Alberto Trombetta
Dipartimento di Scienze Teoriche e Applicate, Università dell'Insubria
Via Ottorino Rossi 9 , 21100, Varese, Italy
tel. +390332218945, +390312386377 email: alberto.trombetta@uninsubria.it

1 Education

- PhD in Computer Science, University of Torino, Italy, 2001
- Laurea in Computer Science, University of Milano, Italy, 1993

2 Professional experience

- Post-doc, Department of Computer Science, University of Milano, Italy, 2001-2002
- Visiting Researcher, Department of Industrial Engineering, Israel Institute of Technology (Technion), Haifa, Israel, Summer 2002
- Visiting Assistant Professor, Department of Computer Sciences, Purdue University, West Lafayette, IN, USA, Summer-Fall 2006
- Assistant Professor (Researcher), Department of Theoretical and Applied Sciences (formerly Department of Information and Communication Sciences), University of Insubria, Varese, Italy, December 2002 – September 2014
- Associate Professor, Department of Theoretical and Applied Sciences, University of Insubria, Varese, Italy, October 2014 – present

3 Research interests and projects

Current works

Security, privacy, and verifiability in data management and analysis

We have studied how to query and update obfuscated data in several scenarios, including encrypted or anonymized repositories or data streams.

Our setting assumes that both the database owner and the data owner are passive, i.e. they strictly follow the protocol and (possibly) learn information by looking at data gathered during the protocol execution. Even in this simplified case, our solutions imply the formulation of non-trivial protocols based on well-known cryptographic primitives. An approach using novel attribute-based cryptographic schemes have been proposed in order to enforce user-defined access policies to sensitive information selectively published in information networks (e.g. online social networks). The deployment of cryptographic schemes like —emphhidden vector encryption is particularly desirable since it allows for a decentralized approach to the

enforcement of access policies. A related, more efficient cryptographic approach has been proposed in order to process SQL-like queries in a private way over an obfuscated database in a private way. Such an approach is orders of magnitude more efficient than other approaches offering the same security level.

In the context of hardware-based security, we have studied the problem of assessing the quality – in terms of measured entropy – of randomness of bitstreams generated by Quantum True Number Generators (QTRNGs)

In collaboration with IBM Research Europe (Dublin), we have proposed techniques for computing SVM-based classifiers in a federated setting with cryptographically protected parameters. Concurrently, we have proposed techniques for verifying the results of an SVM federated classifier using an efficient Zero-Knowledge protocol.

Less recent research topics include:

We have defined extensions to role-based access control in order to model basic components of privacy policies (such as - for example - purposes and obligations) and to provide direct support for expressing complex privacy policies. We have studied the expressive power of such an approach by defining fundamental properties that are relevant to a vast majority of privacy policies (along the lines of what has been done for security policies, e.g. *least privilege* and *separation of duties* properties) and proving these properties are expressible in our model. Furthermore, we compare our approach with existing languages for expressing privacy policy, such as P3P and EPAL.

We have designed and implemented security mechanisms in data-intensive process networks that underlie the correct behavior of almost every critical infrastructure, such as power grids. Such a task is far from trivial since such very specialized distributed systems have very strict constraints, e.g. regarding availability, which is usually extremely high, and computing power of their terminal devices, which is usually very limited. We have investigated the problem of how to add resilience to a wide class of such systems when attacked by malware. Further, we have provided a secure implementation of a widely adopted process network transmission protocol in order to enforce authenticated communication, and we have defined and implemented a novel type of intrusion detection system to be adopted in process networks. This work is done in collaboration with the EU Joint Research Centre (JRC) at Ispra and ENI Corp. at San Donato Milanese. The proposed techniques have been tested in real-world infrastructures.

Data management and analysis in distributed/parallel architectures

We have designed and built several distributed architectures dealing with data acquisition and analysis in real-world scenarios in industrial and domotic settings, in collaboration with the Italian Research Council (CNR, STIIMA Institute).

We have proposed cloud-based, serverless architectures for efficiently performing advanced data reduction and analysis on large scientific datasets, in collaboration with the National Institute for Astrophysics (INAF, Brera Observatory). In particular, we have designed, implemented, and tested in

real-world scenarios an efficient and scalable cloud-based architecture for computing Monte Carlo Markov chain computations over galaxy clusters' data extracted from the publicly available astronomical surveys.

Past works

Fault tolerance

We have studied fault-tolerant, binary search procedures (known as *Ulam's games*), finding simple yet optimal search strategies, in the case that the search process tolerates up to two faults.
In an applied context, we have studied the problem of fault-tolerant trust management. We have proposed extensions of the *TRUST-*$\mathcal{X}$ trust management system in order to apply asynchronous, message-based, checkpointing techniques suitable for mobile environments. We have extended our framework in order to support negotiations among groups of peers, allowing for long-lasting (i.e. spanning over possibly very long time intervals) negotiations. This has implied a rethinking of both the negotiation language, which has been significantly enriched, and the architecture of the framework.

