Università degli Studi di Napoli Parthenope

FITNESS

Fault and Intrusion Tolerant NEtworked SystemS

Attività di Ricerca
Area 9 - IINF-05/A

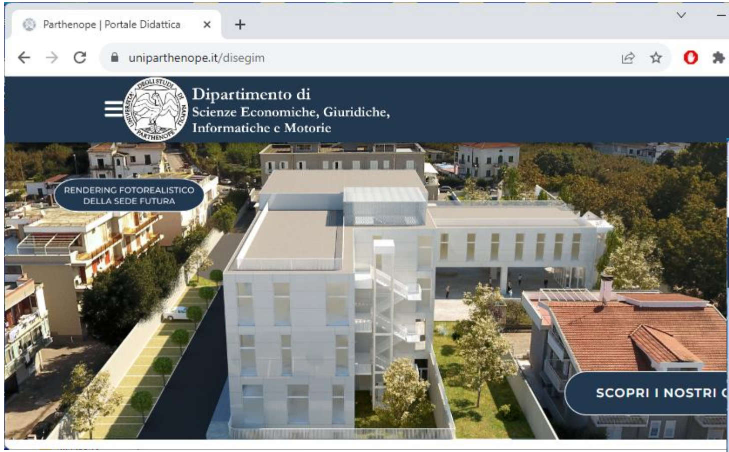
Giovanni Mazzeo

Roadmap

- Key Personnel
- Aree di Ricerca
- Attività Sperimentali
- Progetti EC-Funded
- Progetti Italiani
- Pubblicazioni
- Spin-Off

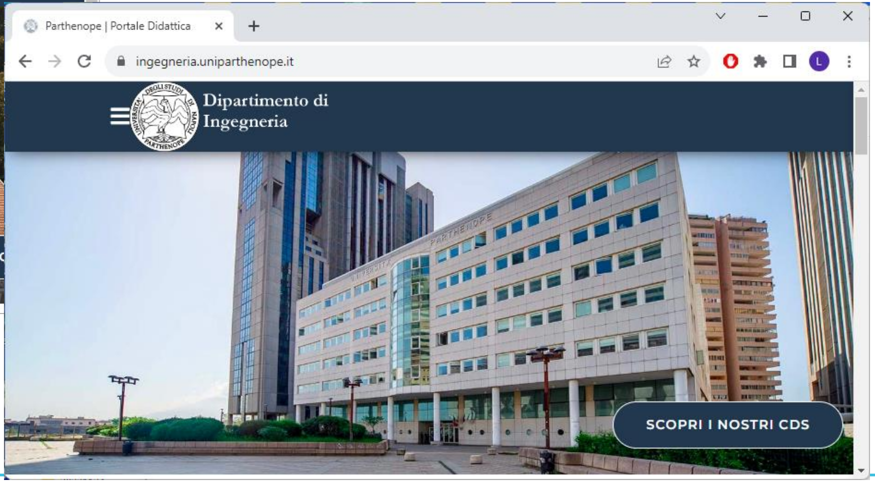
Laboratorio Interdipartimentale

- **FITNESS**:
  - **F**ault and **I**ntrusion **T**olerant **NE**tworked **S**ystem**S**



