Prof.ssa Sabrina Sophy Sicari

CURRICULUM VITÆ E DELL'ATTIVITÀ SCIENTIFICA E DIDATTICA

Indice

1. Dati Personali

Nome e cognome: Sabrina Sophy Sicari

Data di nascita: 18 Settembre 1977

Luogo di nascita: Catania (Italia)

Cittadinanza: Italiana

Residenza: Sito della Guastalla 1, 20122 Milano

Recapito ufficio: Dipartimento di Scienze Teoriche e Applicate (DISTA), Università degli Studi dell'Insubria, Via O. Rossi 9, 21100 Varese, Tel. 0332 218924

Recapito personale: +39 347 6697347

E-mail: sabrina.sicari@uninsubria.it

Url: http://www.dicom.uninsubria.it/~sabrina.sicari/

Periodo di Congedo per Maternità (legge 30/12/71 n.1204): da 29-5-2010 a 29-10-2010

1.1 Posizione attuale

- **Professore Associato**, settore concorsuale 09/H1, settore scientifico-disciplinare ING-INF/05 - Sistemi di Elaborazione delle Informazioni, Università degli Studi dell'Insubria (in ruolo dall'1/09/2016).
- **Membro del collegio del Dottorato di Ricerca** in Informatica e Matematica del Calcolo dell'Università degli Studi dell'Insubria (dal XXXIII ciclo, 2017).
- **Titolare degli insegnamenti** di "Reti di Telecomunicazione" (Laurea in Informatica), "Fondamenti di Internet of Things" (Laurea in Informatica) e di "Innovative Telecommunication Systems" (Laurea Magistrale in Informatica), presso l'Università degli Studi dell'Insubria.
- **Membro dell'Editorial Board** delle riviste scientifiche: Computer Networks (Elsevier), IEEE Internet of Things, Transactions on Emerging Telecommunications Technologies (Wiley), Internet Technology Letters (Wiley), e ITU Journal on Future and Evolving Technologies.

1.2 Settori di ricerca

- Sicurezza e privacy in Internet of Things
- Sicurezza e privacy nelle wireless sensors networks e nelle wireless multimedia sensors networks
- Ingegneria del software

1.3 Lingue straniere

- **Inglese:** ottimo, parlato e scritto.

2. Titoli di studio e professionali

Novembre 2020	Abilitazione Scientifica Nazionale alla funzione di Professore di Prima Fascia nel settore concorsuale 09/H1-Sistemi di Elaborazione dell'Informazioni
Gennaio 2003-Marzo 2006	**Dottorato di Ricerca in Ingegneria Informatica e delle Telecomunicazioni** Dipartimento di Ingegneria Informatica e delle Telecomunicazioni Università degli Studi di Catania (Italia). Tesi di dottorato: "*Quality of Service and Quality of Protection"* Tutor: Prof. Aurelio La Corte
Settembre 1996-Luglio 2002	**Laurea in Ingegneria Elettronica, indirizzo Telecomunicazioni** Università degli Studi di Catania Tesi: "*Virtual Strumentation for Planning of WLAN System*" Relatore: Prof. Aurelio La Corte, Voto: 110/110 cum laude.
Gennaio 2015	Abilitazione Scientifica Nazionale alla funzione di Professore di Seconda Fascia nel settore concorsuale 09/H1-Sistemi di Elaborazione dell'Informazioni

Gennaio 2015	Abilitazione Scientifica Nazionale alla funzione di Professore di Seconda Fascia nel settore concorsuale 01/B1-Informatica
Novembre 2002	Abilitazione all'esercizio della professione di Ingegnere

2.1 Borse di studio e di ricerca

1 Maggio 2010-21 Dicembre 2010	**Borsa di studio dal titolo "Gestione della privacy nelle Reti di Sensori Wireless"** Dipartimento di Informatica e Comunicazione Università degli Studi dell'Insubria, Varese Responsabile: Prof. Alberto Coen-Porisini
Giugno 2008	**Visiting presso Universitat Politècnica de Catalunya, nell'ambito delle ricerche condotte su Wireless Sensor Networks (WSN) e Wireless Multimedia Sensor Networks (WMSN)** Barcellona, Spagna. Tutor. Prof. I.F. Akyildiz from Georgia Institute of Technology, Atlanta, USA
Settembre 2004-Aprile 2006	**Research Scholar** Dipartimento di elettronica dell'informazione (DEI), Politecnico di Milano, Milano Tutor: Prof. Carlo Ghezzi
28-30 Giugno 2004	**Corso Microsoft "Secure architecture for network and data infrastructure accelerated bootcamp"** Microsoft Certified trainer: Sandro Vecchiarelli, Milano

3. Attività Lavorativa

1 Settembre 2016-ad oggi	**Professore Associato per il settore scientifico disciplinare Ing/Inf 05, settore concorsuale 09/H1** Università degli studi dell'Insubria, Varese
22 Dicembre 2010-30 Agosto 2016	**Ricercatore confermato per il settore scientifico disciplinare Ing/Inf 05, settore concorsuale 09/H1** Università degli studi dell'Insubria, Varese
2 Maggio 2006-30 Aprile 2010	**Assegno di Ricerca dal titolo "Sicurezza Protocollare in Architetture Informatiche e di Telecomunicazione"** Dipartimento di Informatica e Comunicazione. Università degli Studi dell'Insubria, Varese Responsabile: Prof. Alberto Coen-Porisini

3.1 Altra attività lavorativa

Gennaio 2004-Aprile 2005	Stage curriculare su Servizi di Sicurezza nell'ambito del corso di dottorato di ricerca presso Atos OriginS.p.a, Milano
Novembre 2002-Gennaio 2003	Stage ICT Helwett Packard (HP), Roma, Italia

4. Attività Didattica

4.1 Attività didattica nell'ambito di corsi di laurea da Professore Associato

Dall'A.A. 2016-2017 ad oggi	Affidamento dell'insegnamento di "***Reti di Telecomunicazione***", per il corso di laurea triennale in Informatica del Dipartimento di Scienze Teoriche e Applicate dell'Università degli studi dell'Insubria, Varese

Dall'A.A. 2017-2018 ad oggi	Affidamento dell'insegnamento di "***Innovative Telecommunication System***", per il corso di laurea magistrale in Informatica del Dipartimento di Scienze Teoriche e Applicate dell'Università degli studi dell'Insubria, Varese
Dall'A.A. 2022-2023	Affidamento dell'insegnamento di "***Fondamenti di Internet of Things***", per il corso di laurea in Informatica del Dipartimento di Scienze Teoriche e Applicate dell'Università degli studi dell'Insubria, Varese
A.A 2016-2017 e A.A 2018-2019	Affidamento dell'insegnamento di "***Laboratorio di Informatica e Comunicazione Multimediale***", per il corso di laurea triennale in Scienze della Comunicazione dell'Università degli studi dell'Insubria, Varese

4.2 Attività didattica nell'ambito di corsi di laurea da Ricercatore

Dall'A.A. 2011-2012 all'A.A. 2015-2016	Affidamento dell'insegnamento di "***Reti di Telecomunicazione***", per il corso di laurea triennale in Informatica del Dipartimento di Scienze Teoriche e Applicate dell'Università degli studi dell'Insubria, Varese
A.A. 2010-2011	Affidamento dell'insegnamento di "***Gestione delle Reti***", per il corso di laurea triennale in Informatica della Facoltà di Scienze, dell'Università degli studi dell'Insubria, Varese

4.3 Attività didattica nell'ambito di corsi di laurea da professore a contratto

Dall' A.A. 2006-2007 all'A.A. 2009-2010	Affidamento dell'insegnamento di "***Complementi di reti di telecomunicazione***", per il corso di laurea specialistica in Informatica, della Facoltà di Scienze, dell'Università degli studi dell'Insubria, Varese
A.A. 2005-2006 A.A. 2007-2008	Responsabile di laboratorio del corso di "***Informatica C***" per il corso di laurea in Ingegneria Aerospaziale (Prof. Vincenzo Martena e Prof.ssa Paola Spolettini), Politecnico di Milano, Milano

4.4 Altre attività didattiche

Settembre 2011-Dicembre 2011	Docente del corso di ***"Funzione di programmazione e gestione dei dati"*** Corso di formazione per il personale dell'azienda A.S.L. di Varese, presso A.S.L di Varese Committente: ASL di Varese, Regione Lombardia
Marzo 2010-Maggio 2010	Docente del corso di "***Funzione di programmazione e gestione dei dati***" Corso di formazione per il personale dell'azienda A.S.L. di Varese, presso A.S.Ldi Varese Committente: ASL di Varese, Regione Lombardia
Settembre 2009-Dicembre 2009	Docente del corso ***"Saperi Specialistici del Sistema Informativo Aziendale e Competenze Applicative della Rete Aziendale"*** Corso di formazione per il personale del CED (Centro Elaborazione Dati) dell'azienda ASL di Varese Committente: ASL di Varese, Regione Lombardia

Ottobre 2008-Dicembre 2008	Docente di "***Fondamenti di Networking"*** Corso di formazione per il personale del CED (Centro Elaborazione Dati) dell'azienda ASL di Varese Committente: ASL di Varese, Regione Lombardia
Maggio 2003-Settembre 2003	Docente di "***Fondamenti di Sistemi Multimediali in Rete***" Corso IFTS-POR 2000-2006 per "Esperto in architetture informatiche in riferimento alla produzione di prodotti multimediali e web nel campo dei beni culturali e del turismo", finanziato dalla Regione Sicilia Committente: Liceo scientifico "Galileo Galilei", Catania
Gennaio 2003-Marzo 2003	Docente di "***Elementi di Telecomunicazioni***" Corso IFTS per "Tecnico superiore per le Telecomunicazioni" finanziato con i fondi P.O.N 2002 dalla Regione Sicilia Committente: Istituto di Istruzione Secondaria Superiore "Ettore Majorana"

4.5 Relatore e correlatore tesi di laurea

È stata ed è relatrice e correlatrice di numerose tesi di lauree sia presso l'Università degli studi di Catania che presso l'Università degli studi dell'Insubria. Fra gli altri:

- V. Pappalardo, "*Qualità del servizio nell'interoperabilità di sistemi GPRS, UMTS, Wi-Fi*", Università degli Studi di Catania, a.a. 2003-2004
- A. Spartà, "*Modellazione di politiche di privacy e loro controllo: un caso di studio*", Università degli Studi dell'Insubria, a.a. 2005-2006
- D. Sartiano, "*Valutazione del rischio di attacco di una rete dall'esterno: il caso del Dipartimento di Informatica e Comunicazione",* Università degli Studi dell'Insubria, a.a. 2006-2007
- P. Marchetti, "*Valutazione del rischio di attacco di una rete dall'interno: il caso del Dipartimento di Informatica e Comunicazione*", a.a. 2006-2007

- L. Longo, "*Security through collaboration in global computing: a computational trust model based on temporal factors to evaluate trustworthiness of virtual identities*", a.a. 2006-2007
- F. Bignardi, "*Un protocollo di localizzazione subacqueo a risparmio energetico"*, Università degli Studi dell'Insubria, a.a. 2007-2008
- S. Rimoldi, "*CLP: Cross-layer data evaluation protocol dealing with secure Localization and Privacy information*", a.a. 2009-2010
- G. Bello, "*SDAP: Secure end-to-end Data Aggregation protocol in Privacy aware wireless sensor networks*", a.a. 2009-2010
- A. Vignati, "*Cross-layerProtocol: implementazione ed analisi delle prestazioni*", a.a. 2010-2011
- A. Tedesco, "*Implementazione di plugin per il software di monitoraggio Nagios*", a.a. 2011-2012
- M. Maffioli, "*ReDA - Valutazione dell'affidabilità dei dati mediante l'uso della reputazione dei nodi sensore in architetture ibrid*e", a.a. 2011-2012
- M. Obiso, "*Software per strumenti di misura automatici*", a.a. 2011-2012
- K. Pinto, "*Sviluppo del sito web aziendale Makerone tramite ASP.net e VB.net*", a.a. 2011-2012
- E. Bonomo, "*SES: SEcure Selecting image transmission in hybrid wireless sensor and mesh network*", a.a. 2012-2013
- A. Rizzardi, "*SETA: a SEcure sharing of Tasks in hybrid Architecture*", a.a. 2012-2013
- A. R. Van Liedekerke, "*Analisi dei requisiti e collaborazione alla realizzazione del portale clienti LIS: profilo installatore*", a.a. 2012-2013
- C. Buffoni, "*Analisi di struttura e componenti del back-end di un portale clienti*", a.a. 2013-2014
- G. Premoli, "*Confronto tra due protocolli basati su tecniche di machine learning per la valutazione della reputazione dei nodi di una rete wireless di sensori*", a.a. 2015-2016
- M. Basilico, "*Implementazione di politiche di enforcement in un'architettura per Internet of Things*", a.a. 2015-2016
- E. D'Angelo, "*Implementazione e confronto di tecniche di gestione delle chiavi per Internet of Things*", A.A. 2015-2016

- M. Colli, "*Progettazione, sviluppo e manutenzione di un servizio per l'invio di notifiche push web: Pushpad*", A.A. 2016-2017
- F. Preite, "*Creazione ed implementazione di una classe OPC UA client*", A.A. 2016-2017
- M. De Salvatore, "*Algoritmi per la revoca delle chiavi di crittografia per un'architettura di Internet of Things*", A.A. 2016-2017
- C. Racioppo, "*Integrazione dell'algoritmo di cifratura CP-ABE per soddisfare i requisiti di compatibilità ed integrità dei dati gestiti da un middleware per Internet of Things*", A.A. 2017-2018
- E. Tamburini, "*Integrazione del paradigma blockchain all'interno di un middleware security-aware per Internet of Things*", A.A. 2017-2018
- M. Cavagnino, "*Integrazione delle funzionalità del fog computing in un middleware per Internet of Things*", A.A. 2018-2019
- A. Turconi, "A*pplicazione per la gestione di richieste d'ordine e interscambio di documenti tra aziende*", A.A. 2018-2019
- E. D'Angelo, "*Crittografia biomolecolare per la protezione dei dati in nano-network per applicazioni di health-care*", A.A. 2018-2019
- L. Di Pasquale, "*Sviluppo applicazioni ad integrazione del software gestionale SAP business one*", A.A. 2018-2019
- S. Agostini, "*Analisi dello stato dell'arte della sicurezza nelle reti 5G, con particolare attenzione alle reti IoT*", A.A. 2019-2020
- F. Coglio, "*La sicurezza nelle nanotecnologie*", A.A. 2019-2020
- S. Contarino, "*Valutazione della qualità del dato all'interno di blockchain in applicazioni nell'ambito di Internet of Things*", A.A. 2019-2020
- R. Pacifico, "*Analisi dei requisiti di sicurezza dei protocolli utilizzati nell'ambito di Internet of Things*", A.A. 2019-2020
- C. Nodeda, "*Monitoraggio della rete tramite Streaming Telemetry*", A.A. 2019-2020
- A. Mirata, "*Continuous Integration - Test and Deploy Automation of a WebApp*", A.A. 2019-2020

