INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team SMIS

Secured and Mobile Information Systems

Rocquencourt

THEME SYM

Table of contents

1. Team

Head of project-team
Philippe Pucheral [PR - UVSQ (Civil servant, on partial secondment)]

Vice-head of project team
Luc Bouganim [CR1 - INRIA]

Part-time research scientist (external partner)
Béatrice Finance [MC - UVSQ]

Administrative assistant
Elisabeth Baque [AI - INRIA]

Ph. D. students
Nicolas Anciaux [UVSQ - ATER]
François Dang Ngoc [UVSQ - INRIA]
Sophie Giraud [UVSQ - MEN]
Aurelian Lavric [Paris 6 - INRIA]
Saïda Medjdoub [UVSQ - EGIDE]
Cristian-Augustin Saita [UVSQ (ATER) - INRIA]

Project technical staff
Nicolas Dieu [engineer ENSEEIHT]

Graduate student intern
Cosmin Cremarenco [Ecole Polytechnique de Bucarest]

Previous members
Chun Yuan [Univ. Tsinghua]
Jean-Pierre Matsumoto [Master Paris 6]

2. Overall Objectives

Keywords: *data confidentiality and privacy*, *mobile and embedded databases*.

The emergence of ubiquitous computing (access data anywhere, anyhow, anytime) and ambient intelligence (smart objects, aware of their environment and able to interact with it) introduces the need for embedding various forms of data in even lighter and specialized computing devices (personal digital assistants, cellular phones, chips dedicated to home networks, cars, health, etc). Thus, the first objective of the SMIS project is to study, develop and validate new data management techniques tackling the strong hardware constraints of ultra-light devices.

By making the information more accessible and by multiplying the - sometimes unconscious - ways of acquiring this information, ubiquitous computing and ambient intelligence induce new threats on data confidentiality. More generally, preserving the confidentiality of personal data spread among a large variety of sources (mobiles, smart objects but also corporate, commercial and public databases) has become a major challenge for the database community. The second objective of the SMIS project is therefore to study, develop and validate new models and techniques that preserve data confidentiality.

The complementarity's of these two research issues is twofold. First, ubiquitous data management generates specific confidentiality problems that must be tackled accurately. Second, data management techniques embedded in secured ultra-light devices (e.g., smart cards, secured tokens) can be the foundation for new security models. Thus, a strong cross-fertilization can be expected between these two research actions.

The expected contributions of the SMIS project will take the form of database query execution and optimization techniques, data storage and indexation models, performance evaluation, access control models and secured data management architectures. The planned research in data confidentiality is at the corner

of different scientific domains (among others, databases, cryptography, system and network security). Thus, cooperation's with external teams (inside and outside INRIA) having complementary skills will be sought.

3. Scientific Foundations

3.1. Ubiquitous data management

Keywords: *co-design*, *mobile and embedded databases*, *smart objects*.

The vision of the future dataspace, a physical space enhanced with digital information made available through large-scale networks of smart objects is paint in [47]. This clearly states the need for data management techniques embedded in highly constrained hardware devices. For example, sensor networks collecting weather or pollution data are evolving towards real distributed databases [42] in which each sensor acts as an active node (i.e., as a micro-data server queryable remotely) [49]. Protecting the confidentiality of portable folders (e.g., healthcare folders, users' profiles) is another motivation to embed data management techniques in tamper-resistant devices (e.g., smart cards) [19]. More generally, embedded database techniques are required in every context where computations have to be performed in a disconnected mode.

To conceive embedded database components is however not obvious. Each target architecture is specifically designed to meet desirable properties (portability, energy consumption, tamper resistance, etc) under imposed hardware constraints (maximum silicium die size, memory technology, etc). In addition, these architectures evolve rapidly to catch new applications. The challenge is then twofold: (i) being able to design dedicated embedded database components and (ii) being able to set up co-design rules helping hardware manufacturers calibrating their future platforms to match the requirements of data driven applications. The interactions between smart objects and the global information system opens up also important research problems.

Few research efforts have been placed so far by the database community on embedded database techniques. While light versions of popular DBMS (e.g., Oracle, SQLServer, DB2) have been designed for powerful handheld devices, DBMS vendors never addressed the more complex problem of embedding database components into chips. The LIFL Lab and Gemplus suggested for the first time a reduced SQL-like interface for smart cards [48]. More recent works have been conducted on smart card databases [19] [41] and on data management techniques for sensor networks [54] [49] but this research field is still at a preliminary stage.

3.2. Data confidentiality

Keywords: *access control management*, *data confidentiality*, *data encryption*.

Data confidentiality has become a major concern for individuals as well as for companies and governments [46]. Several kinds of data are threatened: personal data gathered by visited Web sites or by smart objects used in the daily life, corporate databases hosted by untrusted Database Service Providers, central databases subject to piracy. The CSI/FBI reports that database attacks constitute the principal source of cyber-criminology and that more than fifty percents of the attacks are conducted by insiders [43]. In this context, governments are setting up more constraining legislations. The problem is then to translate laws into technological means: authentication mechanisms, data and communication encryption, access control, intrusion detection, data and operation anonymization, privacy preserving data mining, etc. The area of investigation is extremely large. Our research program focuses on access control management and on the ways access control can be made secure (use of encryption and tamper-resistant devices).