DiSEGIM

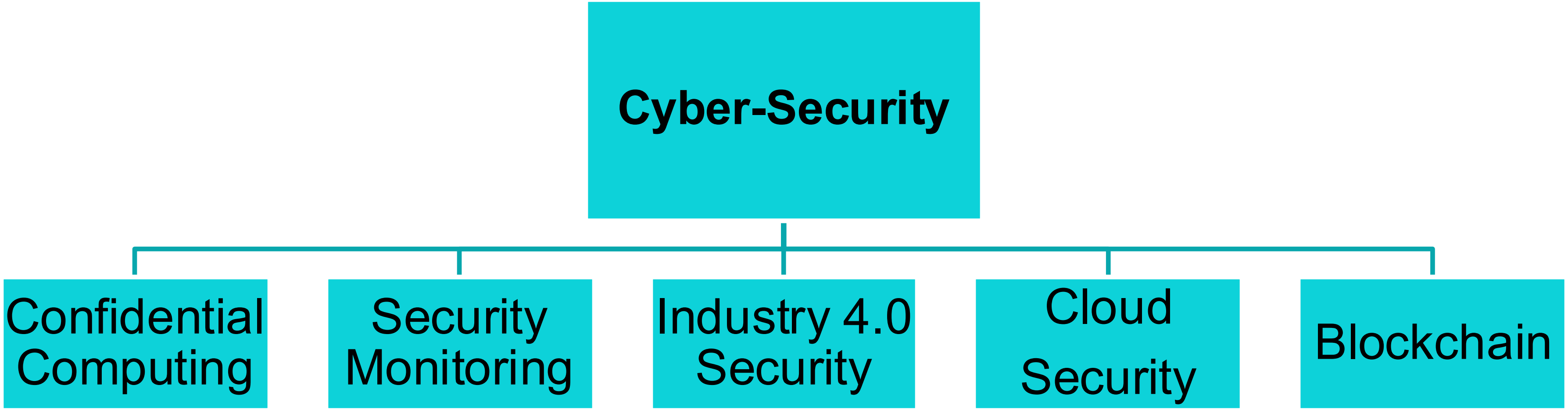
DING



Key Personnel

- **Luigi Romano** (DiSEGIM): Professore Ordinario SSD IINF-05/A
- **Luigi Coppolino** (DING): Professore Associato SSD IINF-05/A
- **Salvatore D’Antonio** (DiSEGIM): Professore Associato SSD IINF-05/A
- **Giovanni Mazzeo** (DiSEGIM): Professore Associato SSD IINF-05/A
- **Roberto Nardone** (DING): Professore Associato SSD IINF-05/A
- **Daniele Granata** (DiSEGIM): RTD-A SSD IINF-05/A
- **5 PhD Students, 2 Research Assistant**