- N. Arioli, "*Implementazione di un'infrastruttura aziendale per l'assistenza ai clienti*", A.A. 2019-2020
- Daniele Maino, "*Sviluppo di un prototipo di rete basato sul paradigma di Internet of Things tramite Node-RED*", A.A. 2019-2020
- A. Guanetti, *"Sviluppo di un'applicazione web per la digitalizzazione e gestione di oggetti smarriti nel Comune di Milano"*, A.A. 2020-2021
- M. Cova, *"Progettazione e sviluppo di un'applicazione web per la gestione della logistica aziendale con architettura a microservizi"*, A.A. 2020-2021
- R. Scari, "Design e implementazione di funzionalità per la gestione dei Curriculum Vitae e degli Stage all'interno del sistema GeCV", A.A. 2020-2021

4.6 Dottorato di ricerca

La Prof.ssa Sicari è:

- Tutor della Dr. Alessandra Rizzardi del corso di dottorato di ricerca in Informatica e Matematica del XXIX ciclo, presso l'Università degli Studi dell'Insubria. Dissertazione dal titolo: "*Security in Internet of Things: Networked smart objects*" dal 01-11-2013 al 21-12-2016
- Membro della commissione giudicatrice dell'esame finale per il conseguimento del titolo di Dottore di ricerca in Ingegneria (Programma: Ingegneria dell'Informazione) dell'Università degli studi di Pisa, A.A. 2012-2013 dal 13-12-2013 al 13-12-2013
- Membro del collegio dei docenti del dottorato di ricerca in Informatica e Matematica del Calcolo, presso l'Università degli studi dell'Insubria dal 17-05-2017 a oggi
- Revisore esterno della tesi del Dr. Emanuele Catania per il dottorato in Ingegneria informatica e delle Telecomunicazioni XXXI ciclo presso l'Università degli studi di Catania, A.A.2017-2018 dal 06-11-2017 al 01-12-2018
- Revisore esterno di una tesi per il dottorato in Ingegneria (Programma: Ingegneria dell'Informazione) presso l'Università degli studi di Pisa, A.A.2019-2020 dal 01-09-2020 a oggi

5. Attività organizzative accademiche

- Membro della commissione AIQUA per il corso di studio in Informatica dell'Università degli studi dell'Insubria, dal 2019 ad oggi.
- Membro della commissione orientamento per il corso di studio in Informatica dell'Università degli studi dell'Insubria, A.A. 2011-2012, 2012-2013; 2013-2014, 2014-2015, 2015-2016, 2016-2017, 2018-2019.
- Membro della commissione giudicatrice dell'esame finale per il conseguimento del titolo di dottore di ricerca in Ingegneria (Programma: Ingegneria dell'Informazione) dell'Università degli studi di Pisa, A.A. 2012-2013
- Organizzatrice e membro della commissione di valutazione dei progetti per l'attribuzione del "*Premio 7 Pixel, in memoria del Ch.mo Prof. Gaetano Aurelio Lanzarone*", edizione 2014, 2015, 2016

6. Attività scientifica

Sabrina Sicari è membro IEEE dal 2009 e membro Senior IEEE dal 2021.

6.1 Coordinamento di attività di ricerca

- Collaborazione scientifica con il gruppo del prof. Mattia Monga - Università statale di Milano. Principali tematiche di ricerca: Risk assessment, localizzazione, wireless sensor networks come dimostrato dalle pubblicazioni e dai progetti dal 01-01-2004 al 22-12-2014
- Membro del gruppo di ricerca in ingegneria del software del Prof. Carlo Ghezzi- Politecnico di Milano.Principale tematica di ricerca: sicurezza in web services nell'ambito del progetto europeo Secse dal 10-09-2004 al 30-04-2006
- Collaborazione scientifica con il Laboratorio di Telematica del Prof. Luigi Alfredo Grieco Dipartimento di Ingegneria Elettrica e dell'Informazione - Politecnico di Bari. Principali tematiche di ricerca: Wireless sensor networks, wireless multimedia sensor networks, Internet of Things, nanotechnologies, come dimostrato dalle pubblicazioni dal 04-05-2007 a oggi

- Collaborazione scientifica con il gruppo del prof. Nicola Gatti - DEI - Politecnico di Milano. Principali tematiche di ricerca: Wireless sensor networks, game theroy come dimostrato dalle pubblicazioni e dal progetto SMScom dal 01-01-2008 al 01-01-2011
- Collaborazione scientifica con il centro di ricerca Create-net del Prof. Imirich Chlamtac. Principali tematiche di ricerca: definizione di architetture security aware per wireless sensor networks, Internet of Things come dimostrato dalle pubblicazioni dal 01-10-2008 al 20-12-2015
- Collaborazione scientifica con il gruppo di basi di dati della profssa. Cinzia Cappiello - DEI - Politecnico di Milano. Principali tematiche di ricerca: Definizione di politiche di privacy e di qualità del servizio per sistemi mobili, definizione di architetture per Internet of Things, definizione di algoritmi di automatic quality and security assessment per Internet of Things, come dimostrato dalle pubblicazioni e dal progetto Mobile service for agrofood domain-MoSe. dal 01-01-2009 a oggi
- Collaborazione scientifica con il gruppo del prof. Stephen Hailes - University College of London. Principali tematiche di ricerca: sicurezza nelle wireless sensor networks e in Internet of Things, dal 01-01-2009 al 20-12-2013
- Collaborazione scientifica con il gruppo di ingegneria del software del prof. Gianluca Dini dell'Università statale di Pisa. Principali tematiche di ricerca: wireless sensor networks, Internet of Things e tecniche di accesso, dal 10-01-2009 a oggi
- Collaborazione scientifica con il gruppo del prof. Thierry Monteil di LAAS_CNRS, Tolosa (Francia). Principali tematiche: M2M come dimostrato dalle pubblicazioni, dal 01-02-2014 al 20-12-2015
- Collaborazione scientifica con il gruppo del prof. Roberto Passerone, Dipartimento di Ingegneria e Scienza dell'Informazione dell'Università di Trento. Principale tematica: simulatori ed emulatori per le wireless sensor networks, come dimostrato dalle pubblicazioni, dal 01-09-2014 al 20-12-2016
- Collaborazione scientifica con U-Hopper con il Dr. Daniele Miorandi. Principali tematiche: sicurezza in Internet of Things, sticky policies, enforcement, risk assessment, blockchain, come dimostrato dalle pubblicazioni, dal 01-01-2016 a oggi

- Responsabile scientifico del gruppo di sistemi di elaborazione delle informazioni del Dipartimento di scienza teoriche e applicate (DISTA), Università degli studi dell'Insubria. Principali tematiche: wireless sensor networks, Internet of Things, definizione di politiche di sicurezza & privacy, nanotecnologie, come dimostrato dalle pubblicazioni. dal 01-09-2016 a oggi
- Responsabile scientifico della borsa di studio dal titolo "Sicurezza in Internet of Things", attribuita alla Dr. Alessandra Rizzardi dal 01-12-2016 al 30-06-2017
- Responsabile scientifico dell'assegno di ricerca " Sicurezza in Internet of Things", attribuita alla Dr. Alessandra Rizzardi dal 01-07-2017 al 31-03-2020

6.2 Partecipazione e responsabilità a progetti di ricerca

- Responsabile scientifico per l'Università degli studi dell'Insubria per il progetto regionale Mobile service for agrofood domain (MoseForAgroFood) responsabile del progetto Prof. Carlo Batini, Università degli studi di Milano Bicocca dal 01-09-2010 al 01-09-2012
- Responsabile scientifico del finanziamento delle attività base di ricerca per l'anno 2017 dal 03-12-2017 a oggi
- Responsabile scientifico del contratto di ricerca con Confartigianato Varese, Italia dal titolo " Smart Living e IoT: Studio e scenari applicativi" dal 27-11-2018 al 31-12-2018
- Membro dell'unità di ricerca per il progetto Europeo “SeCse” - responsabile del progetto Prof. Carlo Ghezzi, Politecnico di Milano dal 01-09-2004 al 01-09-2008
- Responsabile scientifico per l'Università degli studi dell'Insubria per il progetto "SMSCom - SelfManaging Situated Computing" project, ERC advanced grant - responsabile del progetto Prof. Carlo Ghezzi zi, Politecnico di Milano, dal 01-09-2008 al 01-09-2013
- Responsabile tecnico scientifico del contratto di collaborazione fra Dicom e le aziende E security s.r.l. e Ecohmedia s.r.l per integrare il TMS (*Threat Managemnet System*), sviluppato da E-security in collaborazione con Ecohmedia, con il metodo di *risk analysis* sviluppato dalla dr. Sabrina Sicari et al., al fine di analizzare e valutare su basi oggettive il rischio cui è esposto un sistema informatico e telematico complesso,mediante metodo ingegneristico sistematico, maggio 2009-dicembre 2009
- Membro dell'unità di ricerca del Dipartimento di Ingegneria Informatica e delle Telecomunicazioni, dell'Università degli studi di Catania per il progetto "Cluster 16", per lo sviluppo di strumenti virtuali per la didattica nel settore della radio-propagazione (e-learning),

responsabile del progetto di ricerca Prof. Sergio Palazzo, responsabile Scientifico Prof. Aurelio La Corte, da febbraio 2002 a giugno 2002

6.3 Comitati editoriali, comitati scientifici e attività di revisione

6.3.1 Editorial Board

- Membro dell'editorial board della rivista internazionale Computer Networks (Elsevier) dal 01-01-2008 a oggi
- Guest Editor per la Special Issue “Sensor, Systems and Sofware” della rivista internazionale ACM Mobile Networks & Applications (ACM MONET) dal 01-05-2009 al 01-04-2011
- Guest Editor per la Special Issue "Security, Privacy and Trust Management in Internet of Things era (SePrit)" della rivista internazionale Ad Hoc Networks (Elsevier) dal 01-05-2009 al 01-10-2013
- Membro dell'editorial board della rivista internazionale IEEE Internet of Things (IoT) Journal dal 01-01-2016 a oggi
- Membro dell'editorial board della rivista internazionale Transactions on Emerging TelecommunicationsTechnologies (Wiley) - ETT dal 01-01-2017 a oggi
- Membro dell'editorial board della rivista internazionale Internet Technology Letters (Wiley) - ITL dal 01-05-2017 a oggi
- Membro dell'editorial board della rivista internazionale Journal on Future and Evolving Technologies (ITU J-FET) dal 10-08-2020 a oggi

6.3.2 Chair a congressi internazionali

- Membro dello Steering Committee alla conferenza internazionale “S-cube” per le edizioni 2010, 2012, 2013, 2014
- General co-chair e organizzatrice della prima edizione della conferenza internazionale “Sensor Systems and Sofware (S-Cube’09)”, Pisa, 7-9 settembre 2009
- Session Chair nella conferenza internazionale “Sensor Systems and Sofware” (S-cube’09), Pisa, 7-9 settembre 2009

6.3.3 Cominati di programma

- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "IEEE SECON", New Orleans, USA, giugno 2013, Singapore giugno 2014
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "IEEE ICC", Kyoto, Giappone, giugno 2011, Budapest, Ungheria, giugno 2013, Londra, Inghilterra, giugno 2015, Kuala, Lumpur, Malesia, maggio 2016, Parigi, Francia, maggio 2017, Kansas City, MO, USA, maggio 2018, Shanghai, China, maggio 2019, Virtual Conference, giugno 2020, Montreal, Canada, giugno 2021, Seoul, South Korea, maggio 2022
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "IEEE Globecom", Paphos, Isola di Cipro, nell'ottobre 2010, Houston, USA, dicembre 2011, Atlanta, USA, dicembre 2013, Austin, USA, dicembre 2014, San Diego, California, dicembre 2015
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "ACM Quality of service and Security in WIreless and mobile NETwork" (Q2SWinet), Tenerife, Spagna, ottobre 2009, Bodrum, Turchia, ottobre 2010, Miami, USA, ottobre 2011, Paphos, Isola di Cipro, ottobre 2012, Barcellona, Spagna, ottobre 2013
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "Sensornets", Roma, Italia, febbraio 2012, Barcellona, Spagna, febbraio 2013, Lisbona, Portogallo, gennaio2014
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al workshop internazionale "Sesena 2010 (co-located with ICSE)", Zurigo, Svizzera, giugno 2010
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "GIIS 2011", Da Nang, Vietnam, agosto 2011
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "IEEE IWCMC", Istanbul, Turchia, luglio 2011, Cipro, agosto 2012
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "IEEE IWCMC 2012", Sardegna, Itala, agosto 2013
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "IEEE IWCMC 2013", Cipro, agosto 2014, Dubrovinik, Croazia, agosto 2015, Valencia, Spagna, giugno 2016, Paphos, Cipro, settembre 2017
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "S-cube", Miami, USA, dicembre 2010, Lisbona, Portogallo, giugno 2012, Lucca, Italia, giugno 2013

- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "ICDT", Chamonix, Francia, aprile 2012, Venezia, Italia, aprile 2013, Nizza, Francia, febbraio 2014, Barcellona, Spagna, aprile 2015
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "ITC 2013", Shangai, Cina, settembre 2013
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "Mobility", Venezia, Italia, ottobre 2012, Lisbona, Portogallo, novembre 2013, Parigi, Francia, luglio 2014, Brussel, Belgio, giugno 2015, Valencia, Spagna, maggio 2016
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "SNDS", Kerala, India, ottobre 2012, Thiruvanthapuram, India, marzo 2014
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "SNIGM", Nova Scotia, Canada, giugno 2013, Hasselt, Belgio, giugno 2014
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "WMSN 2012", Barcellona, Spagna, ottobre 2012, Lione, Francia, ottobre 2013
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "MoWNet", Roma, Italia, settembre 2014, Cairo, Egitto, aprile 2016, Avignone, Francia, maggio 2017, Tangier, Marocco, aprile 2018
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "SSCC", Mysore, India, agosto 2013, Delhi, India, settembre 2014, Kerala, India, agosto 2015, Jaipur, India, agosto 2016, Manipal, India, agosto 2017, Bangalore, India, agosto 2018
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "IEEE IoT 2013", Lione, Francia, ottobre 2013
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "IEEE WiMob", Cipro, ottobre 2014, Abu Dhabi, ottobre 2015, New York, USA, ottobre 2016, Roma, Italia, ottobre 2017, Limassol, Cipro, ottobre 2018
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "IEEE ICCVE", Las Vegas, USA, dicembre 2013, Vienna, Austria, novembre 2014, Shenzhen, Cina, ottobre 2015, Seattle, USA, ottobre 2016, Graz, Austria, novembre 2022
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "SensorComm 2014", Lisbona, Portogallo, novembre 2014

- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "ICWMC", St.Julians, Malta, ottobre 2015, Barcellona, Spagna, novembre 2016
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "ICMWT 2015", Bangkok, Tailandia, giugno 2015
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "CTRQ 2016", Lisbona, Portogallo, febbraio 2016
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "I4CT 2016", Kota Kinabalu, Sabah, aprile 2016
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "I4CT 2018", Kuching, Malesia, aprile 2018
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "WiCOM 2016", Cina, settembre 2016
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "ACM CoCoNet 2015", Thiruvanthapuram, India, dicembre 2015
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "IEEE AINA 2015", Gwangju,Corea, marzo 2015
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "IEEE I4CT 2015", Kunching, Malesia, aprile 2015
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "IEEE INFOCOM", conferenza virtuale, luglio 2020, conferenza virtuale, maggio 2021, conferenza virtuale, maggio 2022
- Partecipazione in qualità di membro del comitato tecnico di programma (TPC member) al congresso internazionale "IEEE CyberneticsCom", conferenza virtuale, giugno 2022

6.3.4 Attività di revisore

- Revisore su invito di varie riviste internazionali e conferenze internazionali, tra cui: *Pervasive and Mobile Computing (Elsevier); IEEE Transactions on Vehicular Technology; ACM-Monet; International Journal of Computer Applications in Technology(IJCAT); Journal of Sensor and Actuator Networks (JSAN); Security and Communication Networks (SCN); Computer and Electronics in Agriculture (Elsevier); Computers & Electrical Engineering (Elsevier); Transactions on Emerging Telecommunication Technologies (ETT); Sensors; Wireless Communications and Mobile Computing; Computer Networks (Elsevier); IEEE ICC; IEEE ISIE; S-Cube; Mobility; ICDT; ACMQ2SWinet; Mobility; SNDS*

- Membro REPRISE: membro dell'albo degli esperti scientifici istituito presso il MIUR, per la valutazione delle proposte di progetto relative alla ricerca di base.