Trust Management

Trust management is a promising way for establishing through a negotiation process a distributed access control policy between initially untrusting parties. Aside from the previously mentioned (fault-tolerance related) extensions, our work has followed other directions. Namely, we have extended *TRUST-*$\mathcal{X}$ in order to provide support for trust negotiations among peers' groups. The *TRUST-*$\mathcal{X}$ architecture has been modified in order to allow a special peer to become the coordinator of its group and carry on trust negotiations on behalf of the others member. The trust negotiation language provided by the system has been accordingly extended in order to define highly expressive and flexible negotiation policies, protecting sensible resources of the group peers. The proposed techniques have been tested in the context of critical infrastructures' protection and in securing the dynamic bandwidth allocation in cognitive radio systems, in collaboration with the JRC at Ispra.

Data integration and data quality

There are lots of well-known, different approaches to heterogeneous data integration. We have proposed a framework in which represent a vast number of different data integration approaches for evaluating their fitness in matching relational data from different sources. We have identified a large and significant class of relational data mappings (termed *monotone* mappings), for which their fitness' evaluation is very simple and accurate. A relevant feature of the integration of heterogeneous datasets is to assess the quality of the data itself. In respect, we have proposed a methodology that assess the quality of data based on whether they satisfy (or not) integrity constraints called *conditional functional dependencies*. It is well-known that testing the satisfaction of cfds has been proven to be np-hard and thus it

becomes important to discover efficient algorithms and heuristics that yield approximate solutions to this relevant problem. In particular, we propose efficient, techniques aimed at discovering particular classes of cfds on given datasets borrowed from relevant, real-world scenarios.

Business process management

Starting from the OMG standard Business Process Management Notation (BPMN), we have studied the problem of how equip it with sound conceptual foundations. This effort has resulted in a conceptual model for BPMN, whose main features are included in the new version of the standard. Further, we have defined a design methodology for the definition and refinement of business processes using BPMN starting from high-level directives and (usually incomplete and heterogeneous) documentation. Finally, we have extended the notation in order to take into account in the business process representations security-related issues, like views management and privacy policies. The work done has lead our research team to be included in the task force for the standardization of BPMN 2.0, led by OMG. The work on design methodology for complex data models has led to the definition of a general methodology for building an ontology starting from term glossaries.

Management of imprecise data

We have investigated extensions to the Relational Model in order to faithfully represent imprecisely defined data. The proposed extension is based on fuzzy set theory. Extensions to the Relational Algebra (based on fuzzy logic), providing a powerful query language for such extended data model, are defined as well. We have studied the optimization of queries expressed in such query language proving significant equivalences among algebraic expressions that are relevant in the query optimization process. We have also studied the problem of how to represent the quality of data in large, heterogeneous repositories and we have devised methodologies for data quality assessment.

Query languages for semistructured data

We have defined an SQL-like query language – called *eWebSQL* – for querying and restructuring data published on the Web. Being eWebSQL defined on top of the extended relational algebra previously presented, it can easily express relevance-based, nearest neighbour and top-k queries. Furthermore, eWebSQL query execution is optimized by the deployment of the equivalences proved for the extended relational algebra.
We have proposed a sound translation of a very expressive XSLT fragment into an extension of a well-known XML query algebra, called *XTAX*, in order to study equivalence and containment problems for such XSLT fragment. We have proved several XTAX equivalences. Being our translation sound, we use such XTAX equivalence for evaluating whether stylesheets written in our XSLT fragment yield the same results. As in the case of eWebSQL, this is a crucial step for studying XSLT optimization. We have studied how to

manage the evolution of semistructured data in collaborative environments – e.g. wikis – integrating reputation systems in order to semi-automatically drive and regulate modifications and updates in both data and schemas.

Projects & agreements

- *Methodologies and Technologies for Data Management over Internet and Intranets (INTERDATA)*, funded by Italian Ministry of University and Research, 1997-99
- *Integration, Warehousing and Mining of Heterogeneous Sources (D2I)*, funded by Italian Ministry of University and Research, 2000-02
- *Metadata Imprecision in Heterogeneous Data Sources*, jointly funded by Italian and Israeli Research Councils, 2001-02
- *Web Access to Health Services for Alzheimer Patients (AZWeb)*, funded by Fondazione CARIPLO, 2003-04
- *Virtual Communities for Education (VICE)*, funded by Italian Ministry of University and Research, 2003-05
- *EU Integrated Project IST-0015964 Algorithmic Principles for Building Efficient Overlay Computers (AEOLUS)*, coordinator of the Insubria site, 2006-09
- *Digital and Legal Methods for Protecting Privacy and Anonymity (ANONIMO)*, funded by MIUR, 2007-09
- *Security Issues in Critical Infrastructures*, funded by JRC, coordinator of the Insubria site, 2009
- *Semantic Web-Supported Repositories of Veterinary Images (ImmaBase)*, funded by Istituto Zooprofilattico Sperimentale della Lombardia e dell'Emilia-Romagna, coordinator of the Insubria site, 2010-12
- *Applications for the Innovative Monitoring of Elderly Communities (AMICA)*, funded by Regione Lombardia, coordinator of the Insubria site, 2011-12
- *Made-in-Italy Fashion Identity and Originality (MiFido)*, funded by Ministero delle Attività Produttive, 2010-2012
- *Storage and Analysis of Log Data in Large Industrial Process Networks*, coordinator of the Insubria site, funded by ENI Corp., 2011-2012
- *Searching Encrypted Relational Data with Inner Product-based Cryptographic Schemes*, funded by an Amazon Research Grant, 2016.
- *Distributed Architectures for Data Management and Analysis in Domotic and Industrial IoT*, CNR-Insubria Joint Agreement, 2018-present.