Server-enforced access control is widely accepted [39] but remains inoperative against insider attacks. Several attempts have been made to strengthen server-based security with database encryption [50] [45]. However, the Database Administrator (or an intruder usurping her identity) has enough privilege to tamper the encryption mechanism and get the clear-text data. Client-based security approaches have been recently investigated. Encryption and decryption occur at the client side to prevent any disclosure of clear-text data at the server. Storage Service Providers proposing encrypted backups for personal data are crude representative of this approach. The management of SQL queries over encrypted data complements well this approach

[44]. Client-based decryption is also used in the field of selective data dissemination (e.g., Digital Right Management, P2P data exchange). However, the sharing scenarios among users are generally coarse grain and static (i.e., pre-compiled at encryption time). Thus, database encryption and its relationship with access control constitutes an important field of investigation.

In addition, while access control management in a relational database context is well established and normalized, new access control models have to be defined to cope with more complex data (e.g., XML, multimedia streams) and new forms of data distribution (e.g., selective data dissemination).

4. Application Domains

Keywords: *ambient intelligence*, *healthcare*, *home networks*, *sensor networks*, *telecommunication*, *transportation*.

Our work on ubiquitous data management addresses varied application domains. Typically, database components on chip are required each time data-driven applications have to be embedded in ultra-light computing devices. This situation occurs for example in healthcare applications where complex portable folders are embedded into smart cards, in telephony applications where personal data (address book, agenda, etc.) are embedded into cellular phones, in sensor networks where sensors log row measurements and perform local computation on them, in home networks where a collection of smart objects gather information about the occupants to provide them a personalized service, and more generally in most applications related to ambient intelligence.

Meanwhile, mobility and ambient intelligence introduce new threats on data confidentiality and privacy. Indeed, mobility may lead people to store confidential data on untrusted environments (e.g., Database Service Providers, Web-hosting companies) while ambient intelligence makes the gathering of personal data more insidious. Thus, most of the applications mentioned above require new mechanisms to protect the data confidentiality and to better control who is granted access to which data and for which purpose. This concern is in fact general and applies to any situation dealing with personal data. The access control models and techniques developed in our project have therefore a wider application domain than mobility and ambient intelligence. Among others, the digital shared medical folder initiative launched in France (and in other countries) could constitute a valuable domain of experiments for our works on access control models, database encryption and secured smart devices.

5. Software

5.1. Introduction

In our domain of expertise, developing software prototypes is an important mean to validate research solutions. This prototyping task is however difficult since it requires specialized computing devices (e.g., smart cards), themselves sometimes at an early stage of development (see Section 7.1.1). While time consuming, these prototypes are the vector for research publications, for demonstrations at conferences and exhibitions as well as for cooperation's and grants with industry. The recent award (see below) received at the e-gate'04 software contest organized by Axalto, Sun and ST Microelectronics illustrates this strategy.

5.2. PicoDBMS

Participants: Nicolas Anciaux [correspondent], Luc Bouganim, Sophie Giraud, Philippe Pucheral.

As smart cards become multi-application and more and more powerful (32 bit CPU, more than 1MB of stable storage soon), the need for database management arises. PicoDBMS is a full-fledged embedded DBMS (storage, indexation, query processing, access rights and transaction control) addressing this issue. The application domain of PicoDBMS is the management of shared secured portable folders (medical folder, user profile, agenda, etc.). Its indexation and query engines implement new strategies required to cope with

the smart card hardware constraints [19]. A first prototype written in JavaCard has been demonstrated at the VLDB'01 conference [2]. Since then, a second prototype has been written in C and optimized. At the same time, Schlumberger provided us with an experimental smart card platform and modified part of its smart card OS (cf. Section 7.1.1), so that the current prototype exhibits two order of magnitude better performance than its JavaCard counterpart. Extensive experimentations have been done in 2004 on this prototype using a PicoBenchmark defined for embedded applications [24].

5.3. C-SDA

Participants: François Dang Ngoc [correspondent], Luc Bouganim, Nicolas Dieu, Philippe Pucheral.

Several approaches have been proposed to secure databases by means of encryption. Unfortunately, server-based approaches cannot resist to insider attacks while client-based approaches make access control static and coarse grain (cf. Section 3.2). The C-SDA (Chip-Secured Data Access) architecture allows querying encrypted data while controlling fine grain and dynamic personal privileges [10]. C-SDA is a client-based security component acting as an incorruptible mediator between a client and an encrypted database. This component is embedded into a smart card to prevent any tampering to occur on the client side. The CNRS (Centre National de la Recherche Scientifique) took out a patent on C-SDA [11]. A JavaCard prototype has been developed partly with the support of the French ANVAR agency (Agence Nationale pour la VAlorisation de la Recherche) and has been demonstrated at the VLDB'03 conference [13].

5.4. C-SXA

Participants: François Dang Ngoc [correspondent], Luc Bouganim, Cosmin Cremarenco, Nicolas Dieu, Philippe Pucheral.

