UNIVERSITÀ
POLITECNICA
DELLE MARCHE

Facoltà di Ingegneria

# Cybersecurity research at Marche Polytechnic University

**Marco Baldi**
Dipartimento di Ingegneria dell’Informazione

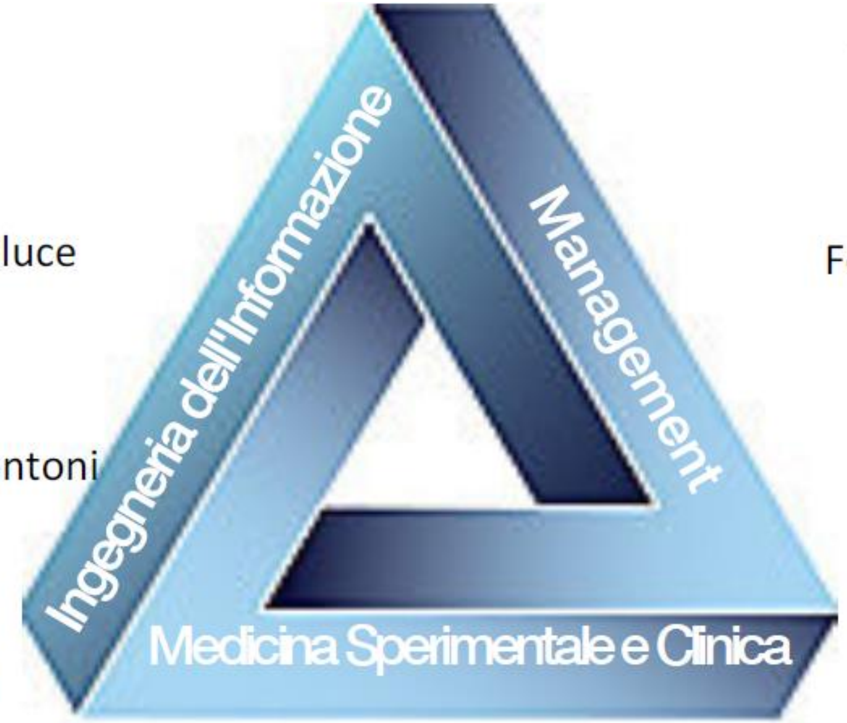
m.baldi@univpm.it
www.univpm.it/marco.baldi

- Marco Baldi

- Franco Chiaraluce

- Emanuele Frontoni

- Luca Spalazzi



- Antonio Di Stasi

