CURRICULUM VITÆ E PROFESSIONALE DI MARTA CATILLO

Dati Personali e Posizione Attuale

Nome e Cognome: Marta Catillo
Luogo e data di nascita:
Codice Fiscale:
Residenza:

Researcher identifier: ORCID 0000-0002-5025-7969

Contatti:
mobile:
e-mail: marta.catillo@unisannio.it
web: https://unisannio.it/it/users/mcatillo

Posizione attuale

- **Ricercatore** (art. 24 c.3-a L. 240/10) presso il Dipartimento di Ingegneria dell'Università degli Studi del Sannio.
- **Titolare dei seguenti insegnamenti** presso l'Università degli Studi del Sannio:
  - **Programmazione 1** (9 CFU) A.A 2025-2026, Laurea Triennale in Ingegneria Elettronica e Biomedica.
  - **Elementi di Informatica** (6 CFU) A.A 2023-2024, A.A 2024-2025, Laurea Triennale in Ingegneria Civile.
  - **Deep Learning: Teoria, Applicazioni e Framework** (4 CFU), A.A 2023-2024, A.A 2024-2025, corso di Dottorato di Ricerca in Tecnologie dell'Informazione per l'Ingegneria.
- **Associate Editor** IEEE Transactions on Industrial Informatics.
- **Editor-in-Chief** International Journal of Open Source Software and Processes, IGI Global (indicizzata da *Scopus*, *Compendex*, *DBLP*, ed altri maggiori indici).

Lingue straniere
Inglese, ottimo (parlato e scritto).
Francese, livello intermedio (parlato e scritto).

Quadro Sintetico del Percorso Formativo-Scientifico

Titoli di studio e professionali

- 2023 **Dottorato di ricerca** in Tecnologie dell'Informazione per l'Ingegneria (XXXV ciclo) conseguito con votazione *Eccellente* presso l'Università degli Studi del Sannio – Tesi: "*On the Use of Machine Learning for Intrusion Detection: Public Datasets, Challenges and Solutions*".
- 2021 Abilitazione all' **esercizio della professione** di Ingegnere dell'Informazione (Sezione A), Università degli Studi del Sannio.
- 2019 **Laurea Magistrale *con lode* in Ingegneria Informatica** (classe delle Lauree Magistrali in Ingegneria Informatica LM-32) conseguita presso l'Università degli Studi del Sannio.

Attività di ricerca presso Università e qualificati istituti italiani o esteri

- Università degli Studi del Sannio:
  - 2024-ad oggi Ricercatore;
  - 2023-2024 Assegnista di ricerca;
  - 2019-2023 Dottoranda;
  - 2019 Borsista di ricerca.
- **Borsista di ricerca** per 12 mesi (Luglio 2018 – Luglio 2019) presso il **Consortium GARR (Roma),** gestore della rete nazionale a banda ultralarga dedicata alla comunità dell'istruzione e della ricerca.

Progetti nazionali ed Europei

- Partecipazione alle attività e membro del gruppo di ricerca del **Progetto BOTITS** "Boosting OT and IT Security", progetto di ricerca finanziato da Silicon Valley Community Foundation, Mountain View, CA 94040-1498 U.S.A. tramite il Laboratorio Nazionale di Cybersecurity CINI. Partecipanti: Università degli Studi del Sannio di Benevento, Università degli Studi di Napoli Parthenope, Università degli Studi di Napoli Federico II.
- Partecipazione alle attività e membro del gruppo di ricerca del **progetto EMELIOT** "Engineered MachinE Learning-intensive IoT system", Progetto di Ricerca di Interesse Nazionale (PRIN 2020 - CUP F83C22000500001). Partecipanti: Università degli Studi di Milano-Bicocca, Politecnico di Milano, Università degli Studi dell'Aquila, Università degli Studi del Sannio di Benevento, Università degli Studi di Salerno.
- Partecipazione alle attività e membro del gruppo di ricerca del **progetto IDA** - Information Disorder Awareness - "Security Rights in Cyber Space - SERICS" Project - PE0000014 - Spoke 2 "Misinformation and Fakes" (CUP D43C22003050001). Partecipanti: Università degli Studi del Sannio di Benevento, Università degli Studi di Napoli Federico II, Università degli Studi di Napoli Parthenope, Università degli Studi della Campania Luigi Vanvitelli.