Chip-Secured XML Access (C-SXA) is an XML-based access rights controller embedded in a smart card. As the de facto standard for describing and exchanging data, XML endows C-SXA with versatile data protection capabilities. C-SXA can evaluate user's privileges on a queried or streaming XML input document and delivers the authorized subset of this same document. User-accessible data can be downloaded from an encryption-protected server or stored on a tamper-resistant smart card. Potential applications span secure portable folders, Digital Rights Management (DRM), parental control and exchange of confidential information among a community of users. C-SXA was the recipient of the Silver Award of the e-gate open 2004 contest organized by Sun, Axalto and ST Microelectronics (84 participating teams from 22 countries) [36]. This awards opens up new industrial cooperation perspectives. A parental control application applied on video streams has also been developed on top of C-SXA and has been demonstrated at the e-smart'04 conference [30]. As for PicoDBMS, this prototype has to be finalized and rewritten in C in order to assess its performance on advanced smart card platforms.

6. New Results

6.1. Ubiquitous data management

Keywords: *benchmarks*, *co-design*, *embedded and ambient databases*, *mobile*, *query evaluation*, *storage and indexation models*, *system on chip*.

Participants: Nicolas Anciaux, Luc Bouganim, Sophie Giraud, Philippe Pucheral.

Preliminary studies led us to design and validate a full-fledged DBMS, called PicoDBMS, embedded in an advanced smart card platform (cf. Section 5.2). The difficult problem is more on tackling the asymmetry between hardware resources (e.g., powerful CPU, tiny RAM) than simply on tackling the resource scarcity. This resource asymmetry entails a thorough re-thinking of existing database techniques [19]. Meanwhile, the rapid evolution and specialization of the hardware platforms motivate the definition of co-design rules to avoid designing ad-hoc techniques from scratch for each new platform [3]. As a first step in this research direction,

we have conducted a comprehensive analysis of the RAM consumption problem. This study provides helpful guidelines to calibrate the RAM resource of a hardware platform according to given application's requirements [4].

Capitalizing on these works, we are today investigating three issues related to the design of embedded database components:

First, we are investigating the impact of different stable storage technologies (EEPROM, Flash, FeRAM, MEMS) on traditional database techniques [27]. Indeed, these memories provide very specific and interesting access properties which impacts database storage, indexation, querying and transaction management.

Second, we generalize the PicoDBMS approach defining a PicoBenchmark. We categorized the different types of queries that may be defined on embedded data and measured the response time and/or the throughput when processing each query type. We investigated different storage and indexation alternatives and assessed their respective performance on an advanced smart card platform and on a cycle accurate hardware simulator provided by Axalto (cf. Section 7.1.1). The conclusions of this performance evaluation allow to decide which database technique/strategy should be embedded in a smart card with respect to a targeted - class of - application [24].

Third, we study the interactions between the ultra-light device(s) and the external information system. Typically, an embedded database component could be used to process (e.g., filter, query, modify) an external flow of information (e.g., data broadcasted by a server in a publishing environment). An external server can also be used as a secondary storage system where part of an embedded database can be swapped [24]. As storage resources, computing resources can be shared as well. For example, a smart card database component can take advantage of the computing resources of the terminal hosting the card reader. The way storage and CPU resources can be externalized is governed by different factors like the device's communication bandwidth and the confidentiality attached to the data.

6.2. Data confidentiality

Keywords: *access control models*, *data confidentiality and privacy*, *database encryption*, *querying encrypted data*, *smart cards and secured computing platforms*.

Participants: Luc Bouganim, François Dang Ngoc, Béatrice Finance, Saïda Medjdoub, Philippe Pucheral, Chun Yuan.

While encryption has been used successfully for years to secure communications, database encryption introduces new theoretical and practical issues [26], such as: how to execute efficiently database queries over encrypted data, how to conciliate declarative (i.e., predicate based) access rights with encryption, how to take advantage of secured computing devices? This research action tries to provide some answers to these questions by devising chip-secured models for querying, updating and sharing encrypted databases. In a previous work [10][11], we proposed a solution called C-SDA (Chip-Secured Data Access), which allows querying encrypted data while controlling predicate-based personal privileges. C-SDA is embedded into a smart card to prevent any tampering to occur on the client side. This cooperation of hardware and software security components allows reestablishing the orthogonality between access right management and data encryption.

C-SDA has been designed in a relational database context with a pull (i.e., client/server) interaction model in mind. However, XML has become a de-facto standard to store, describe and exchange complex (i.e., semi-structured and hierarchical) data according to either a pull or push model. Taking into account XML data changes drastically the problem of access right definition and access right control. We start two research actions in this direction.

The first work, named Chip-Secured XML Access (C-SXA), shares some similarities with C-SDA, namely embedding an access right controller in a smart card. However, this work considers XML data and assumes a push model where a server disseminates encrypted data towards a population of clients having different privileges on these data. This leads to technical solutions rather different from the C-SDA ones. We proposed a streaming evaluator of access control rules based on non-deterministic automata and designed a streaming index structure allowing skipping the irrelevant (i.e. forbidden) parts of the input XML document [31].