- *Secure Data Management and Analysis*, IBM-Insubria Joint Agreement, 2019-present.
- *Scientific Data Analysis in the Cloud*, INAF-Insubria Joint Agreement, 2019-present.

4 Scientific and professional activities

- Italian National Institute of Astrophysics (INAF), associate
- Association for Computing Machinery (ACM), member
- IFIP Working Group 11.10 Protection of Critical Infrastructures, member
- European Association of Theoretical Computer Science (EATCS) Italian Chapter, member
- EU Commission, independent expert for the evaluation of H2020 framework projects' proposals
- Chair of networking and information security track of *ICIT '17* (international conference), co-chair of poster track of *CompSac '12* (international conference)
- Program committee member of *Itrust '08* (international workshop), *IEEE ICDE '09* (international conference), *W3C WWW '09* (international conference), *IEEE ACIS '10* (international conference), *BPM '12* (international conference), *AAI '12* (international conference), *FUN'12* (international workshop), *BPM '13* (international conference), *CAINE '13* (international conference), *BPM '14* (international conference), *SocNet '14* (international workshop), *BPM '15* (international conference), *CAINE '16* (international conference), *Service Computation '17* (international conference), *ITASEC '17* (national conference), *ACM CPSS '17* (international workshop), *CAINE '19* (international conference), *IIAI AAI '20* (international conference), *CAINE '20* (international conference) *HEALTHINF'23* (international conference), *IIAI AAI '23* (international conference),*HEALTHINF'24* (international conference), *IEEE Cyber Security and Resilience'24* (international conference)
- Referee activity for *Acta Informatica* (international journal), *Information Sciences* (international journal), *Data and Knowledge Engineering* (international journal), *IEEE Security & Privacy* (international journal), *IEEE Transactions on Dependable and Secure Computing* (international journal), *IEEE Transactions on Network and Service Management* (international journal), *VLDB Journal* (international journal), *IEEE Transactions on Reliability* (international journal)

5 Teaching experience

Undergraduate courses

- TA of *Information Theory* and *Cryptography*, University of Milano: 1998-1999
- TA of *Database Systems*, Insubria University: 2000-2001
- *Database Systems*, Insubria University: 2002-2009
- *Database Systems Laboratory*, Insubria University: 2002-2009, 2012, 2023-
- *Data Management for Communication Science Majors*, Insubria University: 2000-2005
- *Data Security*, Insubria University: 2006-2010
- *Distributed Systems*, Insubria University: 2009-2021
- *Advanced Models for Data Management*, Insubria University, 2012-
- *Laboratory of software engineering, concurrent and distributed programming and database systems (Lab II)*, Insubria University: 2012-2014
- *Introduction to Programming*, Insubria University: 2014-2022
- *Foundations of Security*, Insubria University: 2022-
- *Foundations of Distributed Ledgers*, Insubria University: 2022-
- Starting from year 2000, I have tutored more than 150 undergraduate and master theses.

Graduate courses

- *Parallel Computing*, Insubria University, 2017
- *Topics in Cryptography*, Insubria University, 2021

6 Selected seminars, short courses and talks

- *Optimal strategies in Ulam's games*, Karlsruhe University, Germany, 1996
- *The AZWeb project*, Insubria University, Italy, 2003
- *Open source database systems*, Insubria University, Italy, 2004
- *XSLT optimization techniques*, Camerino University, Italy, 2004
- *Introduction to cryptography*, Insubria University, Italy, 2005

- *Security and privacy issues in data management*, Camerino University, Italy, 2005
- *Integration of biological data sources*, Insubria University, Italy, 2006
- *Answering queries using pairings*, Nanyang Technological University, Singapore, 2012