Aree di Ricerca



Cyber-Security

Confidential Computing

Security Monitoring

Industry 4.0 Security

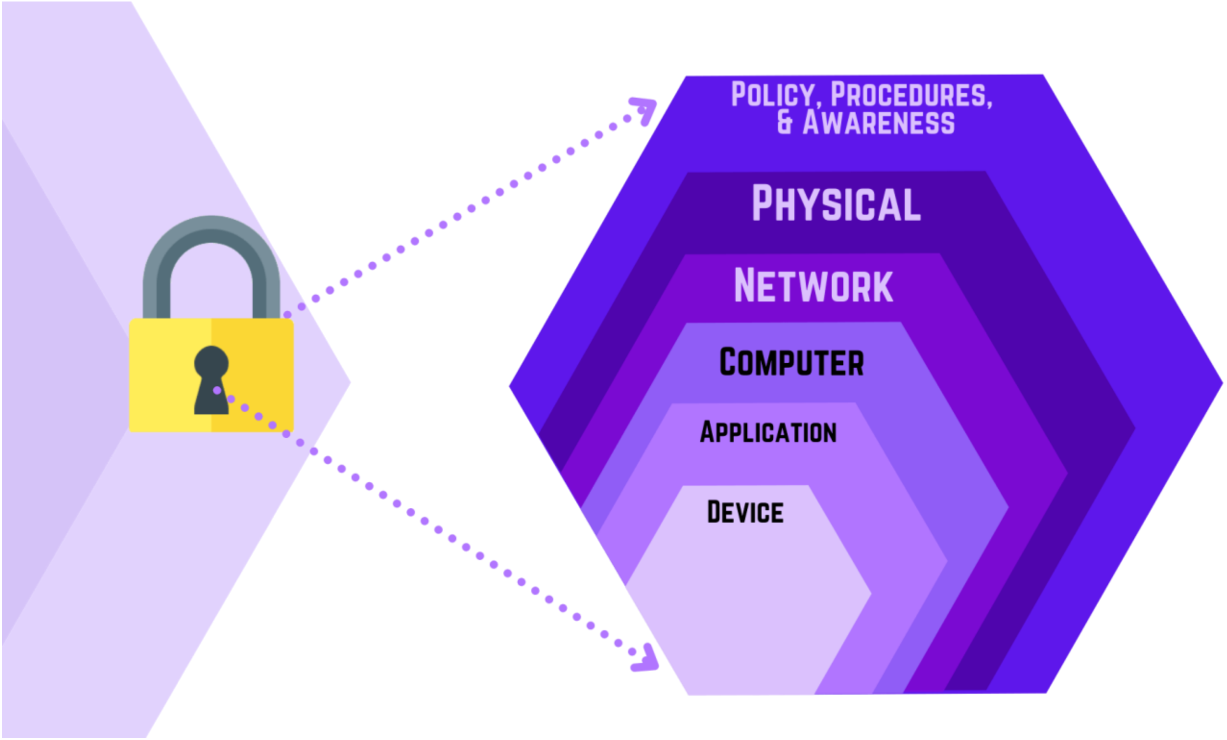
Cloud Security

Blockchain

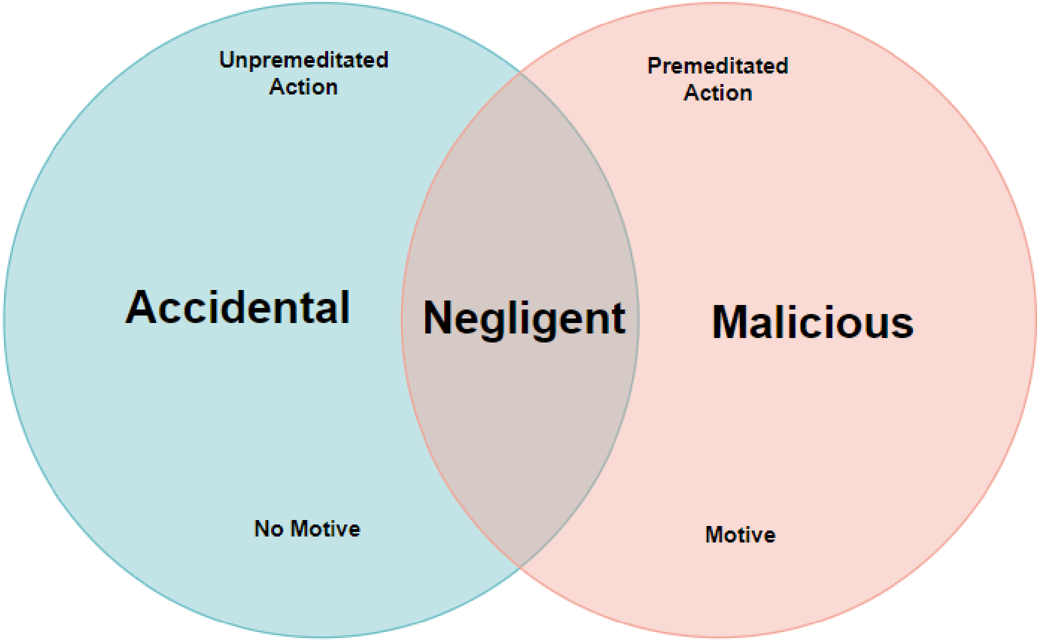
Aree di Ricerca

- Confidential Computing:
  - Tecniche di protezione del dato quando è processato in ambienti non fidati
- Sicurezza nell’industria 4.0:
  - Approcci per garantire la sicurezza in sistemi di controllo industriali i cui protocolli appartengono all’industria 4.0
- Security Monitoring:
  - Soluzioni per garantire l’identificazione di attacchi complessi
- Cloud Security
  - Tecniche per la prevenzione e mitigazione di attacchi in ambiente Cloud
- Blockchain
  - Metodologie per la verifica dell’autenticità ed integrità dei dati mediante blockchain