Additional security mecanisms guarantee that prohibited data can never be disclosed during the processing and that the input document is protected from any form of tampering [25]. A first prototype of C-SXA has been developed and has been the recipient of the Silver Award of the e-gate open 2004 contest (cf. Section 5.4) [30][36].

The second work studies extensions of state of the art access control models for XML. Indeed, existing models attach authorizations to nodes of an XML document but disregard relationships between nodes. However, ancestor and sibling relationships may reveal information as sensitive as the one carried out by the nodes themselves (e.g., classifications, correlations). We advocate the integration of relationships as first class citizen in the access control models for XML. We characterized three essential classes of relationship authorizations and identified the mechanisms required to translate them accurately in an authorized view of a source document [34]. A rule-based formulation for expressing these classes of relationship authorizations and an associated conflict resolution strategy has also been proposed. An experimental evaluation is still on-going.

Both actions are still on-going and will be pursued in 2005.

6.3. Other results

Keywords: *Enterprise Information Integration*, *mediation systems*, *publish-subscribe systems*, *scientific dataflows*.

Participants: Aurelian Lavric, Jean-Pierre Matsumoto, Cristian-Augustin Saita.

As detailed in the SMIS full-text project proposal [35], organizational issues led us to reframe the scientific objectives of the team around the ubiquitous data management and data confidentiality issues. Two PhD students and one engineer continued however working on the resource mediation issue this year.

Cristian-Augustin Saita works on publish-subscribe notification systems and he is interested in the case where the subscriptions and the events specify range intervals for their attributes. Cristian is developing a cost-based adaptive clustering method for large collections of multidimensional extended objects (hyper-intervals or hyper-rectangles), aiming at improving the performance of spatial queries (e.g., to check whether a notification is satisfied) [33]. Cristian plans to defend his PhD thesis in the first half of 2005.

Aurelian Lavric works on data mediation in the EII (Enterprise Information Integration) context. This context introduces the need for data integration solutions providing fast local data acquisition times, fast online verifications and a high degree of freshness for the integrated data. Aurelian considers the problem of consistent answering to EII integration queries, providing execution algorithms for online verification of integrated data in the context of redundant and potentially inconsistent data sources. Aurelian plans to defend his PhD thesis in the first half of 2005.

Jean-Pierre Matsumoto worked as engineer on scientific dataflow systems until September 2004. His system is built above data mediation tier and enables designing data analysis and interpretation processing chains as scientific dataflow. Target applications are today's scientific applications where knowledge is not centralized, participants are autonomous and a high-level language is required to abstract data and programs. This work contributes to an ANVAR innovation program and to the Padoue ACI (cf. Sections 7.1.2 and 8.1.3).

7. Contracts and Grants with Industry

7.1. National grants

7.1.1. Axalto (Schlumberger)

Category: bipartite cooperation
Duration: unbounded
Partners: Axalto, INRIA-SMIS (correspondent: P. Pucheral)
Description: The SMIS project has a long lasting cooperation with the smart card subsidiary of Schlumberger (formerly Bull-CP8, then SchlumbergerSema and now Axalto). Axalto provides SMIS with advanced smart

card platforms, cycle accurate simulators and a strong technical support. SMIS exploits these tools to conduct experiments and performance measurements on different prototypes (cf. Sections 5. and 6.).

7.1.2. ANVAR

Category: ANVAR innovation program
Duration: October 2003 - December 2004
Partners: Médience, INRIA-SMIS (correspondent: J-P Matsumoto)
Description: The objective of this ANVAR program is to complement a software prototype of a powerful mediation system with dedicated wrappers. A mediation system helps defining (and querying) a uniform and integrated view of a collection of distributed and heterogeneous information sources. This prototype has been initially developed by former members of the SMIS team (E. Simon, F. Llirbat, F. Fabret) who launched the Médience startup in 2003. Médience aims at selling this mediation system and developing services on top of it.

7.2. European grants

7.2.1. Ankh-Morpork (A-213 MEDEA+)

Category: MEDEA+ project (Eureka program)
Duration: July 2003 - September 2004 (3-year project labelled in May 2003 but stopped after 1 year due to a budget cut from the French Ministry of Industry)
Partners: Philips, Thomson, Schlumberger, STM, Canal+, Esterel, Cryptolog, INRIA-SMIS (correspondent: P. Pucheral)
Description: This project aimed at ensuring the safety of data contents (i.e., preventing content piracy and infringement of copyrights) and services associated with a home network towards all its connection links. The involvement of SMIS in this project concerned the preservation of user's privacy and the support of non-lucrative access right models (e.g., parental control, free access for educational purpose, etc).