7 Ph.D. students

- Michele Chinosi (2008), *Representing business processes: conceptual model and design methodology*, now at DIGIT DG EU Commission, Brussels, Belgium
- Stefano Braghin (2010), *Advanced techniques in trust negotiations*, now at IBM Research Europe, Dublin, Ireland
- Antonella Zanzi (2012), *Data quality evaluation through data quality rules and data provenance*, now at EU Joint Research Centre, Ispra, Italy
- Andrea Carcano (2012), *Advanced security aspects of industrial control networks*, now at Nozomi Networks (founder), San Francisco, US
- Lorenzo Bossi (2013), *Reputation assessment in collaborative environments*, now at Google, Dublin, Ireland
- Marco Taddeo (2014), *A real-time framework for malicious behavior discovery on Android mobile devices*, now at Sistemi Ufficio srl, Varese, Italy
- Masoomeh (Bahar) Sepehri (co-tutor with Ernesto Damiani, 2017) *Efficient and secure data sharing using attribute-based cryptography*, now at Huawei Labs, Munich, Germany
- Gianfranco Modoni (2017) *An integrative framework for cooperative production resources in smart manufacturing*, now at National Research Council (CNR), Bari, Italy
- Daniele Spoladore (2022), *A novel and validated agile Ontology Engineering methodology for the development of ontology-based applications*, now at National Research Council (CNR), Milan, Italy
- Simone Bottoni (2023), *Secure Privacy-preserving techniques for federated machine learning*, now at Insubria University, Varese, Italy
- Fabio Castagna (2023) *A serverless architecture for efficient and scalable Markov Chain Monte Carlo computations*, now at National Institute of Astrophysics (INAF), Milan, Italy
- Andrea Scaudo (2024) *Advanced Simulation Frameworks and Machine Learning Techniques for Multi-Wavelength Astronomy*, now at National Institute of Astrophysics (INAF), Milan, Italy

- Cesare Gerolimetto Fabrello (Co-tutor with Massimo Caccia, 2025) *Quantum Random Generators in Differential Privacy*, now at RandomPower, Como, Italy

- Antonio Peluso (expected 2027)

8 Publications

International refereed journal papers

1. D. Mundici, A. Trombetta,
   Optimal comparison strategies in Ulam's searching game with two errors.
   Theoretical Computer Science, 182(1-2): 217-232, 1997

2. D. Montesi, A. Trombetta,
   An Imprecision-based query language for the Web.
   Journal of Visual Languages and Computing, 12(1): 3-35,2001

3. E. Bertino, D. Montesi, A. Trombetta,
   Workflow architecture for interactive video management systems.
   Distributed and Parallel Databases, 11(1): 33-51, 2001

4. A. Trombetta, D. Montesi, P. Dearnley,
   A similarity based relational algebra for Web and multimedia data.
   Information Processing and Management, 39(2): 307-322, 2003

5. A. Gal, A. Trombetta, A. Anaby-Tavor, D. Montesi,
   A framework for modelling and evaluating automatic semantic reconciliation.
   VLDB Journal, 14(1): 50-67, 2005

6. A. Trombetta, D. Montesi,
   Equivalences and optimizations in an expressive XSLT subset.
   Acta Informatica, 42(6-7): 515-539, 2006

7. A. Trombetta, M. Chinosi,
   Integrating privacy policies into business processes.
   Journal of Research and Practice in Information Technology, 41(2): 155-170, 2009

8. I. Nai Fovino, A. Trombetta, A. Carcano,
   An experimental investigation of malware attacks on SCADA systems.
   International Journal of Critical Infrastructures Protection, 2(4), 2009

9. I. Nai Fovino, A. Trombetta, S. Braghin,
   Advanced trust negotiations in critical infrastructures.
   International Journal of Critical Infrastructures, 6(3): 225-245, 2009

10. A. Trombetta, Q. Ni, E. Bertino, J. Lobo, C. Brodie, C. M. Karat, J. Karat,
    Privacy-aware role-based access control.

ACM Transactions on Information and System Security (TISSEC), 13(3): 1-31, 2010

11. A. Squicciarini, A. Trombetta, S. Braghin, E. Bertino, F. Paci,
Group-based negotiations in P2P systems.
IEEE Transactions on Parallel and Distributed Systems

12. A. Trombetta, W. Jiang, E. Bertino, L. Bossi,
Privacy-preserving updates to anonymous and confidential databases.
IEEE Transactions on Dependable and Secure Computing (TDSC), 8(4): 578-587, 2011

13. I. Nai Fovino, A. Trombetta, A. Carcano, M. Guglielmi, A. Coletta, M. Masera,
A multidimensional critical state analysis for detecting intrusions in SCADA systems.
IEEE Transactions on Industrial Informatics (TII), 7(2): 179-186, 2011

14. A. Squicciarini, A. Trombetta, S. Braghin, E. Bertino,
A flexible approach to multi-session trust negotiations.
IEEE Transactions on Dependable and Secure Computing (TDSC), 9(1): 16-29, 2012

15. M. Chinosi, A. Trombetta,
BPMN: an introduction to the standard.
Computer Standards & Interfaces, 34(1): 124-134, 2012

16. S. Braghin, A. Trombetta, G. Baldini, I. Nai Fovino,
Distributed access control policies for spectrum sharing.
Security and Communication Networks, 6(8):925-935, 2013