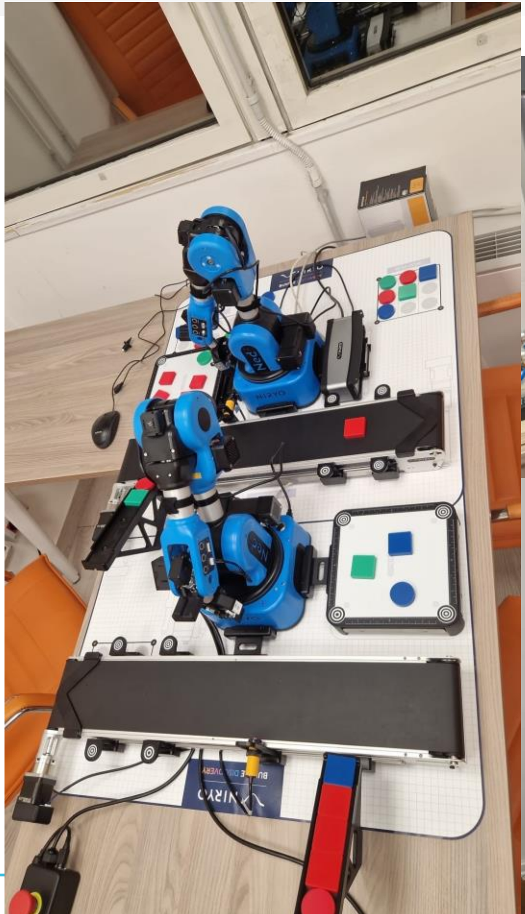
Aree di Ricerca



Protezioni contro i Malicious Insiders



Attività Sperimentali su Flexible Manufacturing



Progetti EC-Funded (FP7, H2020 e HorizonEurope)

INTERSECTION

INTERSECTION (INfrastructure for heTErogeneous, Resilient, SEcure, Complex, Tightly Inter-Operating Networks)

inter SECTION

INSPIRE

INSPIRE (INcreasing Security and Protection through Infrastructure REsilience)

INSPIRE

INSPIRE INCO

INSPIRE INCO (INSPIRE INternational COoperation)

INSPIRE INCO

STREAM

Scalable autonomic s**T**reaming middleware for **REA**l time processing of **M**assive data flows

SAWSOC

SAWSOC (Situation AWare Security Operations Center)

SAWSOC

MASSIF

MASSIF (MAnagement of Security information and events in Service Infrastructures)

>MASSIF<

LeanBigData

LeanBigData

CERTIFY

SERECA

SERECA (Secure Enclaves for REactive Cloud Applications)

SERECA

SecureCloud

SRT-15
Intelligence Push in the Enterprise Realm

encrypt

Protecting the infrastructure of Europe and the people in the European smart cities

CyberSEAS

COMPACT
CYBERSECURITY FOR PUBLIC ADMINISTRATIONS

KONFIDO

INCISIVE
A multimodal AI-based toolbox and an interoperable health imaging repository for the empowerment of imaging analysis related to the diagnosis, prediction and follow-up of cancer