8. Other Grants and Activities

8.1. National grants

8.1.1. ACI CASC

Category: ACI Sécurité
Duration: July 2003 - July 2006
Partners: INRIA-SMIS (CASC coordinator: L. Bouganim), ENS Ulm, LRI, ENST-Bretagne, Univ. Pau
Description: The CASC project focuses on access right management and data confidentiality preservation. More precisely, the goal is to tackle three important weaknesses of existing DBMS access control models: the inability to deal with the complexity of distributed and decentralized organizations, the semantics fuzziness of access control policies when applied to semi-structured and hierarchical data, and the vulnerability of a centralized administration of access rights. The CASC project expects significant advances in the following areas: (i) abstraction of the fundamental concepts required in any access right model and formalization of the associated administration procedures, (ii) definition of a powerful and sound access right model for XML documents and (iii) definition of chip-secured data access and administration architectures. Link: http://www-smis.inria.fr/~bouganim/CASC.

8.1.2. ACI DataGraal

Category: ACI GRID
Duration: June 2002 - June 2004
Partners: INRIA-Regal, INRIA&PRiSM-SMIS (correspondent: B. Finance), IRISA, LISI, LIP, LIP6, LSR-IMAG, ID-IMAG, Hewlett-Packard Labs, N2P3, LIRMM

Description: This project brings together researchers from the distributed system community and from the database community as well as people working on GRID applications. The work done in this project takes the form of regular workshops. A summer school, named DRUIDE, is being organized and will be held at Port-aux-rocs in May 2004. Link: http://www-src.lip6.fr/projets/datagraal.

8.1.3. ACI Padoue

Category: ACI GRID
Duration: June 2002 - June 2005
Partners: LIP6, INRIA-SMIS (correspondent: J-P. Matsumoto), Cemagref, LICS, UMR 3S, CDS, LIRMM, IRD
Description: The Padoue project (Partage des données pour des utilisations en environnement) aims at building a uniform and integrated view of a collection of distributed and heterogeneous environmental information sources. More precisely, the goals of SMIS in the project are: (i) to design wrappers providing a better interoperability with both data and program sources, (ii) to design tools to develop scientific workflows on top of existing program resources. Link: http://www-poleia.lip6.fr/padoue.

8.2. International and national cooperations

The SMIS members have developed international cooperation with the following persons/institutions:

- Mike Franklin (UC Berkeley USA): Collaboration on embedded database systems.
- Philippe Bonnet (DIKU, Denmark): Collaboration on embedded database systems.
- Alejandro Gutiérrez (INCO, Uruguay): long lasting cooperation with INCO. Daniel Calegari has spent 3 months at INRIA (first quarter 2004) thanks to the INRIA-INCO internship program to work on data confidentiality. Juan Diego Ferre will spend 3 months in the same context during the first quarter 2005.
- Chun Yuan (Univ. Tsinghua, China): Post-doctoral fellow (august 2003-august 2004). Cooperation on database encryption.
- Mohamed Ben Ahmed (RIADI, Tunisia): collaboration on the medical applications of PicoDBMS.

At the national level, SMIS members cooperate with several French labs and universities through national projects (see sections 7. and 8.).

9. Dissemination

9.1. Scientific activity and coordination

9.1.1. Collective responsibilities within INRIA

Philippe Pucheral is member of the Bureau du Comité des Projets (project council) of INRIA Rocquencourt since September 2004. He is correspondent for the Mission Formation par la Recherche (Training through Research) and then responsible for the relationships between INRIA Rocquencourt and the Parisian universities.

Luc Bouganim was member of the Comité des Bourses of INRIA Rocquencourt from March 2003 to October 2004. He is member of the Commission Délégations-Détachements of INRIA Rocquencourt since November 2004. Finally, he is the INRIA representative for the summer schools in computer science co-organized by INRIA, CEA and EDF.

Béatrice Finance was member of the Commission Délégations-Détachements of INRIA Rocquencourt up to October 2004.

9.1.2. Collective responsibilities outside INRIA

The SMIS members have conducted, or participated to, the following actions in the research community:

- Philippe Pucheral

- PC member of ACM SIGMOD'04, UbiCom'04, Xsymp'04, SSI'04, BDA'04.
- Member of the Scientific Board of the ACI « Masses de données », a 3-year research program launched by the French Ministry of Research in 2003.
- Member of the CNRS expert committee evaluating the LRI Lab (University of Orsay) in 2004.
- Scientific expert for evaluating the creation of a joint research project in the Franco-Mexican LAFMI lab in 2004.
- Member of the BDA Board (Bases de Données Avancées) since 2002.
- Member of the commission de spécialistes -A- (CSE) 27th section of the universities of Versailles/St-Quentin, Paris X and Cergy.
- Lecturer in DRUIDE'04, summer school on large scale data distribution architectures (DistRibUtIon de Données à grande Echelle).
- Member of the PhD jury of Marie Thilliez (Univ. Valenciennes).

- Luc Bouganim

  - Coordinator of the ACI "Sécurité Informatique" CASC
  - Demonstrations Co-Chair of ACM SIGMOD'04
  - PC member of IDEAS'04, BDA'04, SBBD'04, DMNS'04
  - Member of the Editorial Board of TSI Journal (Technique et Science Informatiques)
  - Co-organizer of DRUIDE'04, summer school on large scale data distribution architectures (DistRibUtIon de Données à grande Echelle).