17. G. Modoni, M. Veniero, A. Trombetta, M. Sacco, S. Clemente,
Semantic based events signaling for AAL systems.
Journal of Ambient Intelligent and Humanized Computing, 9(5):1311-1325, 2018

18. M. Sepehri, M. Sepheri, A. Trombetta,
Secure cloud data sharing using an efficient inner-product proxy re-encryption scheme.
Journal of Cyber Security and Mobility, 6(3):339-378, 2018

19. G. Modoni, D. Mourtzis, M. Sacco, A. Trombetta, M. Veniero,
An event-driven integrative framework enabling information notification among manufacturing resources.
International Journal of Computer Integrated Manufacturing, 32(3):241-252, 2019

20. D. Spoladore, A. Mahroo, A. Trombetta, M. Sacco,
ComfOnt: a semantic framework for indoor comfort and energy saving in smart homes.
Electronics, 8(12), doi: 10.3390/electronics8121449, 2019

21. D. Spoladore, A. Mahroo, A. Trombetta, M. Sacco,
DOMUS: a domestic ontology-managed ubiquitous system.
Journal of Ambient Intelligent and Humanized Computing, 13(6): 3037-3052, 2022

22. M. Perillo, G. Persiano, A. Trombetta,
Secure selections on encrypted multi-writer streams. *ACM Transactions on Privacy and Security (TOPS)*, 25(1):7-33, 2022

23. D. Spoladore, M. Sacco, A. Trombetta,
A Review of Domain Ontologies for Disability Representation. *Expert Syst. Appl.*, 228:120467, 2023

24. D. Spoladore, E. Pessot, A. Trombetta,
A Novel Agile Ontology Engineering Methodology for Supporting Organizations in Collaborative Ontology Development. *Comput. Ind.*, 151:103979, 2023

Book chapters, newsletters, other

1. P. Ciaccia, D. Montesi, W. Penzo, A. Trombetta,
Fuzzy query languages for multimedia data.
Design and Management of Multimedia Information Systems: Opportunities and Challenges,
M.R. Syed editor, Idea Group Publishing, Hershey, PA, US, 2000

2. M. Chinosi, A. Trombetta,
A design methodology for BPMN.
2009 BPM and Workflow Handbook,
Workflow Management Coalition, Lighthouse Point, FL, US, 2009

3. A. Trombetta, W. Jiang, E. Bertino,
Advanced privacy-preserving data management and analysis.
Privacy and Anonymity in Information Management Systems,
J. Herranz, J. Nin Editors, Advanced Information and Knowledge Processing Springer Series, Springer Verlag, Heidelberg, Germany, 2010

4. A. Trombetta, G. Modoni,
Strengthening the Cybersecurity of Manufacturing Companies: A Semantic Approach Compliant with the NIST Framework, in *ERCIM News*, 2018(114), 2018

5. A. Trombetta,
Search on encrypted multi-writer tables,
Encyclopedia of Cryptography, Security and Privacy, Springer, (3rd edition) 2021

6. several articles about security and privacy themes on the site *www.agendadigitale.eu* (in italian), 2018-19

International refereed conference/workshop/symposium papers

1. D. Montesi, A. Trombetta,
   An extraction language for the Web,
   in *Proc. of ACM CIKM Workshop on Internet Data Management.* Washington, US, November 1998

2. E. Bertino, D. Montesi, A. Trombetta,
   Interactive video management systems,
   in *Proc. of Conference on Computer Science and Information Technologies.* Moscow, Russia, January 1999

3. D. Montesi, A. Trombetta,
   Similarity search through fuzzy similarity algebra,
   in *Proc. of IEEE DEXA Workshop on Similarity Search.* Firenze, Italy, September 1999

4. E. Bertino, D. Montesi, A. Trombetta,
   Data, query and answer imprecision through fuzzy and presentation algebras,
   in *Proc. Int'l. Conf. on Fuzzy Set Theory and Applications.* Liptowsky Mikulas, Slovak Republic, January 2000

5. P. Ciaccia, D. Montesi, W. Penzo, A. Trombetta,
   Imprecision and user preferences in multimedia queries: a generic algebraic approach,
   in *Proc. of EATCS Conference on Foundations of Information and Knowledge Systems.* Burg, Germany, February 2000

6. E. Bertino, D. Montesi, A. Trombetta,
   Fuzzy and presentation algebras for Web and multimedia data,
   in *Proc. of Int'l Database Engineering & Application Symposium (IDEAS'00).* Yokohama, Japan, September 2000

7. D. Montesi, A. Trombetta, P. Dearnley,
   A query language for user-defined Web restructurings,
   in *Proc. Int'l. Conf. on Information Technology.* Las Vegas, US, April 2001

8. S. Castano, D. Montesi, A. Trombetta,
   A fuzzy language for querying reconciliated views,
   in *Proc. Int'l Workshop on Databases, Documents, and Information Fusion (DBFusion'02)*, Karlsruhe, Germany, July 2002