Attività Istituzionale Concernente la Didattica

Marta Catillo ha preso parte alla seguente attività istituzionale:

- **2020-2022: cultore della materia** e membro delle commissioni di esame per l'insegnamento Sistemi Concorrenti.
- **2020-2022: cultore della materia** e membro delle commissioni di esame per l'insegnamento Architettura dei Calcolatori.
- **2020-ad oggi: cultore della materia** e membro delle commissioni di esame per l'insegnamento Data Science.
- **2022-ad oggi: cultore della materia** e membro delle commissioni di esame per l'insegnamento Calcolo Parallelo e ad Alte Prestazioni.
- **2023-ad oggi: cultore della materia** e membro delle commissioni di esame per l'insegnamento Calcolatori Elettronici.
- **2023-ad oggi: cultore della materia** e membro delle commissioni di esame per l'insegnamento Sistemi Operativi.

Comitati Editoriali di Riviste Scientifiche Internazionali

- **Associate Editor** *IEEE Transactions on Industrial Informatics.*
- **Editor-in-Chief** *Int'l J. of Open Source Software and Processes*, IGI Global (indicizzato da Scopus).
- **Editorial Review Board Member**, Int'l J. of Open Source Software and Processes (2020-2023), J.UCS (Journal of Universal Computer Science), Frontiers in Big Data (Cybersecurity and Privacy section).

Direzione di Comitati Scientifici o Organizzativi

- **Track Chair** della Safe, Secure and Robust AI (S2RAI-SSRAI) track co-located con la 41st ACM/SIGAPP Symposium on Applied Computing (SAC 2026).
- **Local Chair** della 18th International Conference on Availability, Reliability, and Security (ARES 2023).
- **Workshop Co-chair ed Organizzatore** del 7th International Workshop on Resiliency, Security, Defenses and Attacks (RSDA 2022) co-located con la 33rd IEEE International Symposium of Software Reliability Engineering (ISSRE 2022).
- **Workshop Co-chair ed Organizzatore** del 6th International Workshop on Reliability and Security Data Analysis (RSDA 2021) co-located con la 32nd IEEE International Symposium of Software Reliability Engineering (ISSRE 2021).
- **Workshop Co-chair ed Organizzatore** del 5th International Workshop on Reliability and Security Data Analysis (RSDA 2020) co-located con la 31st IEEE International Symposium of Software Reliability Engineering (ISSRE 2020).

Partecipazione a Comitati Scientifici di Programma

- **SAFE-SN 2025**, The 2nd International Workshop on Safeguarding Social Networks: Privacy, Security, Trust, and Truth in the Age of Misinformation.
- **ANIBUS 2025**, The 1st International Workshop on the Assessment with New Methodologies, Unified Benchmarks, and Environments, of Intrusion detection and response Systems.
- **SYNDAiTE 2025**, The 1st International Workshop on Synthetic Data for AI Trustworthiness and Evolution.
- **WETICE 2025**, The 33rd International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises.
- **S2RAI 2025,** Safe, Secure and Robust AI Track at the SAC25 Conference. The 40th ACM/SIGAPP Symposium On Applied Computing.
- **ARES 2025**, The 20th International Conference on Availability, Reliability and Security.
- **AISec 2024,** The 17th ACM Workshop on Artificial Intelligence and Security.
- **WETICE 2024**, The 32nd International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises.
- **SAFE-SN 2024**, The 1st International Workshop on Safeguarding Social Networks: Privacy, Security, Trust, and Truth in the Age of Misinformation.
- **S2RAI 2024**, Safe, Secure and Robust AI Track at the SAC24 Conference. The 39th ACM/SIGAPP Symposium On Applied Computing.
- **ARES 2024**, The 19th International Conference on Availability, Reliability and Security.
- **CLOUDCOM 2023**, The 14th IEEE International Conference on Cloud Computing Technology and Science.
- **DCDS 2023,** The 5th Workshop on Data-Centric Dependability and Security.
- **ARES 2023**, The 18th International Conference on Availability, Reliability and Security.
- **ARES 2022**, The 17th International Conference on Availability, Reliability and Security.