- Béatrice Finance

  - PC member of BDA'04.
  - Co-organizer of DRUIDE'04, summer school on large scale data distribution architectures (DistRibUtIon de Données à grande Echelle).
  - Member of the Scientific Board of the UFR de sciences of the University of Versailles/St-Quentin.
  - Member of the Administration Board of the ISTY engineering school since 1998.
  - Member of the commissions de spécialistes -B- (CSE) 27th section of the University of Versailles/St-Quentin.

9.2. Teaching activity

The SMIS members have tight links with the University of Versailles/St-Quentin (UVSQ). Béatrice Finance is indeed assistant professor at UVSQ and Philippe Pucheral is professor at UVSQ, on secondment at INRIA. The list of the main courses given by each staff member in 2004 is given below:

- P. Pucheral: co-director of the Master COSY (UVSQ), course on DBMS architecture (40h).
- L. Bouganim: DBMS architecture, data security, database technology (100h, given at UVSQ, ENS Cachan, ENST Paris).
- B. Finance: database technology, programming languages, mediation systems, distributed object systems (240h, given at UVSQ). Also responsible for the 3rd year of the ISTY engineering school.
- N. Anciaux: database technology, programming languages (96h given at UVSQ).
- F. Dang Ngoc: network administration, network programming (60h given at ISTY).
- S. Giraud: elements of computer science, programming languages (122h given at UVSQ).
- A. Lavric: database technology, advanced databases (88h given at Paris V and Paris VII).
- J. P. Matsumoto: database technology, DBMS architecture (80h given at PULV).
- C.-A. Saita: elements of computer science, initiation to databases (75h given at UVSQ).

The SMIS members have supervised a project involving eight students from the ISTY engineering school.

10. Bibliography

Major publications by the team in recent years

[1] M. ABDALLAH, R. GUERRAOUI, P. PUCHERAL. *Dictatorial Transaction Processing : Atomic Commitment without Veto Right*, in "Distributed and Parallel Database Journal (DAPD)", vol. 11, nº 3, 2002.

[2] N. ANCIAUX, C. BOBINEAU, L. BOUGANIM, P. PUCHERAL, P. VALDURIEZ. *PicoDBMS : Validation and Experience*, in "Proc. of the Int. Conf. on Very Large Data Bases (VLDB), Rome, Italy", 2001.

[3] N. ANCIAUX, L. BOUGANIM, P. PUCHERAL. *Database Components on Chip*, in "ERCIM News", vol. 54, 2003.

[4] N. ANCIAUX, L. BOUGANIM, P. PUCHERAL. *Memory Requirements for Query Execution in Highly Constrained Devices*, in "Proc. of the Int. Conf. on Very Large Data Bases (VLDB), Berlin, Germany", 2003.

[5] G. BERNOT, G. BRUNO, C. COLLET, B. FINANCE, Z. KEDAD, D. LAURENT, F. TAHI, G. VARGAS-SOLAR, T. T. VU, X. XUE. *Deliverable MEDIAGRID PL-9, 'Etat de l'art'*, Technical report, 2003, http://www-lsr.imag.fr/mediagrid.

[6] C. BOBINEAU, L. BOUGANIM, P. PUCHERAL, P. VALDURIEZ. *PicoDBMS : Scaling down Database Techniques for the Smartcard*, in "Proc. of the 26th Int. Conf. on Very Large Data Bases (VLDB)", 2000.

[7] L. BOUGANIM, F. FABRET, C. MOHAN, P. VALDURIEZ. *A Dynamic Query Processing Architecture for Data Integration Systems*, in "IEEE Data Engineering Bulletin", vol. 23, nº 2, 2000.

[8] L. BOUGANIM, F. FABRET, F. PORTO, P. VALDURIEZ. *Processing Queries with Expensive Functions and Large Objects in Distributed Mediator Systems*, in "Proc. of the 17th Int. Conf. on Data Engineering (ICDE)", 2001.

[9] L. BOUGANIM, F. FABRET, P. VALDURIEZ, C. MOHAN. *Dynamic Query Scheduling in Data Integration Systems*, in "Proc. of the 16th Int. Conf. on Data Engineering (ICDE)", 2000.

[10] L. BOUGANIM, P. PUCHERAL. *Chip-Secured Data Access : Confidential Data on Untrusted Servers*, in "Proc. of the Int. Conf. on Very Large Data Bases (VLDB), Hong-Kong, China", 2002.

[11] L. BOUGANIM, P. PUCHERAL. *Procédé de sécurisation de bases de données, Patent deposit by the CNRS in august 2001, request for PCT (USA, Europe, Canada, Japan) in august 2002, end of the examination phase in august 2003*, 2003.

[12] L. BOUGANIM, F. DANG NGOC, P. PUCHERAL. *Composant de sécurité C-SXA : spécifications techniques*, Technical report, Final deliverable TR_CSXA_0203, programme d'innovation ANVAR, 2003.

[13] L. BOUGANIM, F. DANG NGOC, P. PUCHERAL, L. WU. *Chip-Secured Data Access : Reconciling Access Right with Data Encryption*, in "Proc. of the Int. Conf. on Very Large Data Bases (VLDB), demo session, Berlin, Germany", 2003.

