel Michel, Secure Distributed Computations, October 2015, Benjamin Nguyen and Philippe Pucheral
- PhD in progress : Julien Loudet, Highly Distributed Queries on Personal Data Management Systems with Strong Privacy Guarantees, July 2016, Luc Bouganim and Iulian Sandu Popa
- 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

10.2.3. Juries

- Nicolas Anciaux : Reviewer of the PhD of Sakina MAHBOUBI (Université de Montpellier, 21/11/2018)
- Luc Bouganim : Reviewer of the PhD of Arezki Laga (University of Bretagne Sud, 20/12/2018)

10.3. Popularization

- Nicolas Anciaux: "Respectez les données personnelles de vos clients avec PLUGDB", Inria Tech Talk, French Tech Central - Station F, 12 Dec. 2018. video: https://youtu.be/9y3VdMe_sAQ, slides: https://french-tech-central.com/events/inria-tech-talk-respectez-les-donnees-personnelles-de-vos-clients-avec-plugdb/
- Nicolas Anciaux: auditions de la mission de préfiguration du « Health Data Hub », DREES, July 2018. Slides: http://petrus.inria.fr/~anciaux/papers/D39.pdf
- Nicolas Anciaux: interview, magazine La Recherche N°535, Mai 2018, "IA : les défis de la stratégie française", pp.14-16, by Gautier Cariou. Link: https://www.larecherche.fr/parution/mensuel-535

11. Bibliography

Major publications by the team in recent years

[1] N. Anciaux, L. Bouganim, P. Pucheral, Y. Guo, L. Le Folgoc, S. Yin. *MILo-DB: a personal, secure and portable database machine*, in "Distributed and Parallel Databases", March 2014, vol. 32, n^{o} 1, pp. 37-63 [*DOI :* 10.1007/s10619-012-7119-x], https://hal.archives-ouvertes.fr/hal-00768355

[2] N. Anciaux, S. Lallali, I. Sandu Popa, P. Pucheral. *A Scalable Search Engine for Mass Storage Smart Objects*, in "41th International Conference on Very Large Databases (VLDB)", Kohala Coast, Hawaii, United States, August 2015, vol. 8, n^{o} 9, pp. 910-921 [*DOI :* 10.14778/2777598.2777600], https://hal.inria.fr/hal-01176458

[3] N. Anciaux, B. Nguyen, I. Sandu Popa. *Tutorial: Managing Personal Data with Strong Privacy Guarantees*, in "17th International Conference on Extending Database Technology (EDBT)", Athens, Greece, March 2014, pp. 672-673 [*DOI :* 10.5441/002/edbt.2014.71], https://hal.inria.fr/hal-01096633

[4] S. Lallali, N. Anciaux, I. Sandu Popa, P. Pucheral. *Supporting secure keyword search in the personal cloud*, in "Information Systems", December 2017, vol. 72, pp. 1 - 26 [*DOI :* 10.1016/j.is.2017.09.003], https://hal.inria.fr/hal-01660599

[5] S. J. Pan, I. Sandu Popa, C. Borcea. *DIVERT: A Distributed Vehicular Traffic Re-Routing System for Congestion Avoidance*, in "IEEE Transactions on Mobile Computing", January 2017, vol. 16, n^{o} 1, pp. 58-72 [*DOI :* 10.1109/TMC.2016.2538226], https://hal.inria.fr/hal-01426424

[6] G. Scerri, B. Warinschi, M. Barbosa, B. Portela. *Foundations of Hardware-Based Attested Computation and Application to SGX*, in "IEEE European Symposium on Security and Privacy, EuroS&P 2016", Saarbrücken, Germany, March 2016, pp. 245-260 [*DOI :* 10.1109/EuroSP.2016.28], https://hal.inria.fr/hal-01417137

[7] C. Q. To, B. Nguyen, P. Pucheral. *TrustedMR: A Trusted MapReduce System based on Tamper Resistance Hardware* , in "23rd International Conference on Cooperative Information Systems (COOPIS)", Rhodes, Greece, October 2015, pp. 38-56 [*DOI :* 10.1007/978-3-319-26148-5_3], https://hal.inria.fr/hal-01254951