9. D. Montesi, A. Trombetta,
   Imprecision Based Queries Over Materialized and Virtual Integrated Views.
   in*Proc. ICEIS Conference*, Angers, France, April 2003

10. A. Gal, A. Trombetta, A. Anaby-Tavor, D. Montesi,
    A Model for schema integration in heterogeneous databases,

in *Proc. of Int'l Database Engineering & Application Symposium (IDEAS'03)*, Hong Kong, China, July 2003

11. A. Anaby-Tavor, A. Gal, A. Trombetta,
Evaluating matching algorithms: the monotonicity principle,
in *Proc. IIWeb IJCAI Workshop*, Cancun, Mexico, August 2003

12. A. Trombetta, D. Montesi,
Equivalences and optimizations in an expressive XSLT fragment,
in *Proc. of Int'l Database Engineering & Application Symposium (IDEAS'04)*, Coimbra, Portugal, July 2004

13. M. Benini, A. Trombetta, M. Acquaviva,
A model for short-term content adaptation,
in *Proc. Int'l. World Wide Web Conference* (poster session), Chiba, Japan, May 2005

14. M. Benini, A. Trombetta, M. Acquaviva,
Short-term content adaptation in web-based learning systems,
in *Proc. IASTED Int'l. Conf. on Web Technologies, Applications and Services (WTAS'05)*, Calgary, Canada, July 2005

15. C. Ghiselli, L. Bozzato, A. Trombetta, E. Binaghi,
Semantic Web meets virtual museums; the *Domus Naturae* project,
in *Proc. ICHIM'05 Conference*, Paris, France, September 2005

16. C. Ghiselli, L. Bozzato, A. Trombetta,
Representation and management of ontologies in cultural heritage domains,
in *Proc. SWAP Italian Semantic Web Workshop*, Trento, Italy, December 2005

17. A. Trombetta, E. Bertino,
Private updates to anonymous databases,
in *Proc. IEEE Int'l. Conf. on Data Engineering (ICDE'06)*, Atlanta, US, April 2006

18. Q. Ni, A. Trombetta, E. Bertino, J. Lobo,
Privacy-aware role-based access control,
in *Proc. ACM Symp. on Access Control Methods And Technologies (SACMAT'07)*, Antibes, France, June 2007

19. A. Squicciarini, A. Trombetta, E. Bertino,
Robust and secure interactions in open distributed systems through recoverable trust negotiations,
in *Proc. IEEE Int'l. Conf. on Distributed Computing Systems (ICDCS'07)*, Toronto, Canada, June 2007

20. A. Coen-Porisini, P. Colombo, S. Sicari, A. Trombetta,
A conceptual model for privacy policies,
in *Proc. IASTED Int'l. Conf. on Software Engineering Applications (SEA'07)*, Boston, US, November 2007

21. A. Squicciarini, A. Trombetta, A. Bharghav-Spantzel, E. Bertino, k-anonymous attribute-based access control, in *Proc. Int'l. Conf. on Information and Computer Security (ICICS'07)*, Zhengzhou, China, December 2007.

22. A. Trombetta, W. Jiang, E. Bertino, L. Bossi, Privately updating suppression and generalization based k-anonymous databases, in *Proc. Int'l. Conf. on Data Engineering (ICDE'08)*, Cancun, Mexico, April 2008.

23. S. Braghin, A. Coen-Porisini, P. Colombo, S. Sicari, A. Trombetta, Introducing privacy in an hospital information system, in *Proc. ACM ICSE Int'l. Workshop on Software Engineering for Secure Systems (SESS'08)*, Leipzig, Germany, May 2008.

24. I. Nai Fovino, A. Trombetta, Information driven association rule hiding, in *Proc. IEEE Int'l. Conf. on Information Technology*, Gdansk, Poland, May 2008.

25. M. Chinosi, A. Trombetta, Integrating privacy policies into business processes, in *Proc. ICEIS Int'l. Workshop on Security in Information Systems (WOSIS'08)*, Barcelona, Spain, June 2008.

26. I. Nai Fovino, A. Trombetta, A. Carcano, Scada malware, a proof of concept, in *Proc. Int'l Workshop on Critical Information Infrastructure Security (CRITIS'08)*, Frascati, Italy, October 2008.

27. A. Squicciarini, A. Trombetta, E. Bertino, S. Braghin, Identity-based long running negotiations, in *Proc. Int'l Workshop on Digital Identity Management (DIM'08)*, Fairfax, US, October 2008.

28. I. Nai Fovino, A. Trombetta, S. Braghin, Advanced trust negotiations in critical infrastructures, in *Int'l Conf. on Infrastructure Systems (NGInfra'08)*, Rotterdam, the Netherlands, November 2008.

29. L. Bozzato, M. Ferrari, A. Trombetta, Building a domain ontology from glossaries: a general methodology, in *Proc. Italian Semantic Web Workshop (SWAP'08)*, Rome, Italy, December 2008.