Attività di Revisione per Riviste Internazionali

Marta Catillo svolge attività di revisione per **riviste internazionali**, di cui si riportano le principali in termini di rilevanza e/o classe di merito:

Primary reviewer:

- Journal of Network and Computer Applications (Elsevier);
- IEEE Transaction On Information Forensics & Security (TIFS);
- Software Quality Journal (Springer);
- International Journal of Information Security (Springer);
- IEEE Access;
- International Journal of Open Source Software and Processes (IJOSSP);
- International Journal of Information Security (Springer);
- International Journal of Machine Learning and Cybernetics (Springer);

- Intelligenza Artificiale;
- Journal of Circuits, Systems, and Computers.

Premi e Riconoscimenti Nazionali ed Internazionali

Best Paper Awards

- **Best Paper Award** alla 19th International Conference on Availability, Reliability and Security (ARES), 2024, Vienna (Austria) per il lavoro *"Towards realistic problem-space adversarial attacks against machine learning in network intrusion detection"*.
- **Best Paper Award** alla 14th International Conference on the Quality of Information and Communications Technology, 2021, Virtual Event per il lavoro "*A Critique on the Use of Machine Learning on Public Datasets for Intrusion Detection*".

Travel Student Grants

- **Travel Student Grant** conferito alla 53rd IEEE/IFIP International Conference on Dependable Systems and Networks, Porto, Portogallo.

Borsa di studio GARR

Consortium GARR (Roma), 2018-2019.

Articoli su Riviste Internazionali

R-1. C. Bernardo, M. Catillo, A. Pecchia, F. Vasca, U. Villano
SPREADSHOT: Analysis of fake news spreading through topic modeling and bipartite weighted graphs
Online Social Networks and Media
Vol. 49, pp. 100324, October 2025
10.1016/j.osnem.2025.100324
Elsevier

R-2. M. Catillo, A. Pecchia, U. Villano
MultiCIDS: Anomaly-based collective intrusion detection by deep learning on IoT/CPS multivariate time series
Internet of Things
Vol. 30, pp. 101519, March 2025
10.1016/j.iot.2025.101519
Elsevier

R-3. M. Catillo, A. Pecchia, U. Villano
Exploring the effect of training-time randomness on the performance of deep neural networks for intrusion detection
Soft Computing
Vol. 28, pp. 1957-1969, January 2024
10.1007/s00500-023-09552-4
Springer

R-4. M. Catillo, A. Pecchia, U. Villano
CPS-GUARD: Intrusion detection for cyber-pysical systems and IoT devices using outlier-aware deep autoencoders
Computers & Security
Vol. 129, Art. No. 103210, June 2023
DOI: 10.1016/j.cose.2023.103210
Elsevier

R-5. M. Catillo, A. Pecchia, U. Villano
Successful intrusion detection with a single deep autoencoder: theory and practice
Software Quality Journal
Vol. 32, pp. 95-123, May 2023
10.1007/s11219-023-09636-2
Springer

R-6. M. Catillo, Massimiliano Rak, U. Villano
A survey on auto-scaling: how to exploit cloud elasticity
International Journal of Grid and Utility Computing
Vol. 14, Issue 1, pp. 37-50, March 2023
10.1504/IJGUC.2023.129702
Inderscience