[14] C. CREMARENCO. *ActiveXML peer on mobile devices, Proc. of the Int. Workshop on Emerging Database Research in Eastern Europe, colocated with VLDB'03, Berlin*, 2003.

[15] B. FINANCE, P. DECHAMBOUX, G. LEBRUN, Y. LEPETIT, T. DELOT. *LDAP, Databases and Distributed Objects : Towards a Better Integration*, in "Int. Workshop on Databases in Telecommunications, colocated with the Int. Conf. on Very Large Data Bases (VLDB), LNCS 2209, Springer 2001, ISBN 3-540-42623X, 140-154", 2001.

[16] B. FINANCE, Z. KEDAD. *Médiations d'informations via les méta-données*, Technical report, Contributions to the final deliverable of CNRS/STIC RTP09, also published as a short version in Journées Bases de Données Avancées (BDA), 2003.

[17] I. MANOLESCU, L. BOUGANIM, F. FABRET, E. SIMON. *Interrogation efficace de ressources distribuées dans des systèmes de médiation*, in "Techniques et Sciences Informatiques (TSI)", vol. 22, n° 10, 2003.

[18] MEDIAGRID PROJECT. *A mediation framework for a transparent access to biological data sources*, in "Proc. of the Entity-relationship Conf. (ER), Chicago, USA", 2003.

[19] P. PUCHERAL, L. BOUGANIM, P. VALDURIEZ, C. BOBINEAU. *PicoDBMS : Scaling down Database Techniques for the Smartcard*, in "Very Large Data Bases Journal (VLDBJ), Best Paper Award VLDB'2000", vol. 10, n° 2-3, 2001.

[20] P. PUCHERAL, ET AL. *Mobilité et bases de données : état de l'art et perspectives*, in "Technique et Science Informatiques (TSI)", vol. 22, n° 3&4, 2003.

[21] P. PUCHERAL. *Bilan de l'AS CNRS Mobilité/Accès aux données*, Technical report, Final deliverable AS19_RTP09, short version published in BDA'03 (Journée Bases de Données Avancées), 2003.

[22] P. PUCHERAL (EDITOR). *Bases de Données Avancées : modèles, systèmes et usages*, in "Technique et Science Informatiques (TSI)", vol. 22, n° 10, 2003.

[23] G. VARGAS-SOLAR, J. ZECHINELLI-MARTINI, D. SOL-MARTINEZ, N. CRUZ-RAMIREZ, A. OLIART-ROS, P. VELASCO-ELIZONDO, C. COLLET, B. FINANCE, Z. KEDAD. *Spatial data integration from distributed and heterogeneous sources*, 2003, Proceedings of the Workshop on Advances in Databases and Information Retrieval, Tlaxcala, Mexico.

Doctoral dissertations and Habilitation theses

[24] N. ANCIAUX. *Systèmes de gestion de bases de données embarqués dans une puce électronique*, Ph. D. Thesis, University of Versailles, France, December 2004.

Articles in referred journals and book chapters

[25] L. BOUGANIM, F. DANG NGOC, P. PUCHERAL. *Tamper-Resistant Ubiquitous Data Management*, in "Int Journal of Computer Systems Science and Engineering (IJCSSE), Special Issue on Mobile Databases", to appear, 2005.

[26] P. PUCHERAL. *Ubiquité et confidentialité des données*, in "book chapter, CNRS Edition", to appear, 2004.

[27] P. PUCHERAL, ET AL. *Mobile Databases : a Selection of Open Issues and Research Directions*, in "ACM Sigmod Record, collective report written under the supervision of P. Pucheral", vol. 33, n° 2, 2004.

[28] B. B. ZHU, C. YUAN, Y. WANG, S. LI. *Scalable Protection for MPEG-4 Fine Granularity Scalability*, in "IEEE Transaction on Multimedia", to appear.

Publications in Conferences and Workshops

[29] M. ADIBA, F. BANCILHON, C. COLLET, J. LE MAITRE, P. PUCHERAL, M. SCHOLL. *Table ronde: Bilans et perspectives de 20 ans de recherche en bases de données*, in "Proc. of the 20èmes Journées Bases de Données Avancées (BDA), Montpellier, France", 2004.

[30] L. BOUGANIM, F. DANG NGOC, P. PUCHERAL. *A Smart XML Access Right Controller for Mobile Applications*, in "Proc. of the 5th e-Smart Int. Conf., Sophia Antipolis, France", 2004.

[31] L. BOUGANIM, F. DANG NGOC, P. PUCHERAL. *Client-Based Access Control Management for XML Documents*, in "Proc. of the 30th Int. Conf. on Very Large Databases (VLDB), Toronto, Canada", 2004.

[32] C. COLLET, K. BELHAJJAME, G. BERNOT, C. BOBINEAU, G. BRUNO, B. FINANCE, F. JOUANOT, Z. KEDAD, D. LAURENT, F. TAHI, G. VARGAS-SOLAR, T.-T. VU, X. XUE. *Towards a Mediation System Framework for Transparent Access to Largely Distributed Sources. The MediaGrid Project.*, in "Semantics for Grid Databases, First International IFIP Conference on Semantics of a Networked World: ICSNW 2004, Paris, France, June 17-19, 2004. Revised Selected Papers", Lecture Notes in Computer Science, vol. 3226, Springer,

2004, p. 65-78.