30. A. Carcano, I. Nai Fovino, A. Trombetta, M. Masera, A secure Modbus protocol, in *IFIP WG 11.10 Int'l Conf. on Critical Infrastructure Protection*, Hanover, US, March 2009.

31. M. Chinosi, A. Trombetta,
Modelling and validating BPMN diagrams,
in *Int'l Workshop on BPMN (BPMN'09)*, Vienna, Austria, July 2009.

32. M. Chinosi, A. Trombetta,
An enhanced XSchema model for BPMN,
in *Proc. Int'l Workshop on Schema Languages for XML*, Riga, Latvia, September 2009.

33. A. Carcano, I. Nai Fovino, A. Trombetta, M. Masera,
State-based network intrusion detection system for scada protocols, a proof of concept,
in *Proc. Int'l Workshop on Critical Information Infrastructure Security (CRITIS'09)*, Bonn, Germany, October 2009.

34. I. Nai Fovino, A. Trombetta, A. Carcano, M. Masera, M. Guglielmi,
A distributed critical state detection system for industrial protocols,
in *IFIP WG 11.10 Int'l Conf. on Critical Infrastructure Protection*, Washington, US, March 2010.

35. S. Braghin, A. Trombetta, G. Baldini, I. Nai Fovino,
Adaptive and distributed access control in cognitive radio networks,
in *Proc. IEEE Int'l Conf. on Advanced Information Networking and Applications (AINA'10*), Perth, Australia, April 2010.

36. I. Nai Fovino, A. Trombetta, A. Carcano, M. Guglielmi, M. Masera,
Modbus/DNP3 state-based intrusion detection system,
in *Proc. IEEE Int'l Conf. on Advanced Information Networking and Applications (AINA'10*), Perth, Australia, April 2010.

37. I. Nai Fovino, A. Trombetta, A. Carcano, M. Guglielmi, M. Masera,
State-based firewall for industrial protocols with critical-State prediction monitor,
in *Proc. Int'l Workshop on Critical Information Infrastructure Security (CRITIS'10)*, Athens, Greece, September 2010.

38. S. Braghin, A. Trombetta, E. Ferrari,
Combining access control and trust negotiations in an on-line social network,
in *Proc. Int'l Conf. on Collaborative Computing (CollaborateCom'10)* (invited paper), Chicago, US, October 2010.

39. S. Braghin, A. Trombetta, E. Ferrari,
A rule-based policy language for selective trust propagation in social networks,
in *Proc. ACM SIGMOD Workshop on Databases and Social Networks (DBSocial'11)*, Athens, Greece, June 2011.

40. S. Braghin, V. Iovino, G. Persiano, A. Trombetta,
Secure and policy-private resource sharing in an online social network,
in *Proc. IEEE Int'l Conf. on Social Computing (SocialCom'11)*, Boston, US, October 2011.

41. L. Bossi, A. Trombetta,
A wiki-based system for schema and data evolution,
in *Proc. XML Prague Conference*, Prague, Czech Republic, February 2012.

42. L. Bozzato, S. Braghin, A. Trombetta,
A method and guidelines for the cooperation of ontologies and relational databases in Semantic Web applications,
in *Proc. Workshop on Semantic Digital Archives (SDA'12)*, Pafos, Cyprus, September 2012.

43. L. Bossi, A. Trombetta, S. Braghin, A. Datta,
A framework for trust-based multidisciplinary team recommendation,
in *Proc. Int'l Conf. on User Modeling, Adaptation and Personalization (UMAP'13)*, Rome, Italy, June 2013.

44. A. Zanzi, A. Trombetta,
Data quality evaluation of scientific datasets – a case study in a policy support context,
in *Proc. Int'l Conf. on Data management Technologies and Applications (Data'13)*, Reykjavik, Iceland, July 2013.

45. M. Taddeo, A. Trombetta, D. Montesi, S. Pierantozzi,
Querying data across different legal domains,
in *Proc. of Int'l Database Engineering & Application Symposium (IDEAS'13)*, Barcelona, Spain, October 2013.

46. G. Baldini, A. Trombetta, M. Taddeo, I. Nai Fovino, V. Mathieu,
Identity-based security systems for vehicular ad-hoc networks,
in *Proc. of Int'l Conf. of Connected Vehicles (ICCVE'13)*, Las Vegas, US, December 2013.

47. L. Bossi, S. Braghin, A. Trombetta,
A multidimensional reputation network for service composition in the Internet Of Things,
in *Proc. of the IEEE Int'l Conf. on Services Computing (SCC'13)*, Anchorage, US, June 2014.

48. A. Zanzi, A. Trombetta,
Discovering non-constant conditional functional dependencies with built-in predicates,
in *Proc. Int'l Conf. on Databases and Expert Systems (DEXA'14)*, Munich, Germany, September 2014.