R-7. M. Catillo, A. Pecchia, U. Villano
A Deep Learning Method for Lightweight and Cross-Device IoT Botnet Detection
Applied Sciences
Vol. 13, Issue 2, Junary 2023
10.3390/app13020837
MDPI

R-8. M. Catillo, A. Pecchia, U. Villano
No more DoS? An empirical study on defense techniques for web server Denial of Service mitigation
Journal of Network and Computer Applications
Vol. 202, Art. No. 103363, June 2022
10.1016/j.jnca.2022.103363
Elsevier

R-9. M. Catillo, A. Pecchia, U. Villano
AutoLog: Anomaly detection by deep autoencoding of system logs
Expert Systems with Applications
Vol. 191, Art. No. 116263, April 2022
10.1016/j.eswa.2021.116263
Elsevier

R-10. M. Catillo, A. Del Vecchio, A. Pecchia, U. Villano
Transferability of machine learning models learned from public intrusion detection datasets: the CICIDS2017 case study
Software Quality Journal
Vol. 30, pp. 955-981, March 2022
10.1007/s11219-022-09587-0
Springer

R-11. M. Catillo, A. Pecchia, M. Rak, U. Villano
Demystifying the role of public intrusion datasets: A replication study of DoS network traffic data
Computers & Security
Vol. 108, Art. No. 102341, September 2021
10.1016/j.cose.2021.102341
Elsevier

R-12. M. Catillo, L.Ocone, M. Rak, U. Villano
Black-box load testing to support auto-scaling web applications in the cloud
International Journal of Grid and Utility Computing
Vol. 12, Issue 2, pp. 139-140, May 2021
10.1504/IJGUC.2021.114823
Inderscience

R-13. M. Catillo, M. Rak, U. Villano
Discovery of DoS attacks by the ZED-IDS anomaly detector
Journal of High Speed Networks
Vol. 25, Issue 4, pp. 349-365, November 2019
10.3233/JHS-190620
IOS Press

Articoli in Atti di Conferenze

C-1. M. Catillo, A. Pecchia, U.Villano,
Detection of Adversarial Examples by Adversarial Training: A Study on the Suitability of FGSM for Hardening NIDS Against Problem-Space Attacks
Proc. of the 20th International Conference on Availability, Reliability and Security (ARES), pp.232-249, 2025, Ghent (Belgio)
10.1007/978-3-032-00644-8_14
Springer

C-2. C. Bernardo, M. Catillo, A. Pecchia, F. Vasca, U. Villano,
Bipartite Graph Modeling for the Analysis of Fake News Propagation
Proc. of the 26 thAdvances in Social Networks Analysis and Mining, pp. 49.63, 2025, Rende (Italia)
/10.1007/978-3-031-85386-9_4
Springer

C-3. M. Catillo, A. Pecchia, U. Villano
USB-IDS-TC: A Flow-Based Intrusion Detection Dataset of DoS Attacks in Different Network Scenarios
Proc. of the 11th International Conference on Information Systems Security and Privacy (ICISSP), vol. 1, pp. 302-309, 2025, Porto (Portogallo)
DOI: 10.5220/0013248600003899
SciTePress

C-4. M. Catillo, A. Pecchia, A. Repola, U. Villano
A critique on the (mis)use of feature-space attacks for adversarial machine learning in NIDS
Proc. the 20th European Dependable Computing Conference (EDCC), pp. 110–115, 2025, Lisboa (Portogallo)
10.1109/EDCC66201.2025.00027
IEEE

C-5. P. Avella, C. Bernardo, M. Catillo, A. Pecchia, F. Vasca, U. Villano,
Topic Modeling for Graph-Based Analysis of Fake News Diffusion
Proc. The 33rd International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), pp. 1-6, 2025, Catania (Italia)
10.1109/WETICE67341.2025.11092262
IEEE