[8] C. Q. To, B. Nguyen, P. Pucheral. *Private and Scalable Execution of SQL Aggregates on a Secure Decentralized Architecture*, in "ACM Transactions on Database Systems", 2016, vol. 41, n^{o} 3, pp. 16:1-16:43, https://hal.archives-ouvertes.fr/hal-01296432

[9] D. H. Ton That, I. Sandu Popa, K. Zeitouni. *TRIFL: A Generic Trajectory Index for Flash Storage*, in "ACM Transactions on Algorithms", July 2015, vol. 1, n^{o} 2, 44 p. [*DOI :* 10.1145/2786758], https://hal.inria.fr/hal-01176563

[10] P. Tran-Van, N. Anciaux, P. Pucheral. *SWYSWYK: A Privacy-by-Design Paradigm for Personal Information Management Systems*, in "International Conference on Information Systems Development (ISD)", Cyprus, Cyprus, September 2017, https://hal.inria.fr/hal-01675090

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] P. Tran-Van. *Secure document sharing through Personnal Cloud*, Université Paris-Saclay, April 2018, https://tel.archives-ouvertes.fr/tel-01779315

Articles in International Peer-Reviewed Journals

[12] 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",

February 2019, vol. 80, pp. 13 - 35 [*DOI :* 10.1016/J.IS.2018.09.002], https://hal.archives-ouvertes.fr/hal-01898705

International Conferences with Proceedings

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

[14] P. TRAN-VAN, N. ANCIAUX, P. PUCHERAL. *Reconciling Privacy and Data Sharing in a Smart and Connected Surrounding*, in "International Conference on Extending Database Technology (EDBT)", Vienna, Austria, March 2018, https://hal.inria.fr/hal-01675093

[15] D. TSOLOVOS. *Enforcing Privacy in Participatory Sensing Systems*, in "Middleware Doctoral Symposium 2018", Rennes, France, ACM, December 2018, https://hal.inria.fr/hal-01910067

National Conferences with Proceedings

[16] R. CARPENTIER, N. ANCIAUX, I. S. POPA, G. SCERRI. *Performance of Large Scale Data-Oriented Operations under the TEE Constraints*, in "34ème Conférence sur la Gestion de Données – Principes, Technologies et Applications (BDA 2018)", Bucharest, Romania, October 2018, https://hal.inria.fr/hal-01947896

[17] J. LOUDET, L. BOUGANIM, I. SANDU POPA. *Privacy-Preserving Queries on Highly Distributed Personal Data Management Systems*, in "34ème Conférence sur la Gestion de Données – Principes, Technologies et Applications", Bucharest, Romania, Proceedings of the BDA 2018 Conference, October 2018, https://hal.inria.fr/hal-01949583

[18] D. TSOLOVOS, N. ANCIAUX, V. ISSARNY. *A Privacy Aware Approach for Participatory Sensing Systems*, in "34ème Conférence sur la Gestion de Données – Principes, Technologies et Applications", Bucharest, Romania, October 2018, https://hal.inria.fr/hal-01947863

Conferences without Proceedings

[19] R. LADJEL, N. ANCIAUX, P. PUCHERAL, G. SCERRI. *Secure and Distributed Computations for a Personal Cloud*, in "APVP 2018 – l'Atelier sur la Protection de la Vie Privée", porquerolles, France, June 2018, https://hal.inria.fr/hal-01947842

[20] R. LADJEL, N. ANCIAUX, G. SCERRI, P. PUCHERAL. *Secure and Distributed Computations for a Personal Data Management System*, in "34ème Conférence sur la Gestion de Données – Principes, Technologies et Applications", Bucarest, Romania, October 2018, https://hal.inria.fr/hal-01947808

Scientific Books (or Scientific Book chapters)

[21] A. MICHEL, B. NGUYEN, P. PUCHERAL. *The Case for Personalized Anonymization of Database Query Results*, in "Data Management Technologies and Applications (DATA'17 Revised Selected Papers)", J. FILIPE, J. BERNARDINO, C. QUI (editors), Communications in Computer and Information Science, Springer, June 2018, vol. 814, pp. 261-285, https://hal.archives-ouvertes.fr/hal-01945674