49. A. Trombetta, G. Persiano, S. Braghin,
Processing private queries over an obfuscated database using hidden vector encryption,
in *Proc. Nordic Conf. on Secure IT Systems (NordSec'14)*, Tromsø, Norway, October 2014.

50. M. Perillo, G. Persiano, A. Trombetta,
Secure queries over an encrypted multi-writer table,

in *Proc. IEEE European Symposium on Security and Privacy (EuroS&P'17)*, Paris, France, April 2017.

51. M. Sepehri, A. Trombetta,
Secure and efficient data sharing with a lightweight attribute-based proxy re-encryption scheme,
in *Proc. Int'l Workshop on Cyber Crime (IWCC'17)*, Reggio Calabria, Italy, September 2017.

52. E. Damiani, M. Sepehri, M. Sepheri, A. Trombetta,
An efficient cryptography-based access control system using inner-product proxy re-encryption scheme,
in *Proc. Int'l Conference on Availability, Reliability and Security (ARES'18)*, Hamburg, Germany, August 2018.

53. D. Spoladore, M. Mondellini, M. Sacco, A. Trombetta,
An ontology-based framework for a less invasive domestic management system,
in *Proc. Int'l Conference on Intelligent Environments*, Madrid, Spain 2020.

54. A. Trombetta, L. Asquini, M. Landoni et al.,
The SOXS scheduler for remote operation at LaSilla: concept and design,
in *Proc. of Society of Photo-Optical Instrumentation Engineers (SPIE) Conference*, 2020.

55. S. Bottoni, S. Braghin, T. Brisimi, A. Trombetta,
Privacy-preserving distributed support vector machines,
in *Proc. Poly/DMAH VLDB Workshop*, Virtual, 2021.

56. D. Spoladore, T. Cilsal, A. Mahroo, M. Sacco, A. Trombetta,
Towards an ontology-based decision support system to support car reconfiguration for novice wheelchair users,
in *Proc. Int'l Conference ICCHP-AAATE*, Lecco, Italy, 2022.

57. S. Bottoni, S. Braghin, A. Trombetta, S. Venugopal,
Adaptive replication strategy in highly distributed data management systems,
in *Proc. IEEE Int'l Conference on Cloud Engineering*, Asilomar, US, October 2022.

58. S. Bottoni, S. Braghin, A.Trombetta, G. Zizzo,
Verifiable federated learning,
in *Proc. NeurIPS Workshop on Federated Learning*, New Orleans, US, December 2022.

59. S. Bottoni, A. Datta, F. Franzoni, E. Ragnoli, R. Ripamonti, C. Rondanini, G. Sagirlar, A. Trombetta,
1DLT: Rapid deployment of secure and efficient evm-based blockchains,
in *Proc. Int'l Conf. on Blockchain Economics, Security and Protocols (Tokenomics'22)*, Paris, France, December 2022.

60. S. Bottoni, A. Trombetta, F. Bertini, D. Montesi, F. Bonin, A. Pascale, M. Gleize, P. Tommasi,
GASTon: a graph-exploration system for indexing, annotating and visualizing PubMed articles to enhance the analysis of social determinants,
in *Proc. Int'l Conf. on Health Informatics (HEALTHINF'23)*, Lisbon, Portugal, March 2023.

61. S. Bottoni, A. Trombetta, F. Bertini, D. Montesi, F. Bonin, A. Pascale, M. Gleize, P. Tommasi,
A graph-based tool for exploring PubMed knowledge base,
in *Proc. IEEE Int'l. Conf. on Data Engineering (ICDE'23)*, Anaheim, US, April 2023.

62. S. Andreon, F. Castagna, M. Landoni, A. Trombetta,
A serverless architecture for efficient and scalable Monte Carlo Markov Chain computations,
in *Proc. Int'l Conf. on Cloud and Big Data Computing (ICCBDC'23)*, Manchester, UK, August 2023.

63. C. Caratozzolo, V. Rossi, K. Vitek, M. Caccia, A. Trombetta,
On-line anomaly detection and qualification of random bit streams,
in *Proc. IEEE Cyber Security and Resilience Conference (CSR'24), Best Paper Award*, London, UK, September 2024.

64. C. Gerolimetto Fabrello, V. Rossi, M. Caccia, A. Trombetta,
Detection and resolution of periodic artifacts in OpenDP's discrete Laplace sampler,
in *Proc. IEEE Cyber Security and Resilience Conference (CSR'26)*, Lisboa, Portugal, August 2026.

65. C. Gerolimetto Fabrello, V. Rossi, M. Caccia, A. Trombetta,
Empirical analysis of randomness quality in differential privacy mechanisms,
in *Proc. IEEE Cyber Security and Resilience Conference (CSR'26)*, Lisboa, Portugal, August 2026.

66. V. Botta, S. Bottoni, M. Campanelli, E. Ragnoli, A. Trombetta,
qedb: Expressive and modular verifiable databases (without snarks),
in *Proc. ACM Conference on Computer and Communications Security (CCS'26)*, The Hague, The Netherlands, November 2026.