C-6. M. Catillo, A. Pecchia, A. Repola, U. Villano
Towards realistic problem-space adversarial attacks against machine learning in network intrusion detection
Conferenza Italiana sulla Cybersecurity (ITASEC), 2025, Bologna (Italia)
*Presentazione dell'omonimo lavoro [C-7]

C-7. M. Catillo, A. Pecchia, A. Repola, U. Villano
Towards realistic problem-space adversarial attacks against machine learning in network intrusion detection
Proc. of the19th International Conference on Availability, Reliability and Security (ARES), Art. No. 114, 2024, Vienna (Austria)
* Winner of the Best Paper Award*
10.1145/3664476.3669974
ACM

C-8. V. Casola, M. Catillo, A. De Benedictis, F. Moretta, A.Pecchia, M. Rak, U. Villano
DEFEDGE: Threat-Driven Security Testing and Proactive Defense Identification for

Edge-Cloud Systems
Proc. of the 38th the International Conference on Advanced Information Networking and Applicationsn (AINA), Lecture Notes on Data Engineering and Communications Technologies, vol. 203, 2024, Kitakyushu (Giappone)
10.1007/978-3-031-57931-8_8
Springer

C-9. M. Catillo, A. Pecchia, U. Villano
Traditional vs Federated Learning with Deep Autoencoders: a Study in IoT Intrusion Detection
Proc. of the 14th IEEE International Conference on Cloud Computing Technology and Science (CLOUDCOM), pp. 208-215, 2023 Napoli (Italia)
10.1109/CloudCom59040.2023.00042
IEEE Computer Society Press

C-10. M. Catillo, A. Pecchia, U. Villano
A Case Study with CICIDS2017 on the Robustness of Machine Learning against Adversarial Attacks in Intrusion Detection
Proc. of the18th International Conference on Availability, Reliability and Security (ARES), Art. No. 74, 2023, Benevento (Italia)
10.1145/3600160.3605031
ACM

C-11. M. Catillo, A. Pecchia, U. Villano
Machine Learning on Public Intrusion Datasets: Academic Hype or Concrete Advances in NIDS?
Proc. of the 53rd International Symposium on Dependable Systems and Networks – Supplemental Volume (DSN-S), pp. 132-136, 2023 Porto (Portogallo)
10.1109/DSN-S58398.2023.00038
IEEE Computer Society Press

C-12. R. Della Corte, M. Catillo, J.F. Ferreira, G. Li
Message from the RSDA 2023 Workshop Chairs
Proc. of the 33rd International Symposium on Software Reliability Engineering Workshops, (ISSREW 2021), Charlotte (USA)
10.1109/ISSREW55968.2022.00018
IEEE Computer Society Press

C-13. M. Catillo, A. Pecchia, U. Villano
Botnet Detection in the Internet of Things through All-in-one Deep Autoencoding
Proc. of the 17th International Conference on Availability, Reliability and Security (ARES), Art. No. 90, 2022, Vienna (Austria)
10.1145/3538969.3544460
ACM

C-14. M. Catillo, A. Pecchia, U. Villano
Simpler is Better: On the Use of Autoencoders for Intrusion Detection
Proc. of the 15th International Conference on the Quality of Information and

Communications Technology (QUATIC), Vol. 1621, 2022, Talavera de la Reina (Spagna)
10.1007/978-3-031-14179-9_15
Springer

C-15. M. Catillo, A. Del Vecchio, A. Pecchia, U. Villano
Transferability of machine learning models learned from public intrusion detection datasets: the CICIDS2017 case study*
Conferenza Italiana sulla Cybersecurity (ITASEC), 2022, Roma (Italy)
*Presentazione dell'omonimo lavoro [R-10]

C-16. M. Catillo, A. Del Vecchio, A. Pecchia, U. Villano
On the Quality of Network Flow Records for IDS Evaluation: A Collaborative Filtering Approach
Proc. of the 32nd IFIP International Conference on Testing Software and Systems (ICTSS), Vol. 13045, 2022, *Virtual Event*
10.1007/978-3-031-04673-5_16
Springer