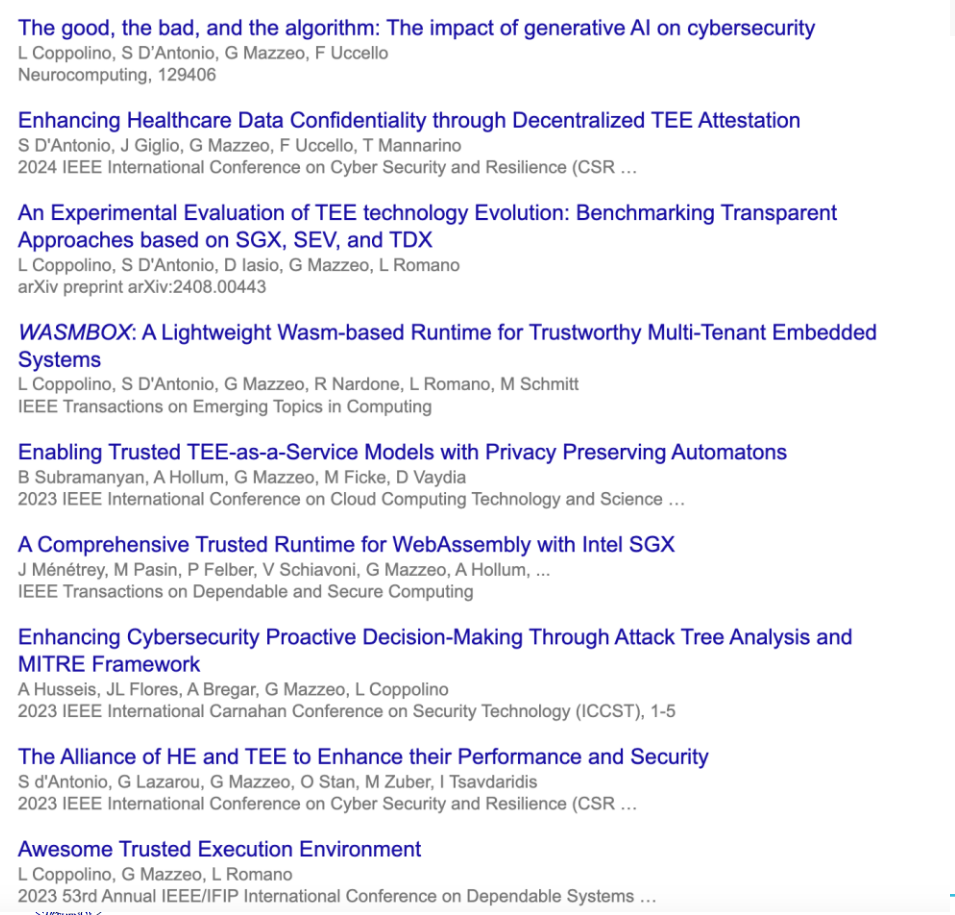
7SHIELD

AI4HEALTHSEC
A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures

Progetti Italiani (PRIN, PNRR, MISE/MIMIT, …)

- AUDACE
- COBELLIS
- ISTINTO
- MIRABILE
- IDA
- EMDAS
- S2
- DOSSIER

Pubblicazioni (più recenti)



The good, the bad, and the algorithm: The impact of generative AI on cybersecurity
L Coppolino, S D'Antonio, G Mazzeo, F Uccello
Neurocomputing, 129406

Enhancing Healthcare Data Confidentiality through Decentralized TEE Attestation
S D'Antonio, J Giglio, G Mazzeo, F Uccello, T Mannarino
2024 IEEE International Conference on Cyber Security and Resilience (CSR …

An Experimental Evaluation of TEE technology Evolution: Benchmarking Transparent Approaches based on SGX, SEV, and TDX
L Coppolino, S D'Antonio, D Iasio, G Mazzeo, L Romano
arXiv preprint arXiv:2408.00443

WASMBOX: A Lightweight Wasm-based Runtime for Trustworthy Multi-Tenant Embedded Systems
L Coppolino, S D'Antonio, G Mazzeo, R Nardone, L Romano, M Schmitt
IEEE Transactions on Emerging Topics in Computing