[33] C.-A. SAITA, F. LLIRBAT. *Clustering Multidimensional Extended Objects to Speed Up Execution of Spatial Queries*, in "Proc. of the Int. Conf. on Extending Database Technology (EDBT), Heraklion, Greece", 2004.

Internal Reports

[34] B. FINANCE, S. MEDJDOUB, P. PUCHERAL. *The Case for Access Control on XML Relationships*, to appear, Rapport de Recherche, n° 5446, INRIA, 2005, http://www.inria.fr/rrrt/rr-5446.html.

Miscellaneous

[35] *SMIS full text project proposal*, 2004, http://www.egateopen.axalto.com/egateopen2004_result.asp.

[36] L. BOUGANIM, F. DANG NGOC, P. PUCHERAL. *Chip-Secured XML Access, Silver Award of the e-gate open 2004 contest delivered at the 14th CardTech/SecurTech (CTST) Int. Conf.*, 2004, http://www.egateopen.axalto.com/egateopen2004_result.asp.

Bibliography in notes

[37] A. ABOU EL KALAM, R. EL-BAIDA, P. BALBIANI, S. BENFERHAT, F. CUPPENS, Y. DESWARTE, A. MIEGE, C. SAUREL, G. TROUESSIN. *Organization based access control*, in "Proc. of the 4th Int. Workshop on Policies for Distributed Systems and Networks", 2003.

[38] R. AGRAWAL, J. KIERNAN, R. SRIKANT, Y. XU. *Hippocratic Databases*, in "Proc. of the 28th Int. Conf. on Very Large Data Bases (VLDB)", 2002.

[39] A. BARAANI, J. PIEPRZYK, R. SAFAVI-NAINI. *Security In Databases: A Survey Study*, in "online", 1996, http://citeseer.ist.psu.edu/baraani-dastjerdi96security.html.

[40] E. BERTINO, S. CASTANO, E. FERRARI, M. MESITI. *Specifying and Enforcing Access Control Policies for XML Document Sources*, in "WWW journal, Baltzer Science Publisher", vol. 3, n° 3, 2000.

[41] C. BOLCHINI, F. SALICE, F. SCHREIBER, L. TANCA. *Logical and Physical Design Issues for Smart Card Databases*, in "ACM Transactions on Information Systems", 2003.

[42] P. BONNET, J. GEHRKE, P. SESHADRL. *Towards Sensor Database Systems*, in "Mobile Data Management", 2001.

[43] COMPUTER SECURITY INSTITUTE. *CSI/FBI Computer Crime and Security Survey*, in "online", 2002, http://www.gocsi.com/forms/fbi/pdf.html.

[44] H. HACIGUMUS, B. IYER, C. LI, S. MEHROTRA. *Executing SQL over Encrypted Data in the Database-Service-Provider Model*, in "Proc. of the Int. Conf. On Management of Data (ACM SIGMOD)", 2002.

[45] J. HE, M. WANG. *Cryptography and Relational Database Management Systems*, in "Proc. of the Int. Database and Engineering and Application Symposium (IDEAS)", 2001.

[46] IBM-HARRIS. *IBM survey of consumer attitudes toward privacy in the United States, the United Kingdom and Germany*, in "online", 1999, http://www.securitymanagement.com/library/ibm_priv.html.

[47] T. IMIELINSKI, B. NATH. *Data, data everywhere*, in "Proc. of the 28th Int. Conf. on Very Large Data Bases (VLDB)", 2002.

[48] INTERNATIONAL STANDARDIZATION ORGANIZATION (ISO). *Integrated Circuit(s) Cards with Contacts - Part 7: Inter industry Commands for Structured Card Query Language (SCQL)*, in "ISO/IEC 7816-7", 1999.

[49] S. MADDEN, M. FRANKLIN, J. HELLERSTEIN, W. HONG. *The Design of an Acquisitional Query Processor for Sensor Networks*, in "Proc. of the Int. Conf. On Management of Data (ACM SIGMOD)", 2003.

[50] ORACLE CORPORTION. *Advanced Security Administrator Guide*, in "Release 10.1", 2003.

[51] ST MICROELECTRONICS. *ST22FJ1M: 1MB Flash smartcard IC*, 2004.

[52] B. SCHNEIER. *Applied Cryptography*, in "book, 2nd Edition, John Wiley & Sons", 1996.

[53] J.-P. TUAL. *MASSC: A Generic Architecture for Multiapplication Smart Cards*, in "IEEE Micro Journal, N° 0272-1739/99", 1999.

[54] Y. YAO, J. GEHRKE. *The Cougar Approach to In-Network Query Processing in Sensor Networks*, in "SIGMOD Record", 2002.

[55] H. YU, D. AGRAWAL, A. EL ABBADI. *Tabular Placement of Relational Data on MEMS-based Storage Devices*, in "Proc. of Int. Conf. On Very Large Databases (VLDB), Berlin, Germany", 2003.