Curriculum Vitae et Studiorum

of Antonino Nocera

1 Studies

1.1 University Studies

- On March 2013, he got his PhD under the supervision of Prof. Domenico Ursino. The title of his thesis is "Analyzing, Modeling and Exploiting Social Internetworking Scenarios".
- On November 2009, he passed the State exam to practice as an Engineer.
- On July 2009, he completed his MsC in Telecommunication Engineering (summa cum laude). The title of his thesis is: "Recommendation of reliable users, resources and Social Networks in a Social Internetworking System".
- On November 2006 he completed his BsC (summa cum laude).
- From October 2009 to February 2009, he followed an internship at Aubay Research and Technologies.

1.2 Further Studies

Antonino Nocera attended the following PhD Schools:

- Infosec 2015 - International Summer School on Information Security. July 6-10, 2015. Bilbao, Spain.
- MODAP 2012- International Summer School on Privacy Aware Social Mining. July 1-6. Leysin, Switzerland.

2 National Scientific Habilitation

On April 2017, Antonino Nocera has obtained the National Research Habilitation as Associate Professor (ING-INF/05).

3 Awards and Acknowledgments

- In 2013, in the context of the Project TENACE, Antonino Nocera is coauthor of a research report available in the Web site of the Information System of the Republic "Sistema di Informazione della Repubblica" (`http://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/tenace -e-la-protezione-delle -infrastrutture-critiche.html`).
- In 2010, Antonino has won the "Serenalla Lucisano" best MsC thesis award in Information Engineering.

4 Job Positions and International Scientific Collaborations

4.1 Job Positions

- Antonino Nocera is currently an RTD-B (Tenure Track Assistant Professor) at the University of Pavia.
- During 2018, he worked with the Information Engineering Group of the Università Politecnica delle Marche, led by Prof. Domenico Ursino, as Cybersecurity and Data Science expert.
- Also in 2018, Antonino Nocera has been appointed Senior Lecturer in Cybersecurity at the Oxford Brookes University in the context of information security and data science.
- From 2013 to 2017, Antonino Nocera was a post-doctoral researcher at the Computer Engineering Group of the University Mediterranea of Reggio Calabria (UNIRC), DIIES department. Specifically:
  - from 2014 to 2017, Antonino Nocera was post-doctoral researcher under the (*Assegno di Ricerca*) program "Attacchi informatici e protezione dell'identità digitale nei servizi online di pagamento elettronico" (Cyber attacks and protection of the digital identity in e-payment services) within the *"Cyber Security District" (Project 2: Digital Services and E-payment Protection; Project 3: Secure De-materialization)* a project of the Programma Operativo Nazionale (PON) Ricerca e Competitività 2007-2013.

  - In 2013 he won a post-doctoral research grant (*Assegno di Ricerca*) entitled "Metodologie basate su TRUST e Reputation e Tecniche di Data Mining per la Protezione di Infrastrutture Critiche" within the project PRIN *TENACE (Protecting National Critical Infrastructures from Cyber Threats)*.
- From 2013 to 2017 Antonino Nocera was part of the research group "Security, Social Networks, and Trust (STS)" local UNIRC unit of the CINI National Cybersecurity Lab and of the Cybersecurity District.

4.2 International Scientific Collaborations

- Started from 2018, Antonino is carrying out data science studies about the evolution of sharing economy in collaboration with Prof. Licia Capra from the University College London (UCL), Prof. Giovanni Quattrone of the Middlesex London University and Dr. Daniele Quercia of the Nokia Bell Labs.
- In May 2018, he has been invited by Prof. Diego Costa Pinto of the NOVA IMS University of Lisbon to carry out research studies in the context of Assortativity in Social Networks and Marketing.
- In September 2016 he has been invited by Prof. Christopher Rosenberger to work with members of the E-payment & Biometrics research unit in the GREYC lab of the Universit de Caen Basse-Normandie & ENSICAEN, Normandy, to develop joint rewards projects in the field of trust on the Internet.

4.3 Further Collaborations and Communication Skills

During his career, Antonino Nocera worked closely with research colleagues from the same University, department staff and, also, external contacts from very prestigious Universities, such as:

- Parthenope University of Naples (Information Security research unit),
- Politecnico di Torino (Computer-Human Interaction research unit),
- Salento University (Database and Cloud research unit),
- University of Calabria (Logic Programming research unit).

4.4 Other Job Positions

From February 25 to April 8 2013, Antonino Nocera worked as scientific collaborator under the program "Implementation of tools for the analysis of Social Internetworking Scenarios" within the DIIES department project "Web Scene", at the Computer Engineering Group of the University Mediterranea of Reggio Calabria, DIIES department.

5 Research Activities

Antonino Nocera is author of about 70 scientific papers published or submitted to International Journals and prestigious International Conferences and Books. The main topics of these activities are: information security, trust, privacy, data science, social network analysis, folksonomies, and recommender systems.

The following are the research metrics of Antonino Nocera according to Google Scholar and Scopus:

	Publications	Citations	H-Index
Scholar	78	898	17
Scopus	66	642	15

Table 1. Bibliometric Indicators.

A detailed statement about Antonino Nocera's research interests is reported in Section 10.

6 Teaching Experience

The teaching activities of Antonino Nocera are currently carried out at the University of Pavia. Specifcally, he is teaching a BsC course in Information Engineering about Object Programming and an MsC course, namely Data Science and Big Data Analytics, for a Data Science track in Computer Engineering.

In 2021, he has been external external lecturer in the course "BIO4334 Informatics for Genomics" (module 2) at the Middlesex University London.

From 2018, Antonino Nocera is collaborating as external lecturer on the teaching activities of the course "Applied Data Analytics - Tools, Practical Big Data Handling, Cloud Distribution" of the Master course in Data Science of the Middlesex University London (course leader Prof. Giovanni Quattrone).

From January 2010 to July 2017, Antonino Nocera has been teaching assistant and tutor of the following BsC courses in Information Engineering at the University Mediterranea of Reggio Calabria:

- Databases.
- Operating System.

Moreover, he has been teaching assistant and tutor of the following MsC courses in Information Engineering at the same University:

- Databases 2.
- Business Intelligence.
- Advanced Java Programming and Mobile.
- Information Security.
- Software Engineering.

In more details, he held the following course modules:

– A set of lectures of concurrent programming in Java.
– A seminar on DBMSs, in which he illustrated the main features of the Oracle DMBS.
– Several tutorship sessions on Relational Algebra, SQL query language and database design.
– A set of lectures on the framework J2EE for the development of Java Web applications. During these lectures, he showed examples on the use of Servlet, JSP, Java Beans and JDBC to create a Web portal.
– A seminar on advanced Java programming, in which he showed examples of portlet technology and illustrated some case studies on the LifeRay Web portal.
– A set of lectures of Android Programming, in which he explained the main properties of the Android operating system and showed a large set of programming examples to describe the main components for the design of Android applications.
– A set of lectures on the Oracle BI suite. In these lectures he showed several examples comprising data integration techniques, data warehousing and data mining leveraging tools from the Oracle BI suite such as: SQL Developer, ODI, AWM and ODM.
– A seminar on the WEKA and KNIME data mining tools.
– A Computer Security seminary on buffer overflow in accordance to the International Cybersecurity program 10k Students, in which he showed some examples of buffer overflow attacks and discussed about the possible countermeasures.
– A set of lectures of Information Security, in which he presented some examples of SQL injection and XSS attacks. Moreover, he presented the Kali Linux distribution and showed some tools for the analysis of vulnerabilities.
– A seminar on software engineer design patterns.

From October 2011 he is also member of the Computer Engineering Exam Commission at the University Mediterranea of Reggio Calabria.
In 2015 he held a course entitled "Informative System for logistic and transportation support" at ITS: Institute "Tecnico Superiore per l'Infomobilità e le infrastrutture logistiche" ITS "PEGASUS", Reggio Calabria.

6.1 Seminaries and Talks

- Antonino has been Invited speaker to a session of SecureCI 2016 - Winter School: Securing Critical Infrastructures- held on January 17-21, 2016 at Cortina D'Ampezzo, Italy, where he described an approach to implementing fine grained Twitter authorization policies on Android mobile applications.
- In November 2016, Antonino Nocera has been invited to hold a speech on Android Security at the United Technology Research Center in Cork, Ireland.
- In 2017 he has been invited by the PhD School of Information Engineering of the University Mediterranea of Reggio Calabria to held a seminary on the security issues in the Android realm.
- In 2018, he held a seminary on Big Data Analytics and Machine Learning at the Piemonte Orientale University.
- Moreover, still in 2018 he held a seminary on the techniques for malware protection in the context of mobile applications at the Università Politecnica delle Marche.
- in May 2018 Antonino has been invited to hold a seminary entitled "Assortativity: The Multi Social Network Perspective" at the NOVA Information Management School of Lisbon.
- In 2020, he held a speech with tile "Dalle Social Network agli scenari di Multi-Social Network: opportunit e problematiche" at the conference 25 KM TRACKS organized by JEKPOT Srl.

6.2 Student Supervisor

Antonino Nocera has been supervisor and co-supervisor of a large number of BsC and MsC thesis and practical training supervisor also in collaboration with colleagues from international Universities. Therefore, he is experienced in working with a wide range of students. Moreover, from 2014 to 2017 he supported a PhD student in the development of her PhD thesis entitled "Organizations and communities: trust, security, and privacy issues".

He is currently supervisor of a research fellow working in the context of NLP and text mining with particular focus on the analysis of data from online social platforms.

7 Editorial Boarding and Conference Organization

Antonino Nocera is editorial board member of a number of scientific International Journals, including *Information Sciences* (Class 1 in the Anvur Classification and 4.3 impact factor journal), Elsevier.

Moreover, he has been involved in the Technical Program Committee of several International Conferences, such as the International Conference on Information Systems Security and Privacy (ICISSP), and the International Conference on Data Science, Technology and Applications (DATA).

In 2013, he has been involved in the Organizing Committee for the 21st National Congress on "Sistemi Evoluti per Basi di Dati" (SEBD'13), Roccella Jonica (RC).
Antonino Nocera has been session chair in a number of International Conferences, such as the 38th edition of the International Computers, Software & Applications Conference (COMPSACW 2014) Moreover, he has served as referee for several International Journals such as, for instance, the IEEE Transactions on Parallel and Distributed Systems, Computer Human Behavior, and International Conferences such as the International Conference on Availability, Reliability and Security (ARES), and the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM).

8 Research Projects

Antonino Nocera participates to a number of research projects. In the following projects he took part to both the proposal and their development.

- *"Analisi di dati attraverso tecniche di Social Network Analysis e Machine Learning per il monitoring dei servizi"*: A research project funded by SKY Italia to develop NLP and text mining solutions based on data coming from social sites. Antonino Nocera has played the role of PI in this project.

- *"Cyber Security District" (Project 2: Digital Services and E-payment Protection; Project 3: Secure De-materialization)* a project of the Programma Operativo Nazionale (PON) Ricerca e Competitività 2007-2013.
  The project started in October 2013.
- PRIN *TENACE (Protecting National Critical Infrastructures from Cyber Threats)*.The project has been carried out from February 2013 to January 2016.
- *"inMoto" (Information MObility for TOurism)*, a project of the Programma Operativo Nazionale (PON) Ricerca e Competitività 2007-2013. The project has been carried out from April 2013 to December 2015.
- *SMBI* (Social Media, E-Service e Business Intelligence: scenari evoluti), a department project aiming at studying new social network analysis issues, e-services and business intelligence. The project started on November 2011.
- *WebScene*, a department project aiming at studying Web services and their evolution. The project started on November 2011
- *HKMS* (Health Knowledge Mining Suite), a regional founded project aiming at the development of OLAP and datamining techniques on health care data to improve health care services. The project has been carried out from July 2011 to April 2013.

9 Scientific Prototypes

Antonino Nocera has been team leader and main developer of several scientific prototypes. Among those the most important are:

- *SNAKE*. The Social Network Account Knowledge Extractor is a system for the extraction of structural data from a multi-social network environment. It supports the main social networks in the current Web scenario (such as, Facebook, Twitter, Google+, Flickr, LiveJournal, etc.). More details about it are available at `http://onlinelibrary.wiley.com/doi/10.1002/spe.2280/abstract`, moreover, a demo version is hosted at `http://http://ictsud.unirc.it:8080/SNAKE/`.
- *BDS*. BDS (Bridge Driven Search) is a new generation crawler specifically tailored for multi-social network scenarios. BDS leverages SNAKE or any other similar system (such as, the Google Social Graph API) to extract information about user contacts in social networks. It implements an innovative strategy to extract samples representative of a multi-social network scenario. Therefore, starting from any seed in any network it can perform a visit also moving through different social networks. Further details available at `http://www.sciencedirect.com/science/article/pii/S0020025513006191`.
- *FindMe*. It is a system based on the approach described in [46]. Its aim is to detect accounts belonging to the same person also in different social networks for which the explicit *me* information is missing. It is able of both finding (possibly) all the accounts of the same person in different social networks starting from any of them (*node-seed crystallization problem* and to enrich a multi-social network sample with missing *me* edges (*edge-seed crystallization problem*. More details at `http://www.sciencedirect.com/science/article/pii/S0020025515003722`.
- *Crawling Framework*. A framework implementing the main crawling techniques for social networks. It provides both classical and multi-social network optimized implementations of state-of-the-art strategies such as: Breadth First Search, Metropolis-Hasting Random Walk, Random Walk, Bridge Driven Search, etc.
- *A Middleware for the Protection of Social Mobile Application*. This system implements the approach described in [49] and realizes an efficient solution to provide fine-grained access control rules for Twitter-based mobile application in Android.
- *Metasploit module for testing Privacy Setting in Facebook*. This module implements the approach described in [51] and provides a tool to test the security of privacy setting in Facebook. It will exploit a Facebook vulnerability to try to reveal profile information (such as the friendlist) for a private account.

In the development of the following scientific prototypes, Antonino Nocera supervised Dr. Serena Nicolazzo during her PhD course:

- *Facebook and Twitter Uniform Sampler.* Uniform sampling of social networks is, generally, a non-trivial technological task. This system leverages the specificities of Twitter and Facebook user identifier which, starting from 2007, are 64-bit identifier. Therefore, by generating a random 64-bit number it is possible to verify whether it is associated with a user or not by accessing the corresponding profile URL. As an example, given an identifier the corresponding Facebook account URL is: `http:\\www.facebook.com/XXX`, where `XXX` is the 64-bit identifier.
- *T2S prototype.* This system implements the Tweet to Sign protocol for social digital signature described in [**?**]. The system is composed of three main applications. A Web application implementing the company-side features described in the protocol, an android application for the hash-chain generation and a Firefox web browser plug-in for the signature integrity verification.
- *K-anonimous log generator.* This system implements the strategy described in [67]. It has been designed for Beaglebone technology, and exploits computer vision and RFID technology to generate k-anonymous logs of people movements inside critical environments.

10 Statement of Research Interests

10.1 Information Security, Trust and Privacy

Trust and reputation models have a very fundamental role in the definition of techniques for the prevention of common attacks, such as: *slandering attack*, *sybil attack*, *self-promoting attack*, *white-washing attack*, etc. My research activity in this field focuses on two specific application contexts: *(i)* sensor networks; *(ii)* Web services and crowdsourcing.

As for the former, Wireless Sensor Networks (WSNs) are being increasingly adopted in several fields because of their advantages with respect to classic sensor networks. However, nodes in a WSN cooperate and this exposes them to several security threats. In [29], we show how trust-based systems are an established solution to ensure security of distributed systems. Specifically, we propose a trust-based approach to make WSNs tolerant against attacks targeting WSN routing layer. Moreover, we show how such attacks are tolerated with low overhead in comparison to unprotected systems. In this work, we focused on a specific typology of attack, namely *sinkhole* attack, and we propose a strategy leveraging special probing messages that WSN nodes use to test the trustworthiness of neighbours during the construction of paths to the base station. A trust model is then built and maintained so that each node can take advantage of the trust tests, also performed by other nodes, to decide its next hop towards the base station.

Concerning the latter context, a lot of evolutionary scenarios in the field of e-commerce, such as social commerce, are always increasing the role of single users in their services. However, by doing so, these systems are more often exposed to the attacks described above due to the intrinsic unreliability of user Web-profiles. This is an extremely up-to-date issue as a lot of most famous Web portals, such as Amazon, eBay, Booking and TripAdvisor, have important functionalities, e.g., the possibility of rating service providers (such as sellers, for instance) which leverages on user feedbacks. Therefore, in [42] we focus on a well known crowdsourced Web system, namely TripAvisor, and propose a reputation model abstractly considering service providers, users and feedbacks, and implementing the theoretical notion of certified reputation to concretely define a strategy to normalize feedback scores towards reliable values. We apply this model to the case of TripAdvisor, by proposing a solution to improve its dependability not increasing invasiveness nor reducing usability of the system.

Another important security aspect is related to the user authentication context and, in particular, to the definition of a new lighter protocol for digital signature. Due to the higher costs of smart cards (HSMs), of the qualified certificates (1999/93/EC) and for the complexity of the signature procedure itself (signature, verification, registration and management of certificates), public-key-encryption-based qualified electronic signature may be low applicable in some application scenarios, such as e-commerce or e-government, in which it could be adopted as a mass tool so that every user should use it to validate their signatures. For this purpose, the European legislation, by recognizing the actual need of the market and the public sector to increase the adoption of secure electronic signature, also promotes lighter solutions based on advanced electronic signature. This makes timely and important the issue of designing new signature protocols that relax the heaviest requirements of public-key-encryption-based qualified electronic signature, still keeping the features of advanced electronic signature. Therefore, in [57], we propose a new electronic signature protocol using neither public-key encryption nor qualified signature creation devices nor qualified certificates. The protocol relies on an innovative model, which

exploits the power of online social networks of sharing information by spreading out on them the signature functions. Moreover, in [**?**], through a deep and formal security analysis, we show that the proposed advanced electronic signature is at least secure as CADES/XADES qualified electronic signature (the most used qualified electronic signature). As a further contribution, we describe a Twitter implementation, showing that the approach is realistic and effective.

The security of critical physical environment and the monitoring of people living or working in such environments is an extremely timely problem. Standard solutions to this issue are mostly based on video surveillance recording the entrance and leaving of each person inside an area in the monitored zone. However, a lot of solutions adopt RFID based strategies to have logs reporting people localization at any time. This allows a precise and decisive restoring of information in a faster way than video surveillance. Although, the continuous monitoring of people movements is acceptable (and already adopted) for very high-critical environments (such as, government buildings, museums, tribunals, etc.) it opens several threats to people privacy, which may result in an unacceptable situation also from a law requirement point of view. Therefore, solving the right trade-off between people privacy and security/safety requirements are an important challenge. In [31], we propose an RFID based system to generate logs allowing us to (partially) trace people with a suitable degree of uncertainty, in such a way that privacy is fully preserved. Logs fulfill a k-anonymity property, according to which we are able to guess who accessed a place (for example, a room of a museum), at a given time, with probability k^{-1}. Indeed, the server receives k-anonymous logs and no party knows detailed information. It is worth noting that this concept of k-anonymity meets the security requirement of identifying the person who was present in a given location at a given time, with uncertainty equal to k.

The distributed fashion of this methodology is the basis of its effectiveness from the point of view of privacy. Indeed, any centralized solution would not be able to protect data from attacks in which we assume that the adversary accesses the server. As an extension to this idea is described in [**?**] where the system is actually designed and validated. The implementation is carried out by leveraging BeagleBone technology to build the *smart* RFID readers.

Still in this context, we extended the above idea by considering a very different scenario, i.e. that of assistive living facilities, in which a posteriori log analysis is no more useful but real time monitoring is needed to guarantee resident support and care. This is an intermediate situation, in which the staff cannot keep a full control on residents because it appears not proportionate w.r.t. the safeguarding of fundamental rights. However, residents' localization cannot be left entirely without monitoring, because in particular cases it is crucial to be able to quickly reach them (e.g., a resident does not show up for an essential therapy) therefore real time monitoring is mandatory. The solution proposed in [50] is based on a probabilistic framework that supports the k-anonymity notion. Specifically, our approach leverages, once again, an infrastructure of (RFID) readers covering the entire area of the assistive living facility, in which residents are equipped with suitably-designed RFID **active** tags. Due to the real time nature RFID tag are now active and send quasi-identifiers that do not disclose residents identity because it is always guaranteed that at least other k residents send the same quasi-identifier at the same stage. This allows us to guess the position of a resident with probability k^{-1}, for any positive integer k. Moreover, the solution guarantees that at least k RFID readers report the same quasi-identifier, so that the privacy requirement k is effective (thus resuming the concept of l-diversity).

Another hot topic recently investigated is related to security in cloud computing. Cloud computing provides users with the possibility to store their data in third-party servers. These data centers may be untrusted or susceptible to attacks, hence they could return compromised query results once interrogated. Query integrity has been widely investigated in the literature, and a number of methods have been proposed to allow users to verify that query results are *complete* (i.e., no qualifying tuples are omitted), *fresh* (i.e., the newest version of the results is returned), and *correct* (i.e., the result values are not corrupted). In [54] we identify a video surveillance setting scenario, in which data streams append operations and range queries are dominant, and the efficiency is a critical factor. In this scenario classical techniques for query integrity, such as those based on Merkle Hash Tree, appear little suitable and we propose a new solution, based on a hash chain, to overcome these drawbacks. Our *flat* structure supports insertions in constant time (if we consider a single-block hash computation as unitary cost) opposite to the logarithmic cost of the hash-tree based solutions.

Always in the context of information security in [49] we explore the topic of mobile applications security. Among mobile applications, those that interact with social network profiles, have a great potential for development, as they intercept another powerful asset of the today cyberspace. However,

one of the problems that can limit the diffusion of social network applications is the lack of fine-grained control when an application uses the APIs of a social network to access a user profile. For instance, in Twitter, the supported access control policy is basically on/off, so that if a (third party) application needs the right to write in a user profile, the user is enforced to grant this right with no restriction in the entire profile. This enables a large set of security threats and can make (even inexpert) users reluctant to run these applications. To overcome this problem, we propose an effective solution working for Android Twitter applications based on a middleware approach, which supports a fine-grained access control to the Twitter user profile. The proposed solution enables other possible benefits, as anomaly-based malware detection leveraging API-call patterns, and it can be extended to a multiple social network scenario.

An attack to the privacy mechanism of Facebook is presented in [51]. In this paper, we study the robustness of Facebook privacy settings, showing that it can be broken even in the less advantageous conditions for the adversary. To do this, we exploit both the potential information extracted from user alter accounts in Twitter and a new concept of interest assortativity we defined in [53]. Starting from the victim Facebook profile, we first identify his alter account on Twitter (if any), and then, thanks to interest assortativity, we are able to select some suitable candidates that can lead to some public friends in common with the victim, thus breaking his privacy. The attack incrementally proceeds, by discovering the most of private friends. The preliminary experimental results, give a first evidence of the effectiveness of our attack, which succeeds even in the most difficult case that is when the information about the victim are minimum.

Another important aspect in the field of Cloud security is related to the integrity verification of query results. Indeed, Cloud computing provides users with the possibility to store their data in third-party servers. These data centers may be untrusted or susceptible to attacks, hence they could return compromised query results once interrogated. This issue becomes particularly crucial in the case a third-party cloud is used to store videosurveillance data. Query integrity has been widely investigated in the literature, and a number of methods have been proposed to allow users to verify that query results are *complete* (i.e., no qualifying tuples are omitted), *fresh* (i.e., the newest version of the results are returned), and *correct* (i.e., the result values are not corrupted). However, in this specific application scenario, in which append operations and range queries on stored datastreams are dominant, and the efficiency is a critical factor, classical techniques for query integrity appear little suitable. Therefore, in [54] we propose a new approach for the verification of the integrity of range query results guaranteeing constant insertion costs still keeping verification efforts comparable to classical solutions.

Another very recent research activity concerns a new protocol for secure transactions. By starting on the consideration that blockchain has attracted a lot of attention by the research community, we developed a new protocol borrowing some ideas from blockchain but using Twitter as communication channel to perform and verify secure transactions [62].

10.2 Data Science and Social Network Analysis

The research activity of Antonino Nocera in the Data Science field mainly concerns Sharing Economy and Social Network Analysis. Specifically, in the context of Sharing Economy, Antonino Nocera is working closely with prestigious international Professors and Researchers from the University College of London, the Middlesex University and the Nokia Bell Labs. In this context, Antonino Nocera is studying the evolution of Sharing Economy from the point of view of guests. He is performing a deep analysis leveraging machine learning approaches and considering several dimensions, such as: time, countries, inter-country flows and review language evolution. Since there was no existing database for studying guest behavior, an important and preliminary task was data extraction. Antonino Nocera focused on Airbnb and built a crawler to sample data from this system. This database has been the premises for the subsequent study he is carrying out in the last months.

Concerning Social Network Analysis, Antonino Nocera mainly performed research activities in the field of Social Network Analysis in Multiple-Social-Networks scenarios. The studies carried out within this research line, have been often related to issues of security, trust and privacy. Specifically, most of the research activities described here, either include some direct application to the context of security, trust and privacy, or are exploited in the research activities described in the previous section regarding social networks.

Nowadays, social networks are a global phenomenon and a powerful tool for user interaction and cooperation. The main feature of social networks is the possibility of reproducing relationships, which take place in disparate social context of real life, in a virtual global environment. The huge number of active users in the most popular social networks is a confirmation that this phenomenon is one of the most important in the Internet scenario. However, the existence of so many independent and heterogeneous social networks introduce important issues in the attempt of using the information they share in the most profitable way. The reference scenario is not the one of a single, isolated, independent social network, but a universe composed of a constellation of several social networks, each forming a community with specific connotations, but strongly interconnected with each other. This makes the analysis of this reality more challenging.

It is a matter of fact that, despite the inherent underlying heterogeneity, the interaction among distinct social networks is the basis of a new emergent internetworking scenario enabling a lot of strategic applications whose main strength will be just the integration of possibly different communities, yet preserving their diversity and autonomy. Clearly, Social Network Analysis approaches may strongly rely on this huge multi-network source of information, which also reflects multiple aspects of people personal life, thus enabling a lot of powerful discovering activities. These scenarios are often referred as Multi-Social Network Scenarios or as Social Internetworking Scenarios (SISs, for short), in which users owning multiple accounts in different social networks and providing special links (called `me` edges) from one to the other are referred as *bridges* as they physically build the interconnection among social networks. Unfortunately, also because the problem is extremely recent, no analyses on SISs nor on models and approaches to handling them have been proposed in the scientific literature.

Concerning the analysis of these new scenarios, a preliminary step consists in the definition of new techniques for the extraction of social network data and new suitable "crawling" strategies tailored for these environments. In [14], we propose a system, called SNAKE (Social Network Account Knowledge Extractor), to support data extraction in a multi-social network scenario. SNAKE, is able to retrieve information about public accounts (such as screen name, contacts and `me` edges) on the major social networks including data concerning the interconnection among them. This last feature allows the transition from a social network to another. Specifically, SNAKE acts as a middleware between social network data and any possible crawler. For this reason, it can be used as a base to implement new generation crawlers to build samples of multi-social network scenarios. An extended version of this project, including a deep experimental campaign to test the effectiveness and the performances of SNAKE, is presented in [45]; moreover, a demo of the system is available online at the address `http://ictsud.unirc.it:8080/SNAKE`.

Because of the intrinsic heterogeneity of information and concepts of the diverse social networks covered by SNAKE, it leverages an ad-hoc model we designed to allow the development of software with suitable abstraction level in the context of multi-social networks. The aim of this model is to generalize concepts, actions and relationships of existing social networks. A preliminary version has been presented in [30] were only the basic features of this model are described. The extended version covering all implementation details and validation activities is reported in [56].

A lot of crawling strategies have been studied and proposed in the context of social network, however, when it comes of multi-social network scenarios the identification of suitable crawling strategies is still an open issue. As a matter of fact, we cannot expect that a crawling strategy that is good for social networks, is valid in a multi-social network scenario too, due to its specific topological features. In other words, is a standard crawling strategy able to correctly navigate through interconnections among social networks? Is there the risk that the crawler tends to remain confined in the social network from which it starts? Equivalently, is a standard crawler able to describe SISs in a realistic way, covering enough the involved social networks, and faithfully measuring their coupling degree and their node average degree? The answers to these questions and the formalization of a new crawling strategy, called *Bridge Driven Search* (BDS, for short), for multi-social network scenarios are proposed in [15]. In this paper, we also provide an initial testing of our proposal showing that it is capable of sampling the considered scenario preserving its peculiarity and topological features. This preliminary research is, then, extended and completed in [35] where all the details about its implementation are provided including a complete experimental campaign showing the effectiveness of the approach and a computational complexity analysis. Finally, in [36] we describe several analysis performed on multi-social network samples extracted using BDS and compare the results with those obtained on samples extracted by applying classical crawling techniques.

In [23] we propose a deep study on social network *bridges* that, as stated above, represent the key actors of multi-social network scenarios. In this paper, we describe a Social Network Analysis campaign whose purpose is drawing a complete "identikit" of this special typology of users. For this purpose, we extracted several samples relying on a set of scenario-tailored crawling strategies and computed most common social network analysis parameters to compare the behaviour of social network users with that of *bridges*. This study allows the low us to better understand the real role of this special type of users in social networks.

As mentioned above, social network users may explicitly declare they *bridge* role by adding information about their accounts in other social sites by means of special arcs called `me` edges (practically corresponding to a link between the two accounts). Unfortunately, for disparate reasons, users do not always make their membership to two distinct social networks explicit. As a consequence, in the overall underlying (social internetworking) graph a big number of missed `me` edges exists, whose discovery represents a very important issue. In other words, an interesting problem of missing link detection arises, which partially overlaps with a link prediction issue, because we may expect that a portion of missing me edges will be inserted in a next stage in the graph. In [17] and [46], we deal with the above problem by proposing an effective solution experimentally tested in a real-life multi-social network scenario. Specifically, in [17] we perform some preliminary study to show verify whether common-neighbor approaches for link prediction can be directly applied to our problem and, then, we sketch our solution and show the effectiveness of the proposal. Then, in [46], we extend and complete this study and describe in full details our approach. Our solution is based on a notion of node similarity, whose usage allows us to detect whether a suitable threshold is exceeded and then a missing me edge between two nodes is detected. The similarity between two nodes is obtained by combining two contributions: a string similarity between the associated usernames, and a contribution based on a suitable recursive notion of common-neighbour similarity. The neighbourhood similarity allows these errors to be detected and avoided. Moreover, we provide a deep experimental campaign in which we test the performance of our approach and compare it with related solutions presented in the literature.

A comparative study of people's behaviour Facebook and Twitter is performed in [47]. We base our analysis on users who possess accounts on both social networks. To this purpose, we adopt the strategies described above to crawl a sample of *bridge* users between Facebook and Twitter and we study a number of behavioural aspects. The first one is about privacy and disclosure of personal information. Recent studies on Facebook have shown that both a strong association between low engagement and privacy concern and a significant relationship between privacy awareness and privacy concerns/self-disclosure exist. Our study aims to answer the question "Is there a connection between user awareness about privacy threats and membership overlap between Twitter and Facebook?". The second aspect we study is about friendship. OSNs are important for maintaining social relations and previous studies have found that friendship is positively correlated with bridging social capital. As for this aspect, we study what is the attitude of users to have friendship relations overlapping between Facebook and Twitter and if a correlation between number of friends in Twitter and Facebook exists. The last issue we deal with concerns the activity of users belonging to both Twitter and Facebook. Our study aims to answer the question "What about user activity and how the prevalence of activity on Facebook or Twitter is correlated to membership overlap?".

Concerning the analysis of this particular scenarios, clustering may be a fruitful point of view from which multi-social network scenarios can be studied. Indeed, every social network includes distinguishing features and a clustering-based approach may highlight the differences among social networks, yet analysing information about the whole system. But when we apply clustering to a social internetworking scenario (SIS), several issues arise that lead to the formulation of the following questions: (1) Which clustering algorithm is suitable for this context? (2) Which crawling strategy is able to build a sample on which clustering-based analysis can give meaningful results? (3) How many seeds (i.e., starting nodes for crawling algorithms) per social network we have to consider? In [28], we deal with the above issues, by analysing a real-life SIS composed of five of the most popular social networks (i.e., Twitter, YouTube, Flickr, MySpace, LiveJournal) by means of different clustering algorithms, different crawling strategies and different number of seeds, seen as independent analysis dimensions. By measuring the significance degree of the experimental results, also in terms of the approach ability to separate different social networks, we find the optimal combination of the above dimensions. The effectiveness of clustering techniques in multi-social network scenarios is also proved in [22], in which we exploit clustering to restore part of the missing explicit information, crucial for SIS-oriented analysis, in anonymized social network samples. The approach is based on clustering to partitioning the whole

graph in subgraphs, each corresponding as much as possible to an original social network, and, as difference, by discovering the interconnections among social networks. Once this task has been done, the analyst will be able to conduct most of the SIS-oriented investigations in a direct way, starting from the basic information concerning the membership of two or more users either to the same or to distinct social networks.

The role of assortativity in real-world and online social networks has been largely investigated in the literature, in which, starting from degree assortativity, several forms of assortativity have been analysed. When moving from a single-social-network to a multiple-social-network perspective, new specific traits can be studied, also under the assortativity magnifying glass. This is the case of membership overlap among networks (i.e., the fact that people belong to more online social networks) as expression of different traits of users' personality. Studying whether online social networks exhibit assortative mixing with respect to membership overlap is a new, challenging, and important problem. We deal with this problem in [26], in which we start by analysing this property on Facebook and, then, we extend this study also to Twitter and improve it by building a more sophisticated and improved model to take others important features into account (such as node-degree assortativity) during the experimental analysis in [44]. A further study on assortativity has been also carried out in [53], in which we focus on Twitter and study how user relationships are influenced by interests. We refer to this form of assortativity as Interest Assortativity and it is measured by using an approach based on public figures of Twitter. The choice of Twitter is related to both the goal of trying to have results little affected by physical friendship. Moreover, Twitter use is driven primarily by interest for entertainment news, celebrity news, and sports news. This allows us to map the abstract concept of interest (or topic) to the concrete entity of public figure, to the extent that a public figure in a given field, say Gordon Ramsay, acts as a representative of a topic, haute cuisine (i.e., high-level cooking), in our example. Thus, we assimilate the followship of a user to the Twitter profile of Gordon Ramsay to the fact that this user is interested in high-level cooking. Once again, the way to study interest assortativity is to observe, for a number of public figures, if the measured probability that two Twitter friends share the followship to the same public figures is higher than the random case (i.e., with no assortativity).

In [24] we propose a new measure of Betweenness Centrality for a multi-social network scenario. The importance of centrality measures in social networks is underlined by the great interest showed by the research community and by the mole of applications working on different domains leveraging on them. However, the classical measures are not able to capture the centrality of nodes w.r.t. a multi-social network environment. Therefore, our approach aims at correcting this measure by considering structural information that strongly characterize this new intriguing environment. Finally, an application of this new centrality measure for team-building has been presented [34].

References

1. M. Arazzi, S. Nicolazzo, A. Nocera, and G. Ubertini. Comparing the Twitter evolution of streaming service providers: a Netflix and Now TV analysis. *Journal of Information Science*. Submitted for Pubblication.
2. E. Corradini, S. Nicolazzo, A. Nocera, D. Ursino, and L. Virgili. A two-tier Blockchain framework to increase protection and autonomy of smart objects in the IoT. *Computer Communications*. Submitted for Pubblication.
3. E. Corradini, A. Nocera, D. Ursino, and L. Virgili. A multi-dimensional investigation of negative reviews in yelp. *International Journal of Information Management*. Currently Submitted for Publication.
4. M. Ferretti, S. Nicolazzo, and A. Nocera. H2O: Secure interactions in IoT via Behavioral Fingerprinting. *Future Internet*. Submitted for Pubblication.
5. S. Nicolazzo, A. Nocera, and D. Ursino. Anonymous Access Monitoring of Indoor Areas. *IEEE Access*. Submitted for Pubblication.
6. P. De Meo, A. Nocera, G. Quattrone, D. Rosaci, and D. Ursino. Finding reliable users and social networks in a social internetworking system. In *Proc. of the International Database Engineering and Applications Symposium (IDEAS 2009)*, pages 173–181, Cetraro, Italy, 2009. ACM Press.
7. A. Nocera, G. Quattrone, G. Terracina, and D. Ursino. Exploitation of user actions to recommend similar users, resources and social networks in a Social Internetworking Scenario. In *Atti del Diciottesimo Convegno Nazionale su Sistemi Evoluti per Basi di Dati (SEBD'10)*, pages 42–53, Rimini, Italy, 2010.
8. P. De Meo, G. Fiumara, A. Nocera, and D. Ursino. The Role of Schema and Document Matchings in XML Source Clustering. *XML Data Mining: Models, Methods, and Applications*, pages 125–153, 2011.
9. P. De Meo, A. Nocera, G. Quattrone, and D. Ursino. A conceptual framework and an underlying model for community detection and management in a Social Internetworking Scenario. In *Atti del Diciannovesimo Convegno Nazionale su Sistemi Evoluti per Basi di Dati (SEBD'11)*, pages 387–394, Maratea (PZ), Italy, 2011.
10. P. De Meo, A. Nocera, D. Rosaci, and D. Ursino. Recommendation of reliable users, social networks and high-quality resources in a Social Internetworking System. *AI Communications*, 24(1):31–50, 2011. IOS Press.
11. P. De Meo, A. Nocera, G. Terracina, and D. Ursino. Recommendation of similar users, resources and social networks in a Social Internetworking Scenario. *Information Sciences*, 181(7):1285–1305, 2011. Elsevier.
12. P. De Meo, A. Nocera, and D. Ursino. A Component-based Framework for the Integration and Exploration of XML Sources. *XML Data Mining: Models, Methods, and Applications*, pages 343–377, 2011.
13. A. Nocera and D. Ursino. An approach to providing a user of a "social folksonomy" with recommendations of similar users and potentially interesting resources. *Knowledge-Based Systems*, 24(8):1277–1296, 2011. Elsevier.
14. F. Buccafurri, G. Lax, B. Liberto, A. Nocera, and D. Ursino. Supporting Community Mining and People Recommendations in a Social Internetworking Scenario. In *Proc. of the International Workshop on Mining Communities and People Recommenders at ECML/PKDD 2012 (COMMPER 2012)*, pages 24–31, Bristol, UK, 2012.
15. F. Buccafurri, G. Lax, A. Nocera, and D. Ursino. Crawling Social Internetworking Systems. In *Proc. of the International Conference on Advances in Social Analysis and Mining (ASONAM 2012)*, pages 505–509, Istanbul, Turkey, 2012. IEEE.
16. F. Buccafurri, G. Lax, A. Nocera, and D. Ursino. Discovering hidden `me` edges in a Social Internetworking Scenario. In *Atti del Ventesimo Convegno Nazionale su Sistemi Evoluti per Basi di Dati (SEBD'12)*, pages 15–26, Venezia, Italy, 2012.
17. F. Buccafurri, G. Lax, A. Nocera, and D. Ursino. Discovering Links among Social Networks. In *Proc. of the European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD 2012)*, pages 467–482, Bristol, United Kingdom, 2012. Lecture Notes in Computer Science. Springer.
18. F. Buccafurri, G. Lax, A. Nocera, and D. Ursino. SISO: a conceptual framework for the construction of "stereotypical maps" in a Social Internetworking Scenario. In *Proc. of the International Workshop on New Frontiers in Mining Complex Knowledge Patterns at ECML/PKDD 2012 (NFMCP 2012)*, pages 160–171, Bristol, UK, 2012.
19. F. Buccafurri, G. Lax, A. Nocera, and D. Ursino. Supporting Information Spread in a Social Internetworking Scenario. *Post-Proceedings of the International Workshop on New Frontiers in Mining Complex Knowledge Patterns at ECML/PKDD 2012 (NFMCP 2012)*, pages 200–214, 2012. Lecture Notes in Artificial Intelligence, Springer.
20. A. Nocera and D. Ursino. An approach to deriving a virtual thematic folksonomy based system from a social inter-folksonomy based scenario. *Web Intelligence and Agent Systems Journal*, 10(4):361–384, 2012.
21. A. Nocera and D. Ursino. PHIS: a system for scouting potential hubs and for favoring their "growth" in a Social Internetworking Scenario. *Knowledge-Based Systems*, 36:288–299, 2012. Elsevier.

22. F. Buccafurri, D. Caridi, G. Lax, A. Nocera, and D. Ursino. Restoring Information Needed for Social Internetworking Analysis from Anonymized Data. In *Proc. of the International Multi-Conference on Computing in the Global Information Technology (ICCGI 2013)*, Nice, France, 2013. IARIA XPS Press.
23. F. Buccafurri, V.D. Foti, G. Lax, A. Nocera, and D. Ursino. Bridge Analysis in a Social Internetworking Scenario. *Information Sciences*, 224:1–18, 2013. Elsevier.
24. F. Buccafurri, G. Lax, S. Nicolazzo, A. Nocera, and D. Ursino. Measuring Betweennes Centrality in Social Internetworking Scenarios. In *Proc. of International Workshop on Social and Mobile Computing for collaborative environments (SOMOCO'13)*, pages 666–673, Gratz, Austria, 2013. Springer Verlag.
25. F. Buccafurri, G. Lax, A. Nocera, and D. Ursino. Bridge-Driven Search in Social Internetworking Scenarios. In *Atti del Ventunesimo Convegno Nazionale su Sistemi Evoluti per Basi di Dati (SEBD'13)*, pages 175–182, Roccella Jonica, Italy, 2013.
26. F. Buccafurri, G. Lax, A. Nocera, and D. Ursino. Internetworking assortativity in Facebook. In *Proc. of the International Conference on Social Computing and its Applications (SCA 2013)*, pages 335–341, Karlsruhe, Germany, 2013. IEEE Computer Society.
27. A. Nocera and D. Ursino. A new ego network model and an approach to extracting an ego network compliant with this model from a Social Internetworking System. *International Journal of Web Based Communities*, 9(4):483–518, 2013.
28. F. Buccafurri, D. Caridi, L. Fotia, G. Lax, A. Nocera, and D. Ursino. A Clustering-based Analysis of a Social Internetworking Scenario. *International Journal of Society Systems Science*, 6(2):101–119, 2014.
29. F. Buccafurri, L. Coppolino, S. D'Antonio, A. Garofalo, G. Lax, A. Nocera, and L. Romano. Trust-Based Intrusion Tolerant Routing in Wireless Sensor Networks. In *Proc. of the International Conference on Computer Safety, Reliability and Security (SAFECOMP 2014)*, pages 214–229, Firenze, Italy, 2014. Springer.
30. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. A Model to Support Multi-Social-Network Applications. In *Proc. of the International Conference Ontologies, DataBases, and Applications of Semantics (ODBASE 2014)*, pages 639–656, Amantea, Italy, 2014. Springer.
31. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. A Privacy-Preserving Solution for Tracking People in Critical Environments. In *Proc. of the International Workshop on Computers, Software & Applications (COMPSAC'14)*, pages 146–151, Västerȧs, Sweden, 2014. IEEE Computer Society.
32. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. Fortifyng TripAdvisor against Reputation-System Attacks. In *Proc. of the World Congress on Internet Security(WORLDCIS 2014)*, pages 21–22, London, UK, 2014. IEEE.
33. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. Generating K-Anonymous Logs of People-Tracing Systems in Surveilled Environments. In *Atti del Ventiduesimo Convegno Nazionale su Sistemi Evoluti per Basi di Dati (SEBD'14)*, pages 37–44, Sorrento Coast, Italy, 2014.
34. F. Buccafurri, G. Lax, S. Nicolazzo, A. Nocera, and D. Ursino. Driving Global Team Formation in Social Networks to Obtain Diversity. In *Proc. of the International Conference on Web Engineering (ICWE 2014)*, pages 410–419, Toulouse, France, 2014. Springer.
35. F. Buccafurri, G. Lax, A. Nocera, and D. Ursino. Moving from Social Networks to Social Internetworking Scenarios: the Crawling Perspective. *Information Sciences*, 256:126–137, 2014.
36. Francesco Buccafurri, Gianluca Lax, Antonino Nocera, and Domenico Ursino. Experiences using bds: A crawler for social internetworking scenarios. In *Social Networks: Analysis and Case Studies*, pages 149–177. Springer, 2014.
37. G. Marra, A. Nocera, F. Ricca, G. Terracina, and D. Ursino. Investigating Information Diffusion in a Multi-Social-Network Scenario via Answer Set Programming. In *Proc. of the International Conference on Web Reasoning and Rule Systems (RR 2014*, pages 191–196, Athens, Greece, 2014. Springer.
38. G. Marra, A. Nocera, F. Ricca, G. Terracina, and D. Ursino. Investigating Node Influence Maximization and Influential Node Characterization in a Multi-Social-Network Scenario via Disjunctive Logic Programming. In *Atti del Ventiduesimo Convegno Nazionale su Sistemi Evoluti per Basi di Dati (SEBD'14)*, pages 264–275, Sorrento Coast, Italy, 2014.
39. P. De Meo, A. Nocera, G. Quattrone, and D. Ursino. A conceptual framework for community detection, characterization and membership in a Social Internetworking Scenario. *International Journal of Data Mining, Modelling and Management*, 6(1):22–48, 2014.
40. F. Buccafurri, L. Fotia, G. Lax, S. Nicolazzo, and A. Nocera. A lightweight electronic signature scheme using Twitter. In *Proc. of the Italian Symposium on Advanced Database Systems (SEBD 2015)*, pages 160–167, Gaeta, IT, 2015.
41. F. Buccafurri, L. Fotia, G. Lax, S. Nicolazzo, and A. Nocera. Trust, Security and Privacy in Smart Cities. In *In Proc. of the 1st CINI Annual Conference on ICT for Smart Cities & Communities (I-Cities 2015)*, Palermo, Italy, 2015.
42. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. A Model Implementing Certified Reputation and its Application to TripAdvisor. In *Proc. of the International Conference on Availability, Reliability and Security (ARES 2015)*, pages 218–223, Touluse, France, 2015. IEEE.

43. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. Accountability-Preserving Anonymous Delivery of Cloud Services. In *Proc. of the International Conference on Trust, Privacy and Security in Digital Business (TRUSTBUS 2015)*, pages 124–135. Springer, 2015.
44. F. Buccafurri, G. Lax, and A. Nocera. A New Form of Assortativity in Online Social Networks. *International Journal of Human-Computer Studies*, 80:56–65, 2015.
45. F. Buccafurri, G. Lax, A. Nocera, and D. Ursino. A system for extracting structural information from Social Network accounts. *Software: Practice and Experience (SPE)*, 45(9):1251–1275, 2015. DOI: 10.1002/spe.2280.
46. F. Buccafurri, G. Lax, A. Nocera, and D. Ursino. Discovering Missing Me Edges across Social Networks. *Information Sciences*, 319:18–37, 2015.
47. Francesco Buccafurri, Gianluca Lax, Serena Nicolazzo, and Antonino Nocera. Comparing twitter and facebook user behavior: privacy and other aspects. *Computers in Human Behavior*, 52:87–95, 2015.
48. F. Buccafurri, L. Fotia, G. Lax, S. Nicolazzo, and A. Nocera. Smart Communities and the Cloud: Security and Privacy Issues. In *In Proc. of the 2nd CINI Annual Conference on ICT for Smart Cities & Communities (I-Cities 2016)*, Benevento, Italy, 2016.
49. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. A Middleware to Allow Fine-Grained Access Control of Twitter Applications. In *Proc. of the international conference on mobile, secure and programmable networking (MSPN 2016)*, pages 168–182, Paris, France, 2016. Springer.
50. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. A Privacy-Preserving Localization Service for Assisted Living Facilities. *IEEE Transaction on Service Computing*, 2016. In Press.
51. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. A threat to friendship privacy in Facebook. In *Proc. of the International Cross Domain Conference and Workshop (CD-ARES 2016)*, pages 96–105, Salzburg, Austria, 2016. Springer.
52. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. Completeness, Correctness and Freshness of Cloud-Managed Data Streams. In *Proc. of the Italian Symposium on Advanced Database Systems (SEBD 2016)*, pages 134–141, Lecce, IT, 2016.
53. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. Interest Assortativity in Twitter. In *Proc. of the International Conference on Web Information Systems and Technologies (Webist 16))*, volume 1, pages 239–246, Rome, Italy, 2016. SCITEPRESS.
54. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. Range Query Integrity in Cloud Data Streams with Efficient Insertion. In *Proc. of the 15th International Conference on Cryptology and Network Security (CANS 2016)*, pages 719–724, Milan, Italy, 2016. Springer.
55. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. Range Query Integrity in the Cloud: the Case of Video Surveillance. In *Proc. of the International Conference for Internet Technology and Secured Transactions (ICITST-2016)*, Barcelona, Spain, 2016. IEEE.
56. Francesco Buccafurri, Gianluca Lax, Serena Nicolazzo, and Antonino Nocera. A model to support design and development of multiple-social-network applications. *Information Sciences*, 331:99–119, 2016.
57. G. Lax, F. Buccafurri, S. Nicolazzo, A. Nocera, and L. Fotia. A new approach for electronic signature. In *Proc. of the International Conference on Information Systems Security and Privacy (ICISSP 16))*, pages 440–447, Rome, Italy, 2016. SCITEPRESS.
58. F. Buccafurri, G. Lax, D. Migdal, S. Nicolazzo, A. Nocera, and C. Rosenberger. Contrasting False Identities in Social Networks by Trust Chains and Biometric Reinforcement. In *Proc. of the International Conference on CYBERWORLDS (CYBERWORLDS 2017)*, Chester, United Kingdom, 2017. Chester, United Kingdom, United Kingdom.
59. F. Buccafurri, G. Lax, S. Nicolazzo, and Assunta Matassa A. Nocera, Luca Console. Discovering good links between objects in the Internet of Things. In *Proc. of the International Conference on Wireless Networks and Mobile Systems (WINSYS 2017)*, 2017.
60. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. A Model for Handling Multiple Social Networks and its Implementation. In *Proc. of the Italian Symposium on Advanced Database Systems (SEBD 2017)*, 2017.
61. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. Not only databases: Social data and cybersecurity perspective. In *A comprehensive guide through the Database research over the last 25 years*. 2017.
62. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. Overcoming Limits of Blockchain for IoT Applications. In *Proc. of the International Conference on Availability, Reliability and Security (ARES 2017)*, Reggio Calabria, Italy, 2017.
63. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. Range Query Integrity in Cloud Data Streams with Efficient Insertion. In *In Proc. of the the Italian Conference on Cybersecurity (ItaSec2017)*, Venice, Italy, 2017.
64. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. Using Twitter for Consensus: Tweetchain as Alternative to Blockchain. In *Proc. of the International Conference on Web Engineering (ICWE 2017))*, Rome, Italy, 2017.

65. F. Buccafurri, G. Lax, S. Nicolazzo, A. Nocera, and F. Ermidio. A system for privacy-preserving analysis of vehicle movements. In *Proc. of the EAI International Conference on ICT Infrastructures and Services for Smart Cities (IISSC 2017)*, Brindisi, Italy, 2017.
66. F. Buccafurri, G. Lax, S. Nicolazzo, A. Nocera, and F. Ermidio. Urban security: a SPID-based system for physical access control. In *Proc. of the EAI International Conference on ICT Infrastructures and Services for Smart Cities(IISSC 2017)*, Brindisi, Italy, 2017.
67. F. Buccafurri, G. Lax, S. Nicolazzo, and A. Nocera. A System for Privacy-Preserving Access Accountability in Critical Environments. *IEEE Pervasive Computing*, 2018. In Press.
68. G. Quattrone, N. Nicolazzo, A. Nocera, D. Quercia, and L. Capra. Is the sharing economy about sharing at all? A linguistic analysis of Aribnb reviews. In *Proc. of the International AAAI Conference on Web and Social Media (ICWSM 2018)*, Stanford, California, 2018.
69. Francesco Buccafurri, Vincenzo De Angelis, Gianluca Lax, Serena Nicolazzo, and Antonino Nocera. The challenge of privacy in the cloud. In Shoba Ranganathan, Michael Gribskov, Kenta Nakai, and Christian Schnbach, editors, *Encyclopedia of Bioinformatics and Computational Biology*, pages 265 – 271. Academic Press, Oxford, 2019.
70. C. Diamantini, A. Nocera, D. Potena, E. Storti, and D. Ursino. Find the Right Peers: Building and Querying Multi-IoT Networks Based on Contexts. In *Proc. of International Conference on Flexible Query Answering Systems (FQAS 2019)*, 2019.
71. C. Diamantini, A. Nocera, D. Potena, E. Storti, and D. Ursino. Multi-Dimensional Contexts for Querying IoT Networks. In *Proc. of the Italian Symposium on Advanced Database Systems (SEBD 2019)*, 2019.
72. P. Lo Giudice, A. Nocera, D. Ursino, and L. Virgili. Building topic-driven virtual iots in a multiple iots scenario. *Sensors*, 2019.
73. E. Corradini, A. Nocera, D. Ursino, and L. Virgili. Defining and detecting k-bridges in a social network: The yelp case, and more. *Knowledge-Based Systems*, 195:105721, 2020.
74. C. Diamantini, A. Nocera, D. Potena, E. Storti, and D. Ursino. Querying the iot using multi-resolution contexts. *IEEE Internet of Things Journal*, pages 1–1, 2020. In Press.
75. S. Nicolazzo, A. Nocera, D. Ursino, and L. Virgili. A privacy-preserving approach to prevent feature disclosure in an IoT scenario. *Future Generation Computer Systems*, 105:502–519, 2020.
76. G. Quattrone, A. Nocera, D. Quercia, and L. Capra. Social Interactions or Business Transactions? What Customer Reviews Disclose about Airbnb Marketplace. In *Proc. of the International World Wide Web Conferences (WWW 2020)*, Taipei, Taiwan, 2020.
77. E. Corradini, A. Nocera, D. Ursino, and L. Virgili. Investigating the phenomenon of nsfw posts in reddit. *Information Sciences*, 566:140–164, 2021.

Milano, March 29, 2021

Antonino Nocera