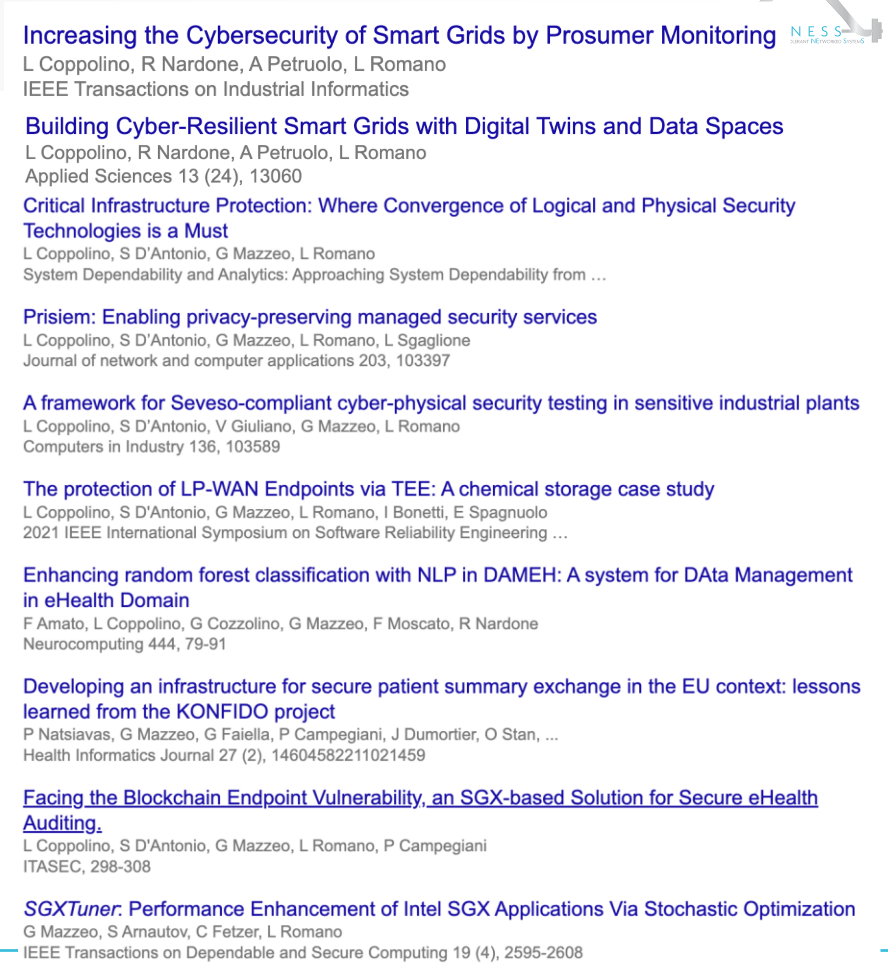
Enabling Trusted TEE-as-a-Service Models with Privacy Preserving Automatons
B Subramanyan, A Hollum, G Mazzeo, M Ficke, D Vaydia
2023 IEEE International Conference on Cloud Computing Technology and Science …

A Comprehensive Trusted Runtime for WebAssembly with Intel SGX
J Ménétrey, M Pasin, P Felber, V Schiavoni, G Mazzeo, A Hollum, …
IEEE Transactions on Dependable and Secure Computing

Enhancing Cybersecurity Proactive Decision-Making Through Attack Tree Analysis and MITRE Framework
A Husseis, JL Flores, A Bregar, G Mazzeo, L Coppolino
2023 IEEE International Carnahan Conference on Security Technology (ICCST), 1-5

The Alliance of HE and TEE to Enhance their Performance and Security
S d'Antonio, G Lazarou, G Mazzeo, O Stan, M Zuber, I Tsavdaridis
2023 IEEE International Conference on Cyber Security and Resilience (CSR …

Awesome Trusted Execution Environment
L Coppolino, G Mazzeo, L Romano
2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems …



Increasing the Cybersecurity of Smart Grids by Prosumer Monitoring
L Coppolino, R Nardone, A Petruolo, L Romano
IEEE Transactions on Industrial Informatics

Building Cyber-Resilient Smart Grids with Digital Twins and Data Spaces
L Coppolino, R Nardone, A Petruolo, L Romano
Applied Sciences 13 (24), 13060

Critical Infrastructure Protection: Where Convergence of Logical and Physical Security Technologies is a Must
L Coppolino, S D'Antonio, G Mazzeo, L Romano
System Dependability and Analytics: Approaching System Dependability from …

Prisiem: Enabling privacy-preserving managed security services
L Coppolino, S D'Antonio, G Mazzeo, L Romano, L Sgaglione
Journal of network and computer applications 203, 103397

A framework for Seveso-compliant cyber-physical security testing in sensitive industrial plants
L Coppolino, S D'Antonio, V Giuliano, G Mazzeo, L Romano
Computers in Industry 136, 103589

The protection of LP-WAN Endpoints via TEE: A chemical storage case study
L Coppolino, S D'Antonio, G Mazzeo, L Romano, I Bonetti, E Spagnuolo
2021 IEEE International Symposium on Software Reliability Engineering …