C-17. R. Della Corte, M. Catillo, J.F. Ferreira
Message from the RSDA 2021 Workshop Chairs
Proc. of the 32nd International Symposium on Software Reliability Engineering Workshops, (ISSREW 2021), *Virtual Event*
10.1109/ISSREW53611.2021.00018
IEEE Computer Society Press

C-18. M. Catillo, A. Del Vecchio, A. Pecchia, U. Villano
A Critique on the Use of Machine Learning on Public Datasets for Intrusion Detection
Proc. of the 14th International Conference on the Quality of Information and Communications Technology (QUATIC), Vol. 1439, 2021, *Virtual Event*
* Winner of the Best Paper Award*
10.1007/978-3-030-85347-1_19
Springer

C-19. M. Catillo, A. Pecchia, M. Rak, U. Villano
A case study on the representativeness of public DoS network traffic data for cybersecurity research
Conferenza Italiana sulla Cybersecurity (ITASEC), 2021, *Virtual Event*
*Presentazione dell'omonimo lavoro [C-24]

C-20. M. Catillo, A. Del Vecchio, L. Ocone, A. Pecchia, U. Villano
USB-IDS-1: a Public Multilayer Dataset of Labeled Network Flows for IDS Evaluation
Proc. of the 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), pp. 1-6, 2021, *Virtual Event*
DOI: 10.1109/DSN-W52860.2021.00012
IEEE Computer Society Press

C-21. M. Catillo, A. Pecchia, U. Villano
Measurement-Based Analysis of a DoS Defense Module for an Open Source Web Server
Proc. of the 32nd IFIP International Conference on Testing Software and Systems 2020 (ICTSS), Vol. 12543, 2020, *Virtual Event*
10.1007/978-3-030-64881-7_8
Springer

C-22. R. Della Corte, C. Gutierrez, J.Hong, M. Catillo
Message from the RSDA 2020 Workshop Chairs
Proc. of the 31st International Symposium on Software Reliability Engineering Workshops, (ISSREW 2020), pp. 35-35, 2020, *Virtual Event*
DOI: 10.1109/ISSREW51248.2020.00019
IEEE Computer Society Press

C-23. M. Catillo, A. Pecchia, U. Villano
Towards a Framework for Improving Experiments on DoS Attacks
Proc. of the 13th International Conference on the Quality of Information and Communications Technology (QUATIC), Vol. 1266, 2020, *Virtual Event*
10.1007/978-3-030-58793-2_25
Springer

C-24. M. Catillo, A. Pecchia, M. Rak, U. Villano
A case study on the representativeness of public DoS network traffic data for cybersecurity research
Proc. of the 15th International Conference on Availability, Reliability and Security (ARES), Art. No. 6, 2020, *Virtual Event*
10.1145/3407023.3407042
ACM

C-25. M. Catillo, L. Ocone, M.Rak, U. Villano
Auto-scaling Applications in the Cloud by Simple Indexes with Complex Loads
Proc. of the 29th International Conference on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), pp. 76-81, 2020, *Virtual Event*
10.1109/WETICE49692.2020.00023.
IEEE Computer Society Press

C-26. M. Catillo, M. Rak, U. Villano
2L-ZED-IDS: A Two-Level Anomaly Detector for Multiple Attack Classes
Proc. of the 34th International Conference on Adavanced Information Networking and Applications (WAINA), Vol. 1150, 2020
10.1007/978-3-030-44038-1_63
Springer

C-27. M. Catillo, M. Rak, U. Villano
Auto-scaling in the Cloud: Current Status and Perspectives
Proc. of the 14th International Conference on P2P, Parallel, Grid, Cloud, and Internet Computing (3PGCIC), Vol. 96, 2019, Antwerp (Belgio)