6.4 Riconoscimenti

6.4.1 Invited keynote talks

Ottobre 2020	Keynote speaker "**19th International Conference on Ad Hoc Networks and Wireless (AdHoc-Now 2020)**" Titolo: "*Internet of Things: towards the development of a smart yet secure world*" Bari, Italia

6.4.2 Invited speaker

Giugno 2009	Relatore su invito a "**SMSCom (Self-ManagingSituated Computing)**" Meeting di progetto di ERC (European Research Council)-"Advanced Grants" Responsabile del Progetto: Prof. Carlo Ghezzi Lago di Como, Como, Italia
Novembre 2008	Relatore su invito alla Panel Discussion "**The Internet of Things and Services**" coordinatore: Prof. Atta BADII from University of Reading, School of System Engineering, United Kingdom Organizzato dalla Commissione Europea, ICT 2008, Lione, Francia
Maggio 2008	Seminario "**An Innovative Risk Assessment Methodology**" Centro di ricerca internazionale Create-Net, Trento,Italia

Luglio 2007	Relatore su invito a workshop "**D.Lgs.231/2001- D.Lgs.196/200 ISO17799 Implicazioni Operative e Metodologie per la Sicurezza Informatica**" Organizzato da COM Metodi s.p.a Milano

6.4.3 Premi per articoli scientifici

Vincitore di "*Best paper award*" alla IEEE International Congress on Ultra Modern Telecommunications and Control Systems, 2010 (ICUMT'10), Mosca, Russia, 2010, per l'articolo "Localization security in wireless sensor networks as a non-cooperative game", autori Dr. Nicola Gatti, Prof. Mattia Monga e Dr. Sabrina Sicari.

7. Attività di ricerca

L'attività di ricerca, svolta da Sabrina Sicari, inizialmente incentrata su problematiche di telecomunicazione, dal 2004- in corrispondenza dell'inizio del periodo di *research scolar* nel gruppo di ingegneria del software, presso il Politecnico di Milano - è stata rivolta a tematiche di ingegneria del software, con eventuali applicazioni alle reti.

L'attività di ricerca, iniziata durante il corso di dottorato, è stata articolata nel corso degli anni su diversi temi. In particolare: dal 2003 al 2005 la ricerca è stata focalizzata sull'analisi della qualità del servizio, integrazione di reti *wireless* eterogenee e sistemi "Voice over IP"; dal 2004 ad oggi sulla definizione di metodologie per la valutazione dei rischi, e le connesse problematiche di sicurezza; dal 2006, a seguito della vincita dell'assegno di ricerca dal titolo "*Sicurezza Protocollare in Architetture Informatiche e di Telecomunicazione*", presso il Dipartimento di Informatica e Comunicazione, dell'Università degli studi dell'Insubria, sul modellamento delle politiche di privacy. Tale attività prosegue ad oggi.

Dal 2007 ad oggi, gli interessi di Sabrina Sicari sono stati ampliati dalle ricerche condotte sulle reti di sensori *wireless* (WSN e WMSN), con particolare attenzione alla:

- definizione di soluzioni finalizzate a garantire la privacy nelle reti WSN, basate su modelli definiti in UML
- definizione e simulazione di metodologie "*cross layer"* aventi lo scopo di valutare la qualità del dato aggregato, alla luce di informazioni di *routing* e di localizzazione
- definizione di architetture ibride (*wireless mesh network* e *wireless sensor network*), in grado di garantire la sicurezza del dato, in condizioni di limitate risorse energetiche
- definizione di algoritmi di localizzazione a basso consumo di potenza, per reti di sensori subacquee
- analisi di reti *wireless* sicure costituite da sensori multimediali (WMSN)
- caratterizzazione del comportamento di nodi "malevoli" con l'ausilio della teoria dei giochi
- valutazione della reputazione dei nodi mediante tecniche di *machine learning*
- confronto delle performance di svariati simulatori utilizzati per valutare protocolli e algoritmi di routing definiti per le WSN.

Infine, dal 2009 le ricerche sulle reti di sensori *wireless* sono state ampliate con ricerche condotte con il nuovo paradigma di *Internet of Things* (IoT) con particolare attenzione alla:

- definizione di soluzioni finalizzate a garantire la privacy & sicurezza, basate su modelli definiti in UML
- definizione di un'architettura di riferimento e sviluppo di un prototipo
- definizione ed implementazione di algoritmi per la valutazione automatica dei dati forniti dalle sorgenti
- definizione ed implementazione di meccanismi sicuri ed efficienti per la condivisione dei servizi offerti da un sistema basato su IoT
- definizione ed implementazione di politiche di enforcement e sincronizzazione delle stesse, in presenza di un sistema distribuito
- utilizzo di sticky policies per garantire la sicurezza e la privacy delle informazioni trasmesse tra diversi domini applicativi
- utilizzo di soluzioni basate su Attribute Based Encryption (ABE) per definire opportune politiche di sicurezza e privacy nell'ambito di IoT

- definizione di opportuni scenari in ambito IoT e relativa applicazione di soluzioni security e privacy-aware
- definizione di metodologie per svolgere un'analisi del rischio all'interno di sistemi IoT
- definizione di soluzioni per prevenire e fronteggiare attacchi ad un sistema IoT
- definizione di soluzioni per garantire sicurezza e privacy nell'architettura Open Source Machine-to-Machine (OM2M)
- definizione di soluzioni per garantire sicurezza e privacy nell'ambito del paradigma Information Centric Networking (ICN)
- definizione di soluzioni per garantire sicurezza e privacy in presenza di nano-tecnologie, all'interno di Internet of Nano-Things (IoNT)
- integrazione del concetto di fog computing e della tecnologia blockchain all'interno di IoT
- analisi dello stato dell'arte della sicurezza nelle reti 5G
- valutazione delle soluzioni proposte, in termini di performance, utilizzando tool e simulatori quali Node-RED, Omnet++, Castalia, Cooja.

- **AREA: Qualità del Servizio**

  La necessità di garantire la qualità del servizio (QoS) è uno dei requisiti chiave di qualunque sistema. Gli enti di standardizzazione hanno definito varie metriche finalizzate alla valutazione della qualità del servizio *end-to-end,* in funzione dei differenti requisiti dell'utente.

  La qualità del servizio può essere stimata in vari modi ed includere differenti requisiti di servizio come *performance, availability, reliability e security.* Le metriche che descrivono la qualità del servizio possono essere definite in modo stocastico o deterministico, o mediante valori medi in intervalli di tempo definiti.

  Il termine qualità del servizio può assumere diversi significati; in letteratura si distingue fra "*Intrinsic Quality of Service", "Perceived Quality of Service" e "Assessed Quality of Service".* Il significato attribuito alla qualità del servizio varia in funzione dell'ambiente, del protocollo utilizzato e del punto di vista (*cliente, service provider, ingegnere*). E' quindi di interesse scientifico l'indagine sui parametri di qualità del servizio in funzione del contesto generale e della applicazione particolare. Lo studio di tecniche atte a garantire un adeguato livello di qualità del servizio è un tema di ricerca ortogonale a vari settori.

In questo ambito Sabrina Sicari ha definito e analizzato un modello di qualità del servizio, suddiviso in livelli che mettesse in luce le metriche per differenti protocolli e applicazioni.

Il modello consta di 8 livelli: *Basic Level; Multimedia Level; Wireless Level; Heterogeneous system; Application Level; Quality of Protection; Perceived QoS e Assessed QoS.* Il *Basic Level* coincide con il concetto di *Intrinsic Quality of Service* ed include i tradizionali parametri di qualità del servizio, di natura esclusivamente tecnica (*delay, bitter, throughput etc.*), che devono essere considerati in qualunque tipo di connessione: a questo livello è chiaro che la qualità del servizio offerta è tanto migliore quanto maggiore è la capacità di garantire la gestione delle priorità, delle congestioni, della banda.

Il *Multimedia Level*, come è chiaro dalla denominazione, pone l'accento sui requisiti dei servizi multimediali. L'inserimento nel modello di questo livello è scaturito dalla necessità di definire nuove tecniche di controllo del traffico e della rete, per riuscire a trasportare servizi multimediali su reti integrate, in modo da garantire adeguate prestazioni in termini di qualità del servizio percepibile dall'utente, anche a fronte di variazioni delle caratteristiche *end-to-end* del canale di comunicazione. I meccanismi classici di controllo, infatti, non tengono conto delle mutue relazioni temporali che legano gli oggetti multimediali appartenenti a flussi informativi distinti. Le stesse definizioni di qualità del servizio possono perdere di significato una volta che flussi monomediali, aventi (singolarmente) requisiti del tutto differenti, vengono combinati insieme per realizzare un servizio multimediale.

Inoltre, meccanismi di controllo progettati per operare in un ambiente di comunicazione cablato possono fallire in presenza di un utente mobile. Quest'ultima problematica ha determinato l'inserimento nel modello di un *Wireless Level*. La mobilità dell'utente, il passaggio da una cella all'altra determina, la criticità di alcuni parametri di qualità del servizio: variazione del ritardo, duplicazione o perdita di pacchetti a causa delle operazioni di *handover*.

La situazione risulta più critica allorquando ci si sposta al livello immediatamente superiore del modello, denominato *Heterogeneous System*, dove occorre garantire un'adeguata qualità del servizio ad un utente mobile che cambia, nei suoi spostamenti, anche il protocollo di accesso. In questo caso, la capacità di garantire un'adeguata qualità del servizio risulta equivalente alla capacità di garantire un'adeguata *session continuity.*

Al variare dell' applicazione, sia essa un'operazione di *web browsing* o un servizio VoIP, variano i requisiti a livello *end-end* di qualità del servizio. Questi aspetti sono affrontati nell'A*pplication Level* del modello.

Tuttavia, non si può pensare di garantire un'adeguata qualità del servizio prescindendo da opportune misure di sicurezza, motivo per cui il livello immediatamente superiore prende il nome di *Quality of Protection*.

Negli ultimi due livelli del modello sono state posizionate la *Perceived Quality of Service* e *l'Assessed Quality of Service,* già definiti in letteratura, che concludono il quadro fornito sulla qualità del servizio e sui relativi parametri prestazionali.

Il modello è stato applicato per l'analisi e l'implementazione di meccanismi finalizzati alla garanzia della *session continuity* in reti *wireless* eterogenee. Sabrina Sicari si è occupata di analizzare e rivedere il concetto di qualità del servizio in un ambiente di comunicazione *wired cum wireless,* alla luce della mobilità dell'utente. A tal fine è stato implementato un appropriato *middleware* che consenta ad un terminale mobile di usufruire di servizi *wireless* IP mobili distribuiti su area metropolitana.

Sabrina Sicari ha anche applicato il modello per la definizione di un algoritmo per garantire qualità del servizio in reti *zeroconfiguration,* mediante la realizzazione di *Virtual LANs,* usando come *testbed* una *home network*.

Infine, il modello è stato integrato con un sistema *Voice over IP*. L'adozione di una soluzione integrata e convergente di voce e dati, su una rete IP, determina un nuovo grado di soddisfazione dell'utente. I parametri di qualità del servizio sono stati utilizzati come criteri per la valutazione dei vantaggi/svantaggi associati all'adozione della nuova tecnologia.

Quindi, la ricerca di Sabrina Sicari, nell'ambito della qualità del servizio, comprende sia l'analisi di algoritmi *zeroconfiguration* che la definizione di *middleware ad-hoc* per reti *wireless* eterogenee, oltre che lo studio di sistemi *Voice over IP*.

Tale attività di ricerca è stata svolta negli anni dal 2003 al 2005. Di seguito maggiori dettagli sulle ricerche, scaturite dall'analisi di ogni livello del modello proposto, i cui risultati sono stati presentati in [R1][R2][R3][C1].

Sottoarea: VLAN Zeroconfiguration Network [R2]

E' stato affrontato il problema della necessità di autoconfigurazione dovuta alla elevata proliferazione di *devices,* e al bisogno di essere costantemente connessi ("*anytime, anywhere*") con una certa garanzia di qualità del servizio. In tale contesto è stato sviluppato un algoritmo in grado di utilizzare in modo congiunto le potenzialità del protocollo *Zeroconfiguration* e delle *Virtual Local Area*

Networks (VLANs). Il protocollo *Zeroconfiguration* è in grado di soddisfare a pieno il requisito di autoconfigurazione, poiché fornisce una classe di indirizzi IP che non richiede alcuna configurazione manuale, né amministrazione. Le VLANs consentono di raggruppare i "*devices*" in funzione dei requisiti di qualità del servizio. Le gestione delle VLANs è demandata ad un VLAN manager, requisito che è implementato estendendo l'architettura dell' OSGi *residential gateway*, sfruttando le potenzialità della struttura a *bundles*. L'obiettivo di questo lavoro di ricerca è di analizzare le funzionalità già contemplate nel protocollo *Zeroconfiguration*, estendendo ed aggiornando lo stesso con opportune integrazioni che garantiscano qualità del servizio mediante un'adeguata segmentazione del traffico. Si suggerisce l'uso del protocollo *Zeroconfigutation* per consentire il "*plug and play*" in sistemi IPv4, a causa della lenta diffusione di IPv6, che prevede dei meccanismi di autoconfigurazione.

Sottoarea: Heterogeneous wireless system [R1]

Sono stati trattati alcuni aspetti relativi alla qualità del servizio in un ambiente *wireless cum wired*, focalizzando l'attenzione sul problema della *session continuity*. La soluzione proposta prevede l'utilizzo di un opportuno *middleware* che consenta ad un terminale mobile di muoversi liberamente all'interno di una MAN (*Metropolitan Area Network*) sfruttando le potenzialità dell' IP *mobility*. La soluzione è stata testata in una *wireless mobility framework*, costituita da "isole *wireless*" dislocate all'interno del campus dell'Università di Catania, collegate mediante fibra ottica con estensione a livello MAN. Tale *framework* consente ad un utente mobile, dotato di un PDA, di usufruire di IP *mobility* usando le potenzialità del *middleware*, basato sulle tre tecnologie *wireless* con differenti livelli di copertura: Bluethoot; Wi-Fi e GPRS.

Sottoarea: VoIP System [R3][C1]

Questa attività, svolta in collaborazione con l'Università degli studi di Messina e con la Sapienza di Roma, ha per oggetto lo studio (da un punto di vista tecnico-economico) dei sistemi "*Voice over IP*"(VoIP), al fine di valutarne l*'Assessed Quality of Service.* L'*Assessed Quality of Service* è un parametro fondamentale, in quanto rappresenta un giudizio complessivo sul sistema/tecnologia in esame. La convergenza di servizi voce *real-time*, su reti per dati basate sul protocollo Internet, coinvolge parecchi aspetti tecnici, che diventano strumentali per la valutazione economica. L'analisi condotta ha dovuto considerare molti fattori fra di loro eterogenei: la qualità del servizio percepita

dall'utente, "*availability*" e "*realibility*" del servizio e del sistema, costi, investimento iniziale, ritorno dell'investimento (ROI), "*break even point*", "*total cost of ownership*". L'indagine è stata realizzata misurando i suddetti parametri nel sistema VoIP implementato *ad hoc* nel *campus* dell'Università degli studi di Catania.