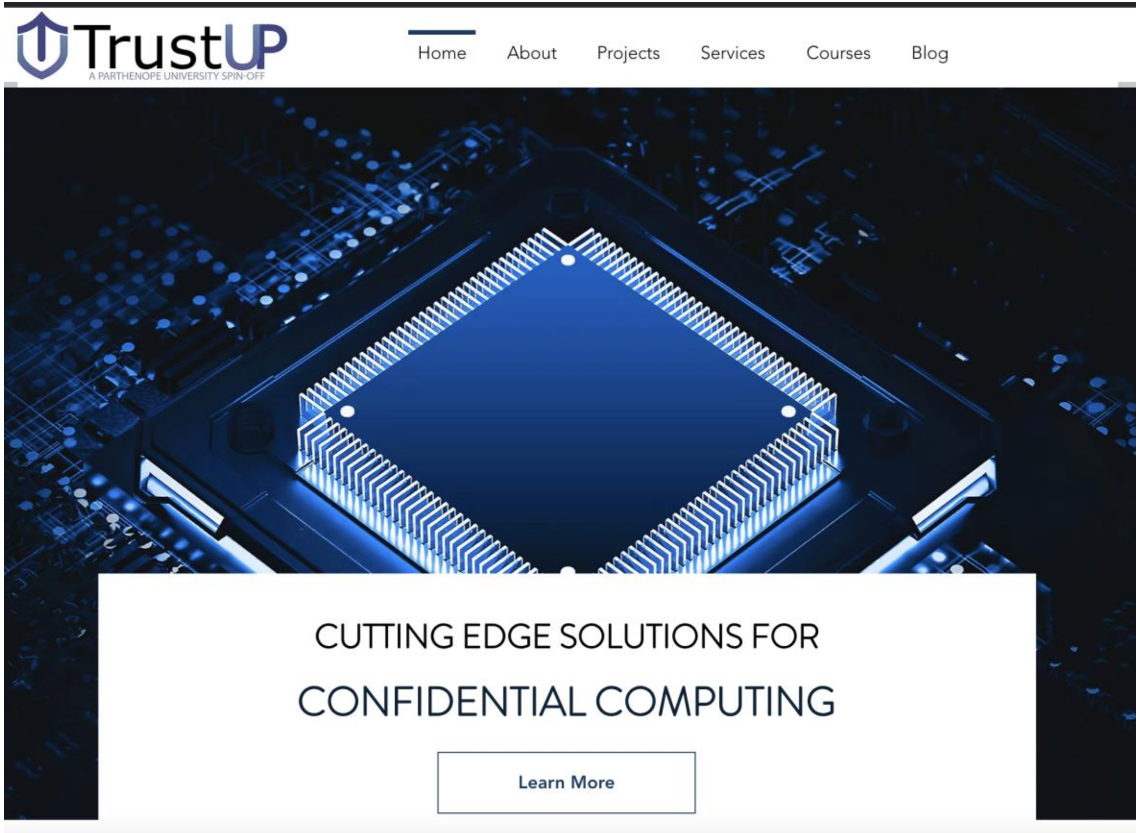
Enhancing random forest classification with NLP in DAMEH: A system for DAta Management in eHealth Domain
F Amato, L Coppolino, G Cozzolino, G Mazzeo, F Moscato, R Nardone
Neurocomputing 444, 79-91

Developing an infrastructure for secure patient summary exchange in the EU context: lessons learned from the KONFIDO project
P Natsiavas, G Mazzeo, G Faiella, P Campegiani, J Dumortier, O Stan, …
Health Informatics Journal 27 (2), 14604582211021459

Facing the Blockchain Endpoint Vulnerability, an SGX-based Solution for Secure eHealth Auditing.
L Coppolino, S D'Antonio, G Mazzeo, L Romano, P Campegiani
ITASEC, 298-308

SGXTuner: Performance Enhancement of Intel SGX Applications Via Stochastic Optimization
G Mazzeo, S Arnautov, C Fetzer, L Romano
IEEE Transactions on Dependable and Secure Computing 19 (4), 2595-2608

Spin-Off – Trust Up



TrustUP

A PARTHENOPE UNIVERSITY SPIN-OFF

CUTTING EDGE SOLUTIONS FOR

CONFIDENTIAL COMPUTING

FITNESS

FAULT AND INTRUSION TOLERANT NETWORKED SYSTEMS

Thank you

UNIVERSITA' DEGLI STUDI DI NAPOLI PARTHENOPE