- **AREA: Sicurezza e Privacy**

Tale attività, svolta sia presso il Dipartimento di Elettronica dell'Informazione (DEI), del Politecnico di Milano, in collaborazione con l'Università Statale di Milano, che presso il Dipartimento di Informatica e Comunicazione (DICOM), dal 2011 Dipartimento di Scienze Teoriche e Applicate (Dista), dell' Università degli studi dell'Insubria di Varese, nasce dalla consapevolezza che, allo stato attuale, non è possibile parlare di qualità del servizio senza una adeguata garanzia di sicurezza e di privacy. La qualità del servizio e la sicurezza/privacy non sono più due filoni separati, ma sia la sicurezza che la privacy diventano un parametro/dimensione di qualità del servizio. Si assiste alla nascita e diffusione di un nuovo concetto: "*Quality of Protection*" (QoP).

Tale attività iniziata nel 2004 prosegue ad oggi. Di seguito maggiori dettagli sulle ricerche scaturite, i cui risultati sono stati presentati in [C2][C3][C4][C5[C7][C8] [C9][C14][C20][R4][R5][R6][R7] [R12][R25][R27]][CH1].

Sottoarea: Web Service Security [R25]

Tale attività, inquadrata nell'ambito del progetto europeo SeCse e svolta all'inizio (anno 2004) del *research period* presso il Dipartimento di Elettronica dell'Informazione (DEI, Politecnico di Milano), in collaborazione con il Cefriel, ha avuto come obiettivo l'analisi e riorganizzazione dello stato dell'arte della sicurezza nelle architetture SOA (*Service Oriented Architecture*) in generale, e *web service* in particolare.

L'adozione delle architetture SOA per lo sviluppo di sistemi a servizi pone problematiche di sicurezza classificabili in due macrocategorie: da un lato, l'esigenza di interazione, per la quale occorre costruire un substrato omogeneo per far dialogare servizi operanti su infrastrutture di sicurezza diverse; dall'altro, i problemi derivanti dalla volontà di consentire l'instaurazione dei suddetti dialoghi anche in modo dinamico, addirittura senza una conoscenza a priori delle aziende coinvolte nelle interazioni. Dallo studio e dall'analisi condotta da Sabrina Sicari, si evince che, allo stato attuale, non esistono soluzioni in grado di soddisfare interamente il requisito di interazione fra modelli di sicurezza

eterogenei: il linguaggio SAML (*Security Assertion Markup Language*) definisce un formato standard per descrivere informazioni di sicurezza (es: di autenticazione e autorizzazione), in modo del tutto indipendente dalle specifiche tecnologie sottostanti. *WS-Security* arricchisce l'intestazione di un messaggio SOAP, definendo un modo standard per trasportare le informazioni relative alla sicurezza fra i due *end-points* della comunicazione, anche in presenza di una trasmissione cui si frappongono uno o più intermediari (HTTPS, ad esempio, supporta solo la sicurezza *point-to-point*).

Il completo soddisfacimento del requisito di interazione non può essere raggiunto solo con l'adozione di un protocollo standard (WS-Security) che estenda SOAP. Infatti, la specifica WS-Security propone un modello astratto per la sicurezza dei sistemi web service; tuttavia, non definisce concreti meccanismi di negoziazione che consentano di trovare un accordo sulla scelta della tipologia di informazioni di sicurezza da trasportare (username/password, piuttosto che certificati X.509, ad esempio) tra le parti che devono interagire.

Inoltre, l'analisi dello stato dell'arte ha evidenziato anche l'assenza di metodologie, tecnologie e *tools* di supporto per venire incontro ai problemi legati al dinamismo, ossia la creazione di legami *on-demand*. Le suddette considerazioni sullo stato dell'arte dei requisiti di sicurezza nelle architetture SOA sono state presentate in [R25].

Sottoarea: Metodologie di Risk Assessment [C2][C3][C4] [C8] [R4][R5][R6][R7][R12]

La sicurezza è un processo caratterizzato da fasi che devono essere eseguite in modo ordinato e sistematico: una fase di fondamentale importanza è rappresentata dal risk assessment. Infatti, come affermano M.Howard e D.LeBlanc, nessun sistema può essere sicuro senza una preventiva indagine sulle minacce e sulle vulnerabilità e quindi sul rischio associato. Pertanto, il risk assessment in generale, e l'analisi del rischio in particolare, sono punti cruciali nella definizione di una soluzione di sicurezza: è fondamentale stabilire la soglia di rischio accettabile.

Sebbene sia chiara alla comunità scientifica l'importanza di una corretta valutazione dei rischi di un sistema, i metodi presenti in letteratura sono solo in grado di valutare l'effetto di ciascuna vulnerabilità singolarmente, senza tener in conto l'effetto dell'interazione fra i suddetti fattori di rischio. L'*attack tree*, pur essendo un metodo largamente diffuso, consente solo di evidenziare dipendenze dirette-strutturali, motivo per cui l'approccio proposto da Sabrina Sicari prevede l'uso congiunto e sequenziale di *attack tree* e *vulnerability dependence graph*. I grafi sono stati già largamente utilizzati nell'ambito della sicurezza, ma ora cambiano le finalità degli stessi, ad esempio gli *attack graphes*,

diagrammi stato-transizione, sono applicati per definire le proprietà di sicurezza di un sistema, mentre i *vulnerability dependence graphes*, utilizzati da Sabrina Sicari, servono solo per l'individuazione e valutazione delle dipendenze. Alla luce delle problematiche evidenziate, si propone un approccio per la valutazione del rischio in ambienti distribuiti basato sulla conoscenza delle vulnerabilità di *links* e componenti, sulle dipendenze reciproche e sul valore della loro *exploitability* (misura della difficoltà a realizzare un attacco). Le dipendenze analizzate tengono conto di vincoli dovuti alla architettura, topologia e contesto. Inoltre, una critica che spesso si muove contro il quantitative *risk assessment* è relativa alla validità dei valori assegnati. La valutazione dell'*exploitability* è approssimativa, basata sulle conoscenze personali/soggettive di esperti nel settore. Quindi, lo scetticismo della comunità scientifica verso la validità e utilità dei risultati del *risk assessment* può essere ricondotto a due principali cause: 1) l' intrinseca difficoltà a trovare un ordine totale fra i valori di *exploitabilities* di differenti vulnerabilità, ossia la difficoltà a confrontare problemi di sicurezza differenti (e non correlati) mediante la stessa metrica, 2) la difficoltà a confrontare le valutazioni del rischio ottenute mediante metriche differenti. Allo scopo di risolvere i suddetti limiti, la metodologia di *risk assessment*, definita da Sabrina Sicari, oltre a valutare le dipendenze fra le vulnerabilità del sistema, risulta svincolata dalla soggettività delle valutazioni degli esperti. L'approccio proposto pone l'accento sull'importanza dell'ordinamento dei valori dell'*exploitability* di ciascuna vulnerabilità, più che sul loro valore assoluto; infatti è importante che gli indici riflettano la difficoltà relativa ad attaccare una data risorsa. La metodologia realizzata è svincolata dai valori di *exploitabilities* basando la valutazione del rischio sulla struttura della metrica prescelta. Inoltre, la metodologia è in grado, utilizzando un approccio sistematico, sia di definire una metrica comune che non privilegi alcun esperto, che una metrica che tenga conto del diverso grado di preparazione di ciascun esperto. In entrambi i casi la metrica comune definita non altera, in alcun modo, i risultati ottenuti dai vari esperti. La metodologia è sostenuta da una ampia e dettagliata formulazione analitica.

Il metodo è anche un valido strumento per la valutazione dell'impatto di nuove vulnerabilità sull'equilibrio del sistema e può essere applicato, oltre che per la valutazione del rischio di un sistema, anche come supporto nell'analisi dell'effetto di alcune soluzione di sicurezza, finalizzate alla riduzione di un rischio valutato.

La metodologia di "*risk assessment*" definita è stata applicata sia ad un sistema "Voice over IP" che alla rete del Dipartimento di Informatica e Comunicazione dell'Università degli studi dell'Insubria, che a sistemi di grandi dimensioni al fine di testarne la validità e l'efficacia su casi reali. I risultati ottenuti sono stati pubblicati in [C2][C3][C4][C8][R4][R5][R6][R7][R12]. Tale attività di ricerca

iniziata durante il corso di dottorato (2004) prosegue ad oggi. I primi risultati furono anche pubblicati nella tesi di dottorato di Sabrina Sicari.

Sottoarea: Modelli per l'Enforcement delle Politiche di Privacy [C5[C7][C9][C14][C20][R27][CH1]

La privacy è un argomento chiave nella società odierna, ed è infatti oggetto di crescente attenzione sia da parte dei consumatori, che delle aziende, della ricerca oltre che degli enti di legislazione. Gli atti legislativi, come *European Union Directive for Personal Data, the Health Insurance Portability and Accountability Act for Healthcare* e *the Gramm Leach Bliley Act for Financial Institute,* sono un esempio della necessità di regolamentare la protezione della privacy degli utenti. Sebbene le aziende abbiano definito varie strategie, finalizzate alla protezione dei dati dell'utente (es. P3P *language*), nessuno di questi approcci definisce un meccanismo sistematico che descriva come i dati personali degli utenti debbano essere trattati, dopo essere stati raccolti.

La garanzia della privacy può essere raggiunta solo mediante delle opportune politiche che determinino l' *enforcement* della privacy stessa all'interno dei sistemi di elaborazione dei dati.

L'obiettivo di questa ricerca è di proporre un modello concettuale che consenta la definizione e l'*enforcement* delle politiche di privacy. Il modello, definito in UML (*Universal Mark Up Language*), è uno strumento di supporto nella fase di *design time* per la realizzazione di sistemi conformi alla vigente normativa sulla privacy, in quanto fornisce un modo semplice per rappresentare tutti i concetti coinvolti nella privacy stessa (es. responsabile trattamento, consenso informato, obbligo e finalità ecc). La rappresentazione in UML, per la descrizione delle politiche sulla privacy, è una soluzione innovativa; infatti l'UML è di solito usato per supportare la fase di design e/o documentazione delle applicazioni software. Inoltre, l'ausilio dell'UML consente di specificare le proprietà della privacy con differenti livelli di astrazione.

Un concetto chiave nella soluzione proposta è quello di predisporre un controllo di accesso basato sul ruolo che definisca, in modo chiaro ed inequivocabile, le azioni che ciascun attore può svolgere in uno specifico contesto.

L'attività di ricerca condotta ha, inoltre, approfondito due requisiti fondamentali per la privacy, il consenso informato e la garanzia di anonimato, proponendo dei *design patterns* basati sul modello concettuale in UML.

I *design patterns* proposti possono essere utilizzati in differenti domini applicativi.

La soluzione ipotizzata, così articolata, è stata presentata in [C5][C7][C9][C14][R27]. Il modello è stato applicato ad un sistema informativo ospedaliero *open source*, Care2x [C7]. Sabrina Sicari è stata inoltre autore su invito di una pagina *Sci-Topics*, dal titolo "*Modeling Privacy Policies*" [R27]. Tale soluzione è stata presentata fra altro nel capitolo avente per titolo "*Privacy aware systems:from models to patterns*" del libro "*Software Engineering for Secure Systems: Industrial and Research Perspectives"* [CH1]. Infine la definizione e modellazione di politiche di privacy e dei relativi protocolli ha trovato applicazione anche nel dominio agro-alimentare nell'ambito del progetto MoseforAgrofood. I risultati ottenuti sono stati presentati in [C20].

Tali ricerche, iniziate nel maggio del 2006, sono oggetto attuale dell'interesse di Sabrina Sicari e segnano l'inizio dell'attività svolta nell'ambito dell'assegno di ricerca dal titolo *"Sicurezza Protocollare in Architetture Informatiche e di Telecomunicazione"*.

- **Area: Reti di Sensori Wireless**

Le recenti novità tecnologiche sia delle comunicazioni *wireless* che dell'elettronica, hanno portato allo sviluppo di reti di sensori *wireless* (*Wireless Sensor Networks*- WSN). Le WSN sono composte da sensori interconnessi mediante una rete di comunicazione *wireless*, in grado di acquisire, elaborare e trasmettere dati verso la *sink*. I domini applicativi delle WSN sono molteplici ed in continua evoluzione. Essi spaziano dai sistemi per la sorveglianza perimetrale al monitoraggio ed il controllo della viabilità urbana/extraurbana, al supporto ad operazioni militari e/o antiterrorismo, telemedicina, assistenza di persone diversamente abili e anziani, monitoraggio ambientale, localizzazione sicura di servizi ed utenti, e controllo in ambito di processi industriali.

Tuttavia, per consentire la diffusione pervasiva di una così vasta ed articolata offerta di servizi innovativi, è necessario il soddisfacimento di requisiti stringenti in termini di sicurezza e privacy, posti dalla maggior parte delle applicazioni citate precedentemente, tenendo presente i vincoli dovuti al contesto tecnologico in cui si opera, cioè la limitata disponibilità di risorse energetiche, di calcolo, di archiviazione, e di banda dei nodi-sensore.

I requisiti sulla sicurezza sono particolarmente critici, poiché la natura *wireless* del collegamento fra i vari nodi-sensore, determina un aumento delle vulnerabilità e, quindi, delle conseguenti minacce all'integrità e alla confidenzialità dei dati trasmessi.

La ricerca sulle reti WSN sicure è rivolta alla formulazione e definizione di soluzioni adatte a garantire, in funzione del contesto applicativo, un adeguato soddisfacimento dei requisisti di sicurezza, privacy e qualità del dato trasmesso, ottimizzando (al tempo stesso) il consumo energetico. L'obiettivo di quest'attività di ricerca è vasto e si articola nei seguenti punti: definizione di soluzioni finalizzate a garantire la privacy nelle reti WSN, basate su modelli definiti in UML; definizione e simulazione di metodologie *cross layer* aventi lo scopo di valutare la qualità del dato aggregato, alla luce di informazioni di *routing* e di localizzazione; definizione di architetture ibride (*wireless mesh network* e *wireless sensor network)* in grado di garantire la sicurezza del dato, tenendo conto delle limitate risorse energetiche; definizione di algoritmi di localizzazione a basso consumo di potenza per reti di sensori subacquee; analisi di reti di sensori multimediali sicure; analisi del comportamento di nodi "malevoli" mediante l'ausilio della teoria dei giochi e valutazione della reputazione dei nodi con l'ausilio di tecniche di *machine learning*. Di seguito maggiori dettagli sulle ricerche scaturite dall'analisi delle reti di sensori, i cui risultati sono stati presentati nei lavori [C6][C10][C11][C12][C13][C14][C15][C16][C17][C18][C19][C21][C24][C26][R8][R9][R10] [R13][R14][R16][R21][R24][R30][B1][B2]. Tale attività di ricerca iniziata nel 2007 prosegue ad oggi.

Sottoarea: Metodologie Cross Layer per la Valutazione della Qualità del Dato[C11][C13][C19][R10]

Le WSN hanno avuto una rapida diffusione nell'ultimo decennio e sono state utilizzate in vari domini applicativi. I vari servizi che utilizzano le WSN come rete di comunicazione richiedono un grande ammontare di dati. Pertanto, allo scopo di fornire dei servizi ottimali è necessario garantire una buona qualità del dato, tuttavia talvolta tale obiettivo non viene raggiunto a causa di attacchi finalizzati a violare la sicurezza della rete. Oltre ad adottare opportuni algoritmi che criptino il dato trasmesso, è necessario valutare l'affidabilità dei nodi che rilevano, aggregano e trasmettono il dato.

L'obiettivo di questa ricerca, svolta in collaborazione con l'Università Statale di Milano, è quindi di definire una metodologia che individui le fasi fondamentali per una corretta valutazione del dato aggregato. La metodologia definita ha adottato un approccio *cross layer*, utilizzando, per l'analisi della qualità del dato, le informazioni sull'affidabilità, in termini di sicurezza, dei nodi attraversati. Il criterio, utilizzato da Sabrina Sicari, per valutare il livello di sicurezza dei nodi si basa sulle informazioni di localizzazione relative ai nodi stessi. In particolare è oggetto di valutazione la "robustezza" delle informazioni di localizzazione. Infatti, la sicurezza nelle WSN è un problema

complesso ed articolato riguardante anche la sicurezza e robustezza degli algoritmi di localizzazione dei nodi. Alla luce della natura distribuita delle reti WSN, in parecchi scenari applicativi la localizzazione dei sensori è "*conditio sine qua non"* per l'erogazione del servizio. L'affidabilità e la riservatezza delle informazioni di localizzazione è di fondamentale importanza e, quindi, è necessario valutarla mediante algoritmi *ad hoc.*

La metodologia proposta si basa sull'uso congiunto di algoritmi di aggregazione sicura *end-to-end* e di algoritmi di verifica della robustezza delle informazioni di localizzazione. Inoltre le informazioni di *routing* sono utilizzate per tener traccia dei nodi attraversati. I risultati ottenuti sono stati presentati in [C11][C13][C19][R10].

Sottoarea: Soluzioni per Garantire la Privacy nelle WSN [C14][C17][R9][R13][R14][B1][B2]

I dati trattati nelle WSN devono essere protetti per garantirne la privacy in quanto possono direttamente o indirettamente rilevare informazioni sensibili degli individui. Il problema di prevenire l'identificazione di un individuo a partire dai propri dati, detto anonimato, è un requisito fondamentale per tutti i sistemi *privacy aware* e quindi, anche per le WSN.

La soluzione trovata in risposta a questa specifica attività di ricerca garantisce l'anonimato nelle WSN mediante la definizione di opportune politiche di privacy. L'approccio, proposto da Sabrina Sicari, si basa su un modello sviluppato in UML che introduce tutti i concetti base (nodo, azione, dato, titolare dei dati, responsabile del trattamento ecc.) e le linee guida necessarie a garantire la privacy nelle reti *wireless* di sensori. Le politiche di privacy sono rappresentate mediante messaggi scambiati fra i nodi e azioni eseguite dai nodi stessi in conformità a protocolli di comunicazione opportunamente definiti.

I risultati ottenuti per questa attività di ricerca sono stati presentati in [C14][C17][R9][R13][R14][B1][B2].

Sottoarea: Architetture Ibride-Mesh Networks e Wireless Sensor Networks [C12][C18][C21][R14]

L'attività di ricerca che la comunità internazionale ha condotto sulle reti di sensori *wireless* è stata sempre condizionata dai limiti in termini di potenza dei nodi-sensore. I nodi-sensore sono infatti dispositivi di piccole dimensioni con limitate risorse in termini di potenza, memoria, capacità di elaborazione. Un obiettivo sempre aperto è la definizione di soluzioni sicure e a basso consumo di potenza. Gli algoritmi di aggregazione dei dati, ampiamente studiati dalla comunità scientifica internazionale, limitano il consumo di potenza riducendo la quantità di dati trasmessi. Tuttavia, per

garantire la diffusione delle WSN nella vita reale occorre soddisfare alcuni requisiti di sicurezza e, qualunque soluzione di tal tipo richiede un investimento in termini di risorse energetiche che, come detto più volte, sono limitate nelle reti *wireless* di sensori. Per superare questo limite, la soluzione proposta da Sabrina Sicari, in collaborazione con il centro di ricerca Create-net di Trento, prevede la definizione di un'architettura ibrida composta da *wireless mesh network* e *wireless sensor networks*. In particolare, i sensori utilizzeranno la propria potenza per rilevare i dati e per criptarli; mentre i *mesh routers* saranno utilizzati per aggregare i dati e trasmetterli verso la *sink*, realizzando in tal modo una suddivisione dei *tasks* e un consequenziale risparmio energetico. Nell'architettura proposta i nodi-sensore sono organizzati in *clusters* e i *mesh routers* svolgono la funzione di *cluster heads*. L'architettura proposta risulta flessibile e scalabile, e particolarmente adatta a realizzare applicazioni nelle quali la *mesh* network fornisce un *backhaul* per supportare contemporaneamente differenti WSNs, assicurando al tempo stesso criptazione e autenticazione *hop-to-hop*.
La performance dell'architettura proposta è stata anche valutata mediante l'utilizzo di un prototipo, sviluppato *ad hoc*. I risultati ottenuti sono stati presentati in [C12][C18][C21][R14].

Sottoarea: Algoritmi di Localizzazione a Basso Consumo di Potenza Subacquei [C6]

Le reti di sensori *wireless* subacquee (*Underwater Wireless Sensor Network*, UWSN) hanno differenti campi di applicazione: dal monitoraggio delle acque; alla prevenzione dei disastri; all'assistenza alla navigazione. Per poter usufruire dei suddetti servizi è necessario sviluppare una adeguata rete di comunicazione subacquea. In particolare, è fondamentale che i sensori vengano localizzati accuratamente all'interno di una rete subacquea. Sebbene molti protocolli di localizzazione di sensori *wireless* terrestri siano stati proposti, le differenti caratteristiche dell'ambiente subacqueo e del mezzo di comunicazione adottato (onde acustiche e non onde RF, utilizzate in ambito terrestre) determinano la necessità di definire nuovi protocolli di localizzazione: obiettivo dell'attività di ricerca di Sabrina Sicari. Le onde acustiche, infatti, introducono problemi quali alti ritardi di trasmissione, *multipath* e elevati errori in trasmissione. L'algoritmo di localizzazione, definito da Sabrina Sicari, riduce il consumo di potenza mediante la riduzione del numero di messaggi scambiati fra i nodi e l'assenza di sincronizzazione fra i nodi stessi. L'algoritmo può essere applicato in reti di grandi dimensioni. L'approccio proposto differenzia il comportamento dei nodi in funzione del livello di potenza residuo a disposizione di ciascun sensore, distinguendo quattro principali stati dei nodi stessi in funzione di potenza e informazioni di localizzazione.

L'algoritmo presenta una buona performance sia in termini di consumo di potenza che di capacità di localizzazione, ossia di numero di nodi in grado di calcolare la propria posizione. I risultati ottenuti sono stati presentati in [C6].

Sottoarea: Reti di Sensori Wireless Multimediali Sicure [C10][R8][R24]

La disponibilità sempre crescente di hardware a basso costo per l'acquisizione di contenuti multimediali (quali videocamere e microfoni in tecnologia CMOS) e di sistemi di comunicazione *wireless* (come IEEE 802.11 e 802.15) ha reso possibile lo sviluppo di reti *wireless* di sensori multimediali (*Wireless Multimedia Sensor Networks, WMSN*). La tecnologia CMOS, infatti, consente di integrare in un unico dispositivo una lente, un sensore per immagini e la logica necessaria per l'esecuzione di algoritmi di elaborazione digitale dei segnali, quali quelli per la stabilizzazione e la compressione delle immagini. Tale dispositivo di acquisizione può essere interfacciato (es. con moduli Cyclops) con sensori *wireless* già disponibili sul mercato (es., Crossbow, MICA2 o MICAz) producendo, come risultato, un sensore multimediale, dotato sia di funzionalità di acquisizione e processing delle immagini, sia di interfaccia di comunicazione, che di moduli di memorizzazione ed unità di alimentazione e controllo. Altri esempi di semplici sensori multimediali sviluppati recentemente sono: Imote; Imote2 e Stargate.

I requisiti posti dalle applicazioni di monitoraggio multimediale, tuttavia, pongono nuove problematiche che l'infrastruttura di comunicazione *wireless* deve essere in grado di risolvere, soprattutto per assicurare la *Quality of Experience (QoE*) desiderata dall'utente. Esse sono legate alle limitate disponibilità energetiche e di calcolo dei sensori, alla complessità delle operazioni di compressione/aggregazione/elaborazione distribuita dei dati, al sovraccarico per la gestione delle politiche di sicurezza, alla qualità del servizio (*Quality of Service, QoS*). I limiti in termini di capacità di calcolo, di memoria e di risorse energetiche, imposti dalle *wireless sensor networks,* diventano ancor più critici nel contesto multimediale delle WMSN, in cui si attuano anche politiche per la gestione della sicurezza e della privacy, in combinazione con schemi di compressione ed elaborazione distribuiti dei contenuti multimediali. Di conseguenza, l'ambito delle WMSN è un campo di ricerca che richiede strumenti e metodologie di progetto nuovi rispetto a quelli già proposti dalla comunità scientifica per le WSN. Il carattere innovativo di questo campo di ricerca viene ulteriormente esaltato dai recenti sviluppi tecnologici nel settore delle nanotecnologie, in grado di incrementare, notevolmente, le potenzialità dei nodi-sensore

L’obiettivo di questa attività, svolta in collaborazione con il Politecnico di Bari, ha per oggetto la definizione ed implementazione di una piattaforma integrata per lo sviluppo di reti WMSN sicure con particolare attenzione verso soluzioni che garantiscano allo stesso tempo: (1) compressione sicura e distribuita dei dati; (2) aggregazione dei dati compressi con tecniche di *in-network processing*; (3) soddisfacimento dei requisisti di sicurezza e privacy; (4) comunicazione in tempo-reale; (5) efficienza energetica. I primi risultati ottenuti sono stati presentati in [C10][R8] e ulteriori risultati sono attualmente oggetto di un prossimo articolo a rivista [R24].

Sottoarea: Wireless Sensor Networks Sicure mediante Analisi Condotte con l'Ausilio della Teoria dei Giochi [C15][C16][R16]

Molte applicazioni delle reti *wireless* di sensore (WSN) sono strettamente legate alle posizioni dei nodi sensore, che non sono necessariamente note a priori. Molti approcci sono stati proposti e alcuni omettono di considerare che le WSN potrebbero trovarsi in luoghi ostili, dove nodi "malevoli" potrebbero, sotto il controllo di un attaccante, coesistere con nodi affidabili. La *Verifiable Multilateration* (VM) propone di risolvere questo problema utilizzando dei nodi àncora, la cui posizione è ben nota, che giochino il ruolo di verificatori. Sebbene la VM sia in grado di valutare l’affidabilità di misure che indicano la posizione dei nodi, esiste circa un 40% della regione monitorata sulla quale non si hanno informazioni sufficienti. E' quindi arduo stabilire la sicurezza delle stesse informazioni di localizzazione e rilevare eventuali comportamenti "malevoli". L’obiettivo di quest’attività, svolta in collaborazione con il Politecnico di Milano e l’Università statale di Milano, è analizzare la robustezza della *Verifiable Multilateration* mediante l’utilizzo della teoria dei giochi. In particolare, VM è stata analizzata utilizzando un gioco non cooperativo con due giocatori. Il primo giocatore rappresenta i verificatori che adottano la VM e vogliono individuare i nodi "malevoli", e il secondo giocatore rappresenta l’attaccante "malevolo" che vuole mascherarsi, pretendendo di essere in una posizione diversa da quella reale.

Grazie all’utilizzo della teoria dei giochi sono state studiate e analizzate tutte le potenzialità della VM con lo scopo di migliorare la strategia del difensore. Fra i vari risultati conseguiti è stata infatti individuata la migliore posizione dei verificatori ed è stato definito un approccio probabilistico per valutare la reputazione dei nodi. Inoltre, è stato studiato il comportamento dei nodi "malevoli" nel

caso in cui ci fossero tre soli verificatori e, successivamente, in presenza di un numero arbitrario degli stessi. Infine, sono stati modellati i cambiamenti nella strategia del nodo malevolo, provando ad individuare le migliore strategia da seguire. I risultati di questa attività sono stati presentati in [C15][C16][R16].

Sottoarea: Valutazione delle reputazione dei nodi di Wireless Sensor Networks Sicure mediante Tecniche di Machine Learning [C24][R30]

La capacità di identificare i nodi "malevoli" rappresenta, a tutt'oggi, una problematica aperta per le reti di sensori *wireless* e diventa particolarmente rilevante per servizi che coinvolgono dati sensibili (es. applicazioni mediche, sistemi di allarme, etc.).

L'obiettivo di questa ricerca è stato definire un metodo, detto *GoNe (Good Network)*, capace di garantire sicurezza e privacy dei dati mediante l'ausilio di tecniche di *machine learning* basate su *Self Organizing Maps (SOM). GoNe* fornisce una valutazione dinamica della reputazione dei nodi e, quindi, della loro affidabilità in presenza di differenti tipi di attacchi, consentendo di classificare il comportamento degli stessi.

I risultati di tale attività svolta in collaborazione con il Politecnico di Bari sono stati presentati in [C24][R30].

Sottoarea: Confronto di simulatori per valutare e validare protocolli proposti per le WSN [R21] [C26]

Negli ultimi anni, il crescente interesse per le applicazioni che utilizzano le WSN ha portato all'introduzione di nuovi metodi di modellazione e ambienti di simulazione, volti a consentire una valutazione e una validazione dei protocolli e degli algoritmi di routing proposti per le WSN stesse, prima della loro effettiva messa in opera in scenari reali. Tali simulatori mettono a disposizione diversi livelli di astrazione dei vari componenti della rete, a partire da caratteristiche di basso livello fino a tool per il calcolo dei consumi energetici. Al fine di testarne le funzionalità, sono stati confrontati, in particolare: Castalia, Mixim, WSNet, PASES, Cooja, TOSSIM. Essi sono stati valutati

all’interno di diversi scenari di riferimento, composti da un diverso numero di nodi. Le metriche in base alle quali sono state condotte le valutazioni sono le seguenti: durata della simulazione, throughput, modellazione del canale di comunicazione, frequenza di ricezione dei pacchetti, latenza e stima dell’accuratezza del calcolo dei consumi. Tali confronti sono stati, anche, eseguiti rispetto a un prototipo reale ed estesi a uno scenario di riferimento che fa uso del protocollo AODV.
I risultati di tale attività, svolta in collaborazione con l’Università di Trento, sono stati presentati in [R21] e [C26].

- **AREA: Internet of Things**

Nell'epoca attuale, centinaia di migliaia di persone nel mondo usano Internet per svariate applicazioni: *web browsing*; invio/ricezione di mail; *download* di contenuti multimediali; utilizzo di *social networks*. Accanto al crescente numero di utenti che accede ad Internet, come infrastruttura per la condivisione di informazioni a livello globale, si assiste alla diffusione di oggetti "intelligenti" (*smart objects*) e capaci di comunicare. E’ prevedibile che nel prossimo decennio contenuti e servizi siano sempre disponibili, aprendo la strada a nuove applicazioni e a un nuovo modo di lavorare e di vivere. In tale prospettiva, il tradizionale concetto di Internet lascerà spazio alla nozione di oggetti intelligenti interconnessi, che sta alla base del paradigma di *Internet of Things* (IoT). Tale innovazione sarà raggiunta introducendo l'elettronica negli oggetti reali (quotidiani) rendendoli quindi, intelligenti. Pertanto, il termine *Internet of Things* è largamente utilizzato per indicare: la rete globale che interconnette gli oggetti intelligenti; l’insieme di tecnologie che supportano tale visione, inclusi RFID, sensori/attuatori etc.; e l’insieme di nuove applicazioni e servizi che aprono nuove opportunità di business. Nel contesto di *Internet of Things* mondo fisico e virtuale si uniscono, garantendo all’utente di essere "*connesso sempre, in ogni luogo, con qualunque oggetto"*.
In tale ambito, la garanzia della sicurezza e della privacy delle informazioni rappresenta un requisito critico ma al tempo stesso fondamentale, al fine di consentire la reale diffusione del paradigma di *Internet of Things*. Tuttavia, le tradizionali contromisure di sicurezza non possono essere applicate a IoT per svariate ragioni (es. limitate risorse energetiche, scalabilità, interoperabilità, etc.). Alla luce di questa riflessione, l’attività di ricerca di Sabrina Sicari è incentrata proprio sulle relative problematiche di sicurezza e privacy ed è stata così articolata: è stato condotto uno studio e una revisione critica dei principali scenari applicativi, delle tecnologie e dei principali obiettivi di ricerca

da perseguire, al fine di rendere IoT una realtà. I risultati di queste ricerche sono stati pubblicati in [R11][R15][R18][R26][B3]. Inoltre, sono state condotte due ricerche più specifiche riguardanti i requisiti di sicurezza e privacy nei database NoSQL e nei protocolli di comunicazione maggiormente utilizzati nelle architetture basate sul paradigma di Internet of Things. I risultati di queste analisi sono stati pubblicati in [R47] e sono in fase di revisione in [R49].

Posto che da un'analisi attenta delle evoluzioni tecnologiche si è appurata una sinergia tra il rivoluzionario approccio di *Internet of Things* e la costante diffusione di robots in molte attività quotidiane, si è ritenuta la visione di *IoT-aided robotics applications* come una realtà possibile. Infatti, nuovi servizi avanzati si baseranno sempre di più sulla interazione fra robots e oggetti, per assistere l'uomo nei suoi bisogni quotidiani. L'attività di ricerca in quest'ambito è stata articolata in due fasi. Innanzitutto è stato condotto un attento studio sullo stato dell'arte in ordine alle principali tematiche connesse a *IoT-aided robotics services*, ossia comunicazione, applicazioni robotiche in *pervasive environments*, approcci basati sulla semantica per acquisire il consenso, problematiche di sicurezza, privacy e trust. Successivamente, alla luce dello studio condotto, sono stati messi in luce i principali obiettivi delle future ricerche. Infatti, a fronte della consapevolezza delle elevate potenzialità di tali applicazioni, la strada da percorrere per la loro reale e concreta diffusione richiede che molti relativi problemi tecnici aperti trovino una soluzione. I risultati di questi studi sono presentati in [R17].

Infine, alla luce dell'attenta analisi dello stato dell'arte condotta su IoT, la ricerca di Sabrina Sicari e del suo gruppo si è focalizzata sulla definizione di: un'architettura di riferimento; un modello di riferimento in UML in grado di rappresentare tutte le entità coinvolte e le reciproche relazioni; politiche di *enforcement*; un algoritmo *ad hoc* per la valutazione dei dati provenienti da sorgenti differenti in termini di requisiti di sicurezza, privacy e qualità; un prototipo dell'architettura e alcune soluzioni atte a garantire sicurezza in *Open source M2M project* (OM2M). Di seguito maggiori dettagli sulle ricerche scaturite, i cui risultati sono stati presentati nei lavori [C22][C23][C25][R19][R20][R22][R23][R28][R29][R32][R33][R34][R35][R36][R37][R38][R39][R40][R41][R42][R43][R44][R45][R46][R48][R50][CH1]. La Prof.ssa Sicari lavora attualmente su queste tematiche.

Sottoarea: NOS-Architettura di riferimento [C25][R19][R20]

Internet of Things (IoT) implica la gestione di un enorme ammontare di dati eterogenei che devono soddisfare innanzitutto un requisito di affidabilità al fine di rendere robusti i servizi erogati. Infatti,

accanto ai requisiti di sicurezza e privacy, i sistemi IoT richiedono una garanzia di qualità del dato per fornire accurate informazioni. Si noti, ad esempio che in alcuni scenari, errori o dati mancanti possono avere un impatto critico sulle azioni da intraprendere e sulle decisioni da prendere. In tale prospettiva, l'attività di ricerca è stata rivolta alla definizione di una nuova architettura a livelli, chiamata *NOS (NetwOrked Smart object)* in grado di garantire sicurezza e qualità dei dati, in base alle esigenze dell'utente, fornendo quindi dei servizi *customizzati*.

Infatti, i dati provenienti da sorgenti eterogenee (es. RFID, sensori, *social networks*, etc.), definite *E-Nodes*, sono raccolti dai *NOS* costituiti da tre livelli: *Analysis, Data Annotation e Integration*. I livelli *Analysis* e *Data Annotation* eseguono un insieme di azioni allo scopo di fornire in *output* una rappresentazione normalizzata dei dati acquisisti, definiti *IoT data*, a partire da dati eterogenei. Si noti che *IoT data* soddisfano specifici requisiti sintattici e contengono una descrizione semantica indipendentemente dalla sorgente di origine. In particolare, il livello *Analysis* è responsabile di valutare il livello di sicurezza e privacy dei dati (es.integrità, confidenzialità, autenticazione e anonimato) e la qualità dei dati stessi (es. accuratezza, provenienza, reputazione della sorgente). Si noti che per, quanto concerne la sicurezza, è stato sviluppato da Sabrina Sicari e dal suo gruppo un nuovo algoritmo, in grado di valutare automaticamente i relativi requisiti, nonché quelli di privacy dei dati provenienti da sorgenti eterogenee [R20].

Il livello *Data Annotation* ha il compito di rappresentare le informazioni ottenute dal livello *Analysis* seguendo delle specifiche regole sintattiche e includendo una descrizione semantica del contenuto dei dati; in altre parole i dati saranno annotati con dei metadati (es. valutazione numerica di ciascun requisito di sicurezza, privacy e qualità dei dati).

I dati così normalizzati possono essere integrati allo scopo di soddisfare le specifiche richieste dell'utente; queste operazioni sono eseguite dal livello *Integration*. Si noti che l'integrazione valuta i requisiti dell'utente in termini di sicurezza, privacy e qualità dei dati al fine di selezionare quelli che meglio soddisfino i bisogni del cliente nei differenti scenari applicativi. Infatti, i servizi agli utenti attualmente forniscono dei dati, senza spesso considerare il livello di sicurezza, privacy e qualità richiesti dallo specifico dominio.

Riassumendo NOS fornisce: un'interfaccia verso sorgenti eterogenee per la raccolta di dati; una valutazione della sicurezza e della qualità dei dati; informazioni all'utente in un formato standard.

I risultati di tale attività, svolta in collaborazione con il Politecnico di Milano e il centro di ricerca Create-net, sono stati presentati in [R19]. Infine, la performance di tale *middleware* è stata testata mediante un prototipo sviluppato *ad hoc* [C25][R20]. Nel prototipo i vari livelli che compongono

NOS comunicano mediante servizi *RESTful*; mentre NOS è sviluppato su *RaspberryPi*. I dati da analizzare vengono ricavati in tempo reale da *open data streams* disponibili sul web e vengono resi disponibili ai servizi interessati tramite il protocollo *publish/subscribe MQTT* [R22]. L'implementazione dei moduli che compongono NOS è realizzata mediante la piattaforma *Node.JS* e il database non relazionale *MongoDB*, che consente un'evoluzione dinamica del modello dei dati.

Sottoarea: Dal Modello alle Politiche di Enforcement [C22][R23][R28][R29]

Nel contesto eterogeneo di IoT è fondamentale fornire un modello ben definito, adatto per tutte le applicazioni e le architetture di IoTe capace di garantire un certo livello di privacy e qualità dei dati, sin dalle prime fasi della relativa progettazione, specificandone sia le entità coinvolte (es. utenti, servizi, tecnologie, *IoTPlatform*) che le reciproche relazioni. Infatti, dall'analisi della precedente letteratura emergeva come non fossero disponibili soluzioni per *Internet of Things* capaci di gestire, contemporaneamente, i requisiti di sicurezza e qualità del dato, come invece è in grado di fare il modello definito da Sabrina Sicari e dal suo gruppo.

Il modello generale proposto, sviluppato in UML, infatti, descrive e analizza i requisiti di sicurezza, privacy e qualità del dato affrontati ad ogni livello dell'architettura NOS, al fine di sviluppare servizi *privacy aware,* usando dati con un certo livello di qualità. I risultati di tale attività, svolta in collaborazione con il Politecnico di Milano, sono stati presentati in [C22].

Il modello in questione rappresenta il punto di partenza per lo sviluppo di servizi sicuri caratterizzati da un certo livello di qualità dei dati. Per gestire eventuali violazioni delle politiche è necessario, infatti, definire dei nuovi meccanismi di *enforcement*,validi per il contesto di *Internet of Things*.

L'obiettivo di queste ricerche è stato la definizione di un insieme di politiche flessibili di *enforcement*, capaci di garantire sicurezza e qualità,anche in caso di tentativi di violazione, nel dominio altamente dinamico di IoT, caratterizzato da un numero elevato di dispositivi interconnessi. L'adozione delle suddette politiche garantirà un alto grado di robustezza del sistema. Si noti che per gestire le interazioni fra le entità coinvolte e i conflitti di politiche *cross domain*, è stato definito un linguaggio sfruttando le potenzialità di XML. Tali politiche sono state integrate nel prototipo dell' architettura NOS, usando JSON.

I risultati di tale attività di ricerca, svolta in collaborazione con il Politecnico di Bari, il Politecnico di Milano e il centro di ricerca Create-net, sono stati presentati in [R29][R28][R23].

Sottoarea: Analisi del rischio e gestione degli attacchi [R12] [R13]

Sia i produttori che i consumatori dei dati all'interno di un sistema IoT dovrebbero essere consapevoli dei rischi e delle potenziali minacce in cui le informazioni trasmesse possono incorrere. Non è sufficiente monitorare il comportamento delle sorgenti dei dati e delle entità che accedono alle risorse della rete IoT, ma è necessario condurre anche un'analisi dei rischi relativi all'infrastruttura IoT che si occupa dell'acquisizione, dell'elaborazione e della condivisione dei dati. Infatti, una maggiore affidabilità delle piattaforme IoT porterebbe ad una loro più rapida e crescente diffusione. A tal fine, è stata proposta una metodologia general-purpose in grado di svolgere una procedura di risk assessment all'interno di un sistema IoT. Tale soluzione tiene in considerazione sia parametri statici che dinamici della rete IoT, per tutto il ciclo di vita compiuto dai dati. In questo modo è possibile rivelare eventuali criticità e definire opportune contromisure. I risultati di questo lavoro, svolti in collaborazione con U-hopper, sono stati pubblicati in [R13].

Fra gli attacchi più frequenti e difficili da riconoscere all'interno di una rete IoT vi è il Denial of Service (DoS). Esso mira ad 'esaurire' le risorse della rete IoT fino a comprometterne il funzionamento. Tale tipo di attacco è ancora più grave quando colpisce non solo le sorgenti dei dati, ma la piattaforma IoT stessa. Al fine di riconoscere e fronteggiare attacchi DoS viene proposta una tecnica, denominata REATO, integrata all'interno della piattaforma NOS. La performance di tale soluzione è stata valutata mediante un apposito test-bed, in termini di: carico computazionale, latenza, tempo impiegato per riconoscere e fronteggiare l'attacco. I risultati di questo lavoro, svolti in collaborazione con U-hopper, sono stati pubblicati in [R12].

Sottoarea: Scenari applicativi [C29] [R33] [R36] [R37] [R41] [R45] [R46] [R48]

Il paradigma IoT trova applicazione in diversi scenari, tra cui: smart building, smart health, smart agriculture, smart transport, smart logistics, ambienti militari, e così via. Alla luce delle soluzioni security e privacy-aware presentate fino ad ora, Sabrina Sicari ha sviluppato alcuni casi di studio, per analizzare ulteriormente l'impatto delle tecniche e delle metodologie proposte all'interno di scenari IoT reali. In particolare, in collaborazione con il Politecnico di Bari, è stato messo in opera un test-bed reale all'interno di uno smart building. L'obiettivo principale di tale lavoro è la possibilità di: (i) acquisire dati sia scalari che multimediali da sorgenti eterogenee; (ii) condividere le informazioni elaborate tramite un'interfaccia comune; (iii) applicare i meccanismi di enforcement delle politiche di sicurezza e privacy. La piattaforma IoT è costituita da NOS integrata con TLSensing; garantire

l'interoperabilità tra queste due tecnologie è stato un ulteriore obiettivo della collaborazione, i cui risultati sono pubblicati in [C29].

Strettamente legato al caso di studio di una smart home è il lavoro pubblicato in [R33], nel quale il data-set, contenente i dati relativi ai consumi reali di un certo numero di case domotiche, è utilizzato per testare ulteriormente le performance della piattaforma NOS, a cui è applicato l'utilizzo delle sticky policies.

Infine, il tool Node-RED, sviluppato per coadiuvare gli sviluppatori nella progettazione di sistemi IoT, è stato utilizzato per definire uno scenario in ambito smart transport e smart logistics, nonché per modellare una soluzione security-aware per garantire l'autenticità dei prodotti appartenenti al settore dell'occhialeria. Diverse sono le tecnologie coinvolte, che vengono emulate all'interno della piattaforma, tra cui: RFID, comunicazioni tramite protocollo MQTT, MongoDB, Java. I risultati sono pubblicati in [R36] [R41].

La performance di Node-RED è stata inoltre testata in altri quattro casi d'uso in ambito, rispettivamente, smart retail, smart parking, smart home e smart health, dimostrando l'efficacia di questo tool nel rappresentare il comportamento, le interazioni e le performance di questi scenari eterogenei. Ulteriori scenari analizzati riguardano ambienti indoor e outdoor. I risultati sono stati pubblicati in [R37] e [R45], mentre sono in fase di revisione i risultati presentati in [R48]. Inoltre, il medesimo tool ha permesso di progettare un sistema di gestione remota della quarantena per i casi di COVID-19. Il lavoro è stato pubblicato in [R46].

Sottoarea: Open Source Machine to Machine (OM2M) [C23]

Machine-to-Machine (M2M) è un concetto dominante nel panorama di *Internet of Things*, che promette di interconnettere milioni di dispositivi nel prossimo futuro. Tuttavia, M2M soffre di un'elevata frammentazione del mercato e della mancanza di standards. Per colmare tale vuoto, l'European Telecommunication Standards Istitute (ETSI) ha rilasciato un insieme di specifiche per lo sviluppo di una comune piattaforma di servizi M2M. In tale prospettiva, si colloca *Open source M2M project* (OM2M), una piattaforma di servizi conforme alle indicazioni di ETSI, che fornisce delle *RESTful API* per migliorare l'interoperabilità fra sistemi. Si tratta di un'architettura modulare, sviluppata sopra il livello OSGi, estendibile mediante opportuni *plugins* che supporta parecchi protocolli e tecnologie.

Tuttavia, OM2M, attualmente, affronta solo marginalmente le problematiche di sicurezza. Obiettivo di questa attività di ricerca è dunque definire una soluzione in grado di gestire opportunamente le

politiche di sicurezza e privacy. A tale scopo è stata definita una nuova entità, chiamata *Resources_Security*, che fornisce un'interfaccia ad un nuovo *plugin* esterno, chiamato *Security_ Enforcement plugin* che conterrà le politiche di sicurezza e privacy e i relativi meccanismi di *enforcement*.

Questa attività di ricerca, in fase iniziale, è svolta in collaborazione con il Politecnico di Bari e il CNRS, LAAS dell'Università di Tolosa che è tra i principali sviluppatori di OM2M. I primi risultati sono stati pubblicati in [C23].

Sottoarea: Information Centric Networking (ICN) [C28]

Information Centric Networking (ICN) rappresenta un nuovo paradigma, emergente nell'ambito di Internet of Things, volto a fornire un'infrastruttura di rete basata sulla distribuzione delle informazioni sulla base del contenuto, superando in questo modo l'attuale approccio host-centric. I vantaggi consistono in una migliore gestione della mobilità dei devices, una maggiore scalabilità, una migliore gestione del caching dei contenuti, e una maggiore resistenza dell'intero sistema a guasti e tentativi di attacco. Le principali caratteristiche del paradigma ICN sono: (i) l'identificazione delle entità di rete (ad esempio, sorgenti di dati, contenuti, servizi, devices in generale) tramite un nome anziché tramite l'indirizzo IP (che rappresenta a tutti gli effetti una "posizione" all'interno della rete); (ii) un sistema di routing basato sia sui nomi che sugli indirizzi.

Per quanto riguarda la sicurezza e la privacy, poche soluzioni erano in grado di affrontare tali problematiche all'interno del contesto ICN, a maggior ragione se questo tipo di infrastruttura fosse inserita all'interno di un ambiente IoT. Per questi motivi, l'attività di ricerca è stata rivolta alla definizione di un modello architetturale sicuro in un contesto ibrido ICN-IoT, all'interno delle iniziative dell'Information Centric Networking Research Group (ICNRG) e dell'Internet Research Task Force (IRTF). Le seguenti funzionalità sono state integrate con meccanismi di sicurezza volti a prevenire possibili tentativi di violazione: "device and service discovery", "naming service", "content delivery". Questa attività di ricerca è stata svolta in collaborazione con il Politecnico di Bari. I risultati sono stati presentati e pubblicati in [C28].

Sottoarea: Fog computing e 5G [R43] [R42] [C30] [C31]

La crescente diffusione di tecnologie ed applicazioni legate all'ambito di IoT, conduce sempre di più alla presenza di dispositivi connessi su larga scala. Diversi protocolli e standard si trovano, dunque, a dover cooperare, al fine di gestire e trasmettere la grande quantità di dati forniti. Le problematiche

principali che emergono sono legate a scalabilità ed interoperabilità, nonché alla sicurezza ed alla privacy dei dati sensibili. Una soluzione a tali problematiche è rappresentata dal concetto di *fog computing*, che, grazie alla sua natura distribuita, si presenta come un'evoluzione del *cloud computing*. Su questo nuovo paradigma è stato, innanzitutto, condotto uno studio e una revisione critica delle soluzioni esistenti riguardanti, principalmente la sicurezza e la privacy. L'obiettivo è quello di mettere in luce le problematiche aperte e definire nuove attività di ricerca in quest'ambito. I risultati di quest'analisi sono in corso di revisione [R43].

I concetti del *fog computing* sono stati, inoltre, applicati in una rete IoT, composta da due *layer* distribuiti, formati, rispettivamente da una rete di NOSs e da una rete di *brokers*. L'obiettivo di tale infrastruttura è gestire in maniera efficiente sia l'acquisizione e il *processing* dei dati, che la condivisione delle informazioni con gli utenti finali. I risultati ottenuti sono pubblicati in [C30] e [C31].

Il concetto di pervasività delle reti mobili si sta concretizzando sempre di più grazie alla recente diffusione delle reti 5G, le quali promettono di rivoluzionare le comunicazioni wireless, fornendo servizi più veloci con ritardi molto bassi. Tuttavia, la diffusione della tecnologia 5G genera anche importanti problematiche in termini di sicurezza e privacy, legate all'affidabilità dei dispositivi connessi. Nel survey presentato in [R42] vengono discussi i seguenti requisiti: integrità, confidenzialità, autenticazione, controllo degli accessi, *trust*, *privacy*, applicazione delle politiche di accesso alle risorse e *intrusion detection*. Nell'analisi viene tenuto in considerazione il ruolo dei paradigmi emergenti, come IoT, fog *computing* e *blockchain*.

Sottoarea: Nano-tecnologie [R39] [R50]

Nuovi metodi di acquisizione, trasmissione e condivisione dei dati si stanno diffondendo, principalmente grazie alla miniaturizzazione e ai nuovi protocolli di comunicazione, incoraggiati dall'innovazione scientifica. In particolare, l'interesse per le nano-tecnologie sta crescendo, negli ultimi anni, in molti domini applicativi, come sanità, bio-medicina, settore agro-alimentare, attività industriali, scenari militari/difesa. I loro principali vantaggi sono la miniaturizzazione e la pervasività. Inoltre, possono essere interconnessi con le reti di comunicazione esistenti e, in ultima analisi, con Internet, aprendo così la strada ad un nuovo paradigma di comunicazione, denominato *Internet of Nano-Things (IoNT)*. Tale tipo di scenario implica la gestione di una grande mole di dati e, dunque, richiede di mettere in atto rigidi controlli sul flusso e sulla divulgazione di dati sensibili. Per gestire in modo efficiente l'enorme quantità di dati e renderli disponibili sottoforma di servizi per i

consumatori, è necessario creare una nuova architettura e dei metodi, in grado di affrontare problemi di scalabilità e interoperabilità. Tale innovazione porta una serie di sfide da affrontare, al fine di fornire un sistema efficiente, sicuro e affidabile. Infatti, la sicurezza e la privacy rappresentano requisiti critici anche nel contesto di *IoNT*. Le soluzioni tradizionali non sono adeguate rispetto a questo nuovo approccio, a causa della natura stessa delle entità coinvolte: le nano-tecnologie. Partendo da tali presupposti, è stata definita un'architettura in grado di fornire funzionalità di sicurezza all'interno di una nano-rete, grazie all'utilizzo di due tipi di comunicazione: onde elettromagnetiche e reazioni molecolari. Tale attività è stata svolta in collaborazione con il Politecnico di Bari, che ha messo a disposizione un proprio simulatore per nanotecnologie per sviluppare la soluzione proposta. I risultati sono stati pubblicati in [R39]. In corso di revisione, sempre seguendo questo filone di ricerca e di collaborazione, è in fase di revisione una soluzione di crittografia a livello di nano-sensori [R50].

8. Pubblicazioni

Si riporta l'elenco delle pubblicazioni di cui Sabrina Sicari è autore e/o coautore, suddivise per categoria. Il seguente prospetto riassume il numero di pubblicazioni per ciascuna categoria.

Categoria	Quantità
Articoli su riviste internazionali referate	46
Articoli su riviste internazionali non referate	2
Articoli su riviste nazionali non referate	1
Articoli in atti di conferenze internazionali	31
Capitoli di libri internazionali	2
Libri	3
Articoli in fase di revisione	4

8.1 Indicatori bibliometrici

Valori degli indicatori bibliometrici, numero di citazioni e indice di Hirsch riportati da alcune delle

principali fonti bibliometriche al 12 dicembre 2020.

Metrica	Google Scholar	Scopus
Citazioni	7810	4507
H-index	23	19

8.2 Riviste internazionali referate

- [R1] Andrea Calvagna, Aurelio La Corte, Sabrina Sicari "*Mobility and quality of service across heterogeneous wireless networks"*, in Computer Networks, Elsevier, Vol. 47- n.2, pag. 203-217, 2005
- [R2] Aurelio La Corte, Sabrina Sicari "*Quality of Service in Home network:VLANzeroconfiguration network*", in International Journal of Internet Protocol Technology, Inderscience Publishers, Vol.1- n.4, pag.228-235, 2006
- [R3] Aurelio La Corte, Sabrina Sicari *"Assessed Quality of Service and Voice and Data Integration: a Case Study",* in Computer Communications, Elsevier, Vol.29 n.11: pag.1992-2003, 2006
- [R4] Marco Benini, Sabrina Sicari "*Assessing the risk of intercepting VoIP calls",* in Computer Networks, Elsevier, Vol. 52 n.12: pag.2432-2446, 2008
- [R5] Marco Benini, Sabrina Sicari *"Risk Assessment in Practice: A Real Case Study",* in Computer Communications, Elsevier, Vol.31, n.15: pag. 3691-3699, 2008
- [R6] Marco Benini, Sabrina Sicari *"Risk Assessment via partial orders",*in Advanced in Computer Science and Engineering, Pushpa Publishing House, Vol.3 n.1: pag.19-46, 2009
- [R7]Marco Benini, Sabrina Sicari *"Mathematical Derivation of a Risk Assessment Procedure"* in International Journal of Applied Mathematics, Vol. 40 n.2: pag.52-62, 2010
- [R8] Luigi Afredo Grieco, Sabrina Sicari, Gennaro Boggia "*Open Issues in Secure Wireless Multimedia Sensor Networks"* in IEEE COMSOC MMTC E-Letter- Special Issue on Multimedia Over Embedded Systems-Vol.5, 2010

- [R9] Sabrina Sicari, George Roussos, Stephen Hailes "*Mobile Networks and Applications (MONET) Special Issue on Sensor Systems and Software"* (editorial) in ACM Mobile Networks and Applications Vol.16 n.2, 2011
- [R10] Alberto Coen-Porisini, Sabrina Sicari *"Improving data quality using a cross layer protocol in wireless sensor networks"* in Computer Networks, Elsevier, Vol. 57 n.16: pag.3655-3665, 2012
- [R11] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, Imirich Chlamtac *"Internet of things: Vision, applications and research challenges"* in AD HOC Networks, Elsevier, Vol.10 n.7: pag.1497-1516,2012
- [R12] Marco Benini, Sabrina Sicari "*Dealing with the security behaviour of large scale systems"*in Journal of Information Assurance and Security (JIAS), Vol.7 n.3:pag. 229-240, 2012
- [R13] Sabrina Sicari, Alfredo Grieco, Gennaro Boggia, Alberto Coen-Porisini "*DyDAP: A dynamic data aggregation scheme for privacy aware wireless sensor networks"* in The Journal of Systems & Software (JSS), Vol.85 n.1: pag.152-166, 2012
- [R14] Sabrina Sicari, Roberto Riggio, Alberto Coen-Porisini "*Dare:evaluating Data Accuracy using node REputation"*in Computer Networks, Elsevier,Vol.57 n.15:pag. 3098-3111, 2013
- [R15] Sabrina Sicari, Stephen Hailes, DamlaTurgut, Sanaa Sharaffedine, Udai Desai *"Security, Privacy and Trust Management in the Internet of Things era- SePriT"* in Ad Hoc networks, Elsevier,Vol.11 n.8: pag. 2623-2624, 2013
- [R16] Nicola Basilico, Nicola Gatti, MattiaMonga, Sabrina Sicari *"Security Games for Node Localization through Verifiable Multilateration"* in IEEE Transactions on Dependable and Secure Computing, IEEE,Vol.11 n.1:pag. 72-85, 2014

[R17] Luigi Alfredo Grieco, Alessandro Rizzo, Simona Colucci, Sabrina Sicari, Giuseppe Piro, Donato Di Paola, Gennaro Boggia "*IoT-aided robotics applications: Technological implications, target domains and open issues"*in Computer Communications, Elsevier, Vol. 54:pag.32-47, 2014

- [R18] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, Alberto Coen-Porisini: *"Security, privacy and trust in Internet of Things: The road ahead*" Computer Networks, Elsevier, Vol. 76: pag. 146-164, 2015
- [R19] Sabrina Sicari, Cinzia Cappiello, Daniele Miorandi, Francesco De Pellegrini, Alberto Coen-Porisini "*A security-and quality-aware system architecture for Internet of Things*" in Information Systems Frontiers (Springer), 58: 43-55, 2016
- [R20] Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, Cinzia Cappiello, Alberto Coen-Porisini:*"A secure and quality-aware prototypical architecture for the Internet of Things"* in Information Systems (Elsevier), 58: 43-55, 2016
- [R21] Ivan Minakov, Roberto Passerone, Alessandra Rizzardi, Sabrina Sicari: *"A Comparative Study of Recent Wireless Sensor Network Simulators"*, in ACM Transactions on Sensor Networks, ACM TOSN, 12 (3): 20:1-20:39 (2016)
- [R22] Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, Alberto Coen-Porisini: *"AUPS: an Open Source AUthenticated Publish/Subscribe system for the Internet of Things"*, in Information Systems (Elsevier), 62:29-41, 2016
- [R23] Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, Cinzia Cappiello, Alberto Coen-Porisini: *"Security Policy Enforcement for Networked Smart Objects"*, in Computer Networks (Elsevier), 108:133-147, 2016
- [R24] Michele Tortelli, Alessandra Rizzardi, Sabrina Sicari, Luigi Alfredo Grieco, Gennaro Boggia, Alberto Coen-Porisini: *"S²DCC: Secure Selective Dropping Congestion Control in hybrid wireless multimedia sensor networks"*, in Wireless Networks (Springer), 1-20, 2016
- [R28] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, Giuseppe Piro, Alberto Coen-Porisini: *Policy Enforcement Framework for Internet of Things Applications in the Smart Health*. Smart Health Journal (Elsevier) 3: 39-74 (2017)
- [R29] Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, Alberto Coen-Porisini: *Dynamic Policies in Internet of Things: Enforcement and Synchronization*. IEEE Internet of Things Journal: 4 (6): 2228-2238 (2017)
- [R30] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, Alberto Coen-Porisini: *Performance comparison of reputation assessment techniques based on self organizing maps in*

wireless sensor networks. Wireless Communications and Mobile Computing: vol. 2017, Article ID 7623742 (2017)

- [R31] Ivan Minakov, Roberto Passerone, Alessandra Rizzardi, Sabrina Sicari: *A Comparative Study of Recent Wireless Sensor Network Simulators*. ACM Transactions on Sensor Networks 12 (3): 20:1-20:39 (2016)
- [R32] Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, Alberto Coen-Porisini: *Security towards the Edge: Sticky Policy Enforcement for Networked Smart Objects*. Information Systems (Elsevier) 71: 78-89 (2017)
- [R33] Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, Alberto Coen-Porisini: *Securing the Smart Home: a real case study*. Internet Technology Letters (Wiley): 1 (3): e22 (2017)
- [R34] Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, Alberto Coen-Porisini: *REATO: REActing TO denial of service attacks in the Internet of Things.* Computer Networks: 137: 37-48 (2018)
- [R35] Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, Alberto Coen-Porisini: *A Risk Assessment Methodology for the Internet of Things.* Computer Communications (2018): 129: 67-79
- [R36] Sabrina Sicari, Alessandra Rizzardi, Alberto Coen-Porisini: *Smart Transport and Logistics: a Node-RED implementation*. Internet Technology Letters (Wiley): e88 (2019)
- [R37] Sabrina Sicari, Alessandra Rizzardi, Alberto Coen-Porisini: *How to evaluate an Internet of Things system: models, case studies, and real developments*. Software Practice and Experience: 49 (11) (2019)
- [R38] Sabrina Sicari, Alessandra Rizzardi, Gianluca Dini, Pericle Perazzo, Michele La Manna, Alberto Coen-Porisini: *Attribute-Based Encryption and Sticky Policies for Data Access Control in the Internet of Things: a comparison.* International Journal of Information Security (2019), in press
- [R39] Sabrina Sicari, Alessandra Rizzardi, Giuseppe Piro, Alberto Coen-Porisini, Luigi Alfredo Grieco: *Beyond the Smart Things: towards the definition and the performance assessment of a secure architecture for the Internet of Nano-Things.* Computer Networks (2019): 162
- [R40] Daniele Miorandi, Alessandra Rizzardi, Sabrina Sicari, Alberto Coen-Porisini: *Sticky*

policies: a survey. IEEE Transactions on Knowledge and Data Engineering, in press (2019)

- [R41] Sabrina Sicari, Alessandra Rizzardi, Alberto Coen-Porisini: *Smart certification: protecting the originality of the product in the eyewear sector*. Internet Technology Letters (Wiley): 3(3) (2020)
- [R42] Sabrina Sicari, Alessandra Rizzardi, Alberto Coen-Porisini: *5G in the Internet of Things era: an overview on security and privacy challenges*. Computer Networks (Elsevier): 179 (2020)
- [R44] Alessandra Rizzardi, Sabrina Sicari, Alberto Coen-Porisini: *Securing the access control policies to the Internet of Things resources through permissioned blockchain*. Concurrency and Computation: Practice and Experience (Wiley): in press (2022)
- [R45] Sabrina Sicari, Alessandra Rizzardi, Alberto Coen-Porisini: F*rom design to prototyping in the Internet of Things: a domotics case study*. ITU Journal on Future and Evolving Technologies: Internet of Everything 2 (5) (2021)
- [R46] Sabrina Sicari, Alessandra Rizzardi, Alberto Coen-Porisini: *Home Quarantine Patient Monitoring in the Era of COVID-19 Disease*. Smart Health Journal (Elsevier): 23 (2022)
- [R47] Sabrina Sicari, Alessandra Rizzardi, Alberto Coen-Porisini: *Security&privacy issues and challenges in NoSQL databases*. Computer Networks (Elsevier): 206 (2021)

8.3 Riviste nazionali non referate

- [R25] Diego Beretta, Massimiliano Colombo, Sabrina Sicari *"La Sicurezza nelle Architetture SOA*", in ICT Security,pag. 20-22,2005

8.4 Riviste internazionali non referate

- [R26] Sabrina Sicari "*Internet of Things: It's the network, stupid!*", in http://www.icst.org/portals/, 2008
- [R27] Alberto Coen-Porisini, Pietro Colombo, Sabrina Sicari, *"Modeling Privacy Policies"*, in SCI-Topics page http://www.scitopics.com/Modeling_Privacy_Policies.html, 2009

8.5 Proceedings di conferenze internazionali

- [C1] Antonella Brachetti, Aurelio La Corte, Antonio Puliafito, Sabrina Sicari "*Convergence of Voice and Data Services in Ethernet-based Metropolitan Area Network (VoIP System)"*, in Proceeding of international conference on *"Advances in the Internet, Processing, Systems, and Interdisciplinary research"(IPSI 2004),3-6* giugno 2004, Studenica, Belgrado, Serbia
- [C2] Davide Balzarotti, Mattia Monga, Sabrina Sicari, *"Assessing the Risk of Using Vulnerable Components*", in Proceedings of the international workshop on "*Quality of Protection. Security Measurements and Metrics" (QoP'05)QoP2005,* in conjuction with the 10th " European Symposium on Research in Computer Security" (ESORICS 2005) and the 11th "IEEE International Software Metrics Symposium",Springer, pag. 65–78, Milano, Italia,15 settembre 2005
- [C3] Marco Benini, Sabrina Sicari "*Risk Assessment: Intercepting VoIP Calls*", in Proceeding of the international conference on "*VIP Symposia on Internet related research*"*(VIPSI 2007),* Venezia, Italia, 19-22 marzo 2007
- [C4] Marco Benini, Sabrina Sicari *"A Mathematical Framework for Risk Assessment"*, in Proceeding of the IFIP international conference on "*New Technologies, Mobility and Security" (NTMS'07)*, Springer, pag. 457-467, Parigi, Francia, 2-4 maggio 2007
- [C5] Alberto Coen-Porisini, Pietro Colombo, Sabrina Sicari, Alberto Trombetta "*A Conceptual Model for Privacy Policies",* in Proceeding of the 11thinternational conference on*"Software Engineering Application" (SEA'07)*, Acta Press,pag. 570-577Cambridge, Massachusetts, USA , 19-21novembre 2007
- [C6] Sabrina Sicari, Marco Benini *"A Power Conservative Localization Algorithm*", in Proceeding of the international conference on *"IEEE Gold 2008 Remote Sensing"*, IEEE, ESA-ESRIN Frascati, Italia, 22-23 maggio 2008
- [C7] Stefano Braghin, Alberto Coen-Porisini, Pietro Colombo, Sabrina Sicari "*Introducing Privacy in Hospital Information System"*, in Proceeding of the 4thACM international workshopon "*Software engineering for secure systems"(SESS'08-ICSE'08)*, in conjunction with the 30thInternational Conference on Software Engineering (ICSE 2008), ACM, pag. 9-16, Lipsia, Germania, 17-18 maggio 2008

- [C8] Marco Benini, Sabrina Sicari "*Towards a More Secure System: How to Combine Expert Evaluation*", in Proceeding of the4thACM international conference on *"Security and Privacy in Communication Networks"(SecureComm'08),* ACM, Istabul, Turchia, 22-25 settembre 2008
- [C9] Alberto Coen-Porisini, Pietro Colombo, Sabrina Sicari, "*Dealing with Anonymity: a Design Pattern for Privacy-aware Systems*" in Proceeding of the international conference on *"Software Technology and Engineering"(ICSTE'09),* Word Press, Chennai, Tamil Nadu, India, 24-26 luglio2009
- [C10] Sabrina Sicari, Pietro Colombo, Alfredo Grieco, Gennaro Boggia, "*Secure Wireless Multimedia Sensor Network: a Survey"*in Proceeding ofthe 3rdIEEE international conference on "*Mobile Ubiquitous Computing, Systems, Services and Technologies" (Ubicomm'09),*IEEE, Sliema, Malta, 11-16 ottobre 2009
- [C11] Mattia Monga, Sabrina Sicari "*Assessing Data Quality by using a Cross Layer Approach"* in Proceeding of the IEEE International conference on Ultra Modern Technology (ICUMT'09) , St. Petersburg, Russia, ottobre 12-14 2009
- [C12] Roberto Riggio, Sabrina Sicari "*Secure Aggregation in Hybrid Mesh and Wireless Sensor Networks*" in Proceeding of the IEEE International workshop on Scalable Ad Hoc and Sensor Networks(SASN'09) , St. Petersburg, Russia,ottobre 12-13 2009
- [C13] Mattia Monga, Sabrina Sicari "*On the Impact of Localization Data in Wireless Sensor Networks with Malicious Nodes"* in Proceeding of the ACM International Workshop on "Security and Privacy in GIS and LBS" (SPRINGL'09), Seattle (WA), USA, 3novembre 2009
- [C14] Alberto Coen-Porisini, Pietro Colombo, Sabrina Sicari "*Dealing with Anonymity in Wireless Sensor Network"* in Proceeding of the 25th ACM International Symposium On Applied Computing (ACM-SAC'10), Losanna, Svizzera, 22-26 marzo 2010
- [C15] Nicola Gatti, Mattia Monga, Sabrina Sicari "*Localization security in wireless sensor networks as a non-cooperative game"* in Proceeding of the IEEE International Congress on Ultra Modern Telecommunications and Control Systems, 2010 (ICUMT'10), (Best paper award winner), Moscow, Russia, 18-20 ottobre 2010

- [C16] Nicola Gatti, Mattia Monga, Sabrina Sicari "*A localization game in wireless sensor networks*" in Proceeding of the International Conference on Decision and Game Theory for Security (GameSec 2010), Berlin, Germany, 22-23 novembre 2010
- [C17] Alberto Coen-Porisini, Sabrina Sicari "*SeDAP: Secure Data Aggregation Protocol in Privacy aware Wireless Sensor Networks"*in Springer Proceeding of the 2nd International Conference on Sensor Systems and Software (S-Cube 2010), Miami, Florida, USA, 14-15 dicembre 2010
- [C18] Roberto Riggio, Tinku Rasheed, Sabrina Sicari "*Performance Evaluation of an Hybrid Mesh and Sensor Network"* in IEEE Proceeding of Globecom 2011, International Conference, Houston, Texas, USA, 5-9 dicembre 2011
- [C19] Alberto Coen-Porisini, Sabrina Sicari "*Cross layer Data Assessment in Wireless Sensor Networks"*in Proceeding of Sensornets 2012, International Conference on sensor networks, Roma, Italia, 24-26 febbraio 2012
- [C20] Donato Barbagallo, Cinzia Cappiello, Alberto Coen-Porisini, Pietro Colombo, Marco Comerio, Flavio De Paoli, Chiara Francalanci, Sabrina Sicari "*Towards the definition of a framework for service development in the agrofood domain: a conceptual model*" in Proceeding of Webist 2012, 8th International Conference on Web Information Systems and Technologies, Webist 2012, Porto, Portogallo, 18-21 aprile 2012
- [C21] Sabrina Sicari, Luigi Alfredo Grieco, Alessandra Rizzardi, Gennaro Boggia, Alberto Coen-Porisini "*SETA: A SEcure sharing of TAsks in clustered wireless sensor networks*" in Proceeding of the 9th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications 2013, WiMob 2013, Lione, Francia, 7-9 ottobre 2013
- [C22] Sabrina Sicari, Alessandra Rizzardi, Alberto Coen-Porisini, CinziaCappiello "*A NFP Model for Internet of Things applications*" in Proceeding of the 10th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications 2014, WiMob 2014, IEEE, DOI: 10.1109/WiMOB.2014.6962181, ISBN: 978-1-4799-5041-6, pg.265-272, Larnaca, Cyprus, 8-10 ottobre 2014
- [C23] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, Thierry Monteil, Alberto Coen-Porisini: "*Secure OM2M Service Platform*" in Proceeding of Self-IoT 2015, Grenoble, Francia, 7-10 luglio 2015

- [C24] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, Alberto Coen-Porisini. "*GoNe: dealing with node behavior*", in Proceeding of the 5th IEEE International Conference on Consumer Electronics, IEEE 2015 ICCE, IEEE, ISBN: 978-1-4799-8748-1/15/, Berlino, 6-9 ottobre 2015
- [C25] Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, Alberto Coen-Porisini "*Networked Smart Objects: Moving Data Processing Closer to the Source*", in Proceedings of the 2nd International Conference of IoT as a Service, IoTaaS 2015, Roma, 26-27 ottobre 2015
- [C26] Ivan Minakov, Roberto Passerone, Alessandra Rizzardi, Sabrina Sicari: *" Routing Behavior across WSN Simulators: the AODV Case Study"*, in 12th IEEE WFCS 2016, May 3-6 2016, Portugal
- [C27] Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, Alberto Coen-Porisini: *Internet of Things: Security in the Keys*. 12th ACM International Symposium on QoS and Security for Wireless and Mobile Networks 2016, Q2SWinet 2016, Malta, 13-17 Novembre 2016
- [C28] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, Alberto Coen-Porisini: *Secure ICN-IoT Architecture*. IEEE International Conference on Communications, ICC 2017, Parigi, 21-25 Maggio 2017: 417-422
- [C29] Donatello Costantino, Giovanni Malagnini, Francesco Carrera, Alessandra Rizzardi, Pietro Boccadoro, Sabrina Sicari, Luigi Alfredo Grieco: *Solving Interoperability within the Smart Building: a Real Test-Bed*. IEEE International Conference on Communications, ICC 2018: 1-6, Kansas City (USA), 20-24 Maggio 2018
- [C30] Sabrina Sicari, Alessandra Rizzardi, Alberto Coen-Porisini: *Increasing the pervasiveness of the IoT: fog computing coupled with pub&sub and security*. IEEE International Conference on Smart Internet of Things (IEEE SmartIoT 2020), Beijing (Cina) 14-16 Agosto 2020: 64-71
- [C31] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, Alberto Coen-Porisini: *Testing and evaluating a secure-aware pub&sub protocol in a fog-driven IoT environment*. 19th International Conference on Ad Hoc Networks and Wireless (AdHoc-Now 2020), Bari, 19-21 Ottobre 2020: 183-197

8.6 Articoli sottomessi *(Under review)*

- [R43] Sabrina Sicari, Alessandra Rizzardi, Alberto Coen-Porisini: *Insights into security and privacy towards fog computing evolution.* Under Review - Major Revision inviata (2022)
- [R48] Alessandra Rizzardi, Sabrina Sicari, Alberto Coen-Porisini: *Towards rapid prototyping and development of indoor and outdoor monitoring applications.* Under Review - Major Revision inviata (2022)
- [R49] Alessandra Rizzardi, Sabrina Sicari, Alberto Coen-Porisini: *Analysis on functionalities and security features of Internet of Things related protocols.* Under Review - Major Revision inviata (2022)
- [R50] Alessandra Rizzardi, Giuseppe Piro, Sabrina Sicari, Luigi Alfredo Grieco, Alberto Coen-Porisini: *Bio-molecular cryptography for protecting nano-network transmissions in healthcare applications.* Under Review (2021)

8.7 Capitolo di libro

- [CH1] Alberto Coen-Porisini, Pietro Colombo, Sabrina Sicari *"Privacy aware systems: from models to patterns",* in "*Software Engineering for Secure Systems: Industrial and Research Perspectives*"; libro edito da IGI Global (formerly Idea Group Inc.), curato da Dr. Haralambos Mouratidis, University of East London, Inghilterra, pp 1-27, 2011
- [CH2] Sabrina Sicari, Alessandra Rizzardi, Cinzia Cappiello, Daniele Miorandi, Alberto Coen-Porisini: *Towards Data Governance in the Internet of Things*. New Advances in the Internet of Things, edited by Springer (2017) 715: 59-74

8.8 Libri

- [B1] Stephen Hailes, Sabrina Sicari, George Roussos (Eds.) "Sensor Systems and Software", Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, Vol. 24, ISBN: 978-3-642-11527-1, Springer, 2010

- [B2] Stephen Hailes, Sabrina Sicari, George Roussos, Daniele Miorandi and Muriel Medard (Guest Editors.) "Ad-hoc Wireless Network Systems", Special Issue of Mobile Networks & Applications (ACM Monet), Vol. 16, Springer, 2011
- [B3] Sabrina Sicari, Stephen Hailes, DamlaTurgut, Sanaa Sharaffedine, Udai Desai (Guest Editors.) "Security, Privacy and Trust Management in the Internet of Things era- SePriT", Special Issue of Ad Hoc networks, Elsevier, 11(8), 2013

Autorizzo il trattamento dei dati personali ai sensi del Decreto Legislativo 196/2003 e del Regolamento Generale per la Protezione dei Dati UE 2016/679.

In fede

Varese, 26/04/2022 *Sabrina Sophy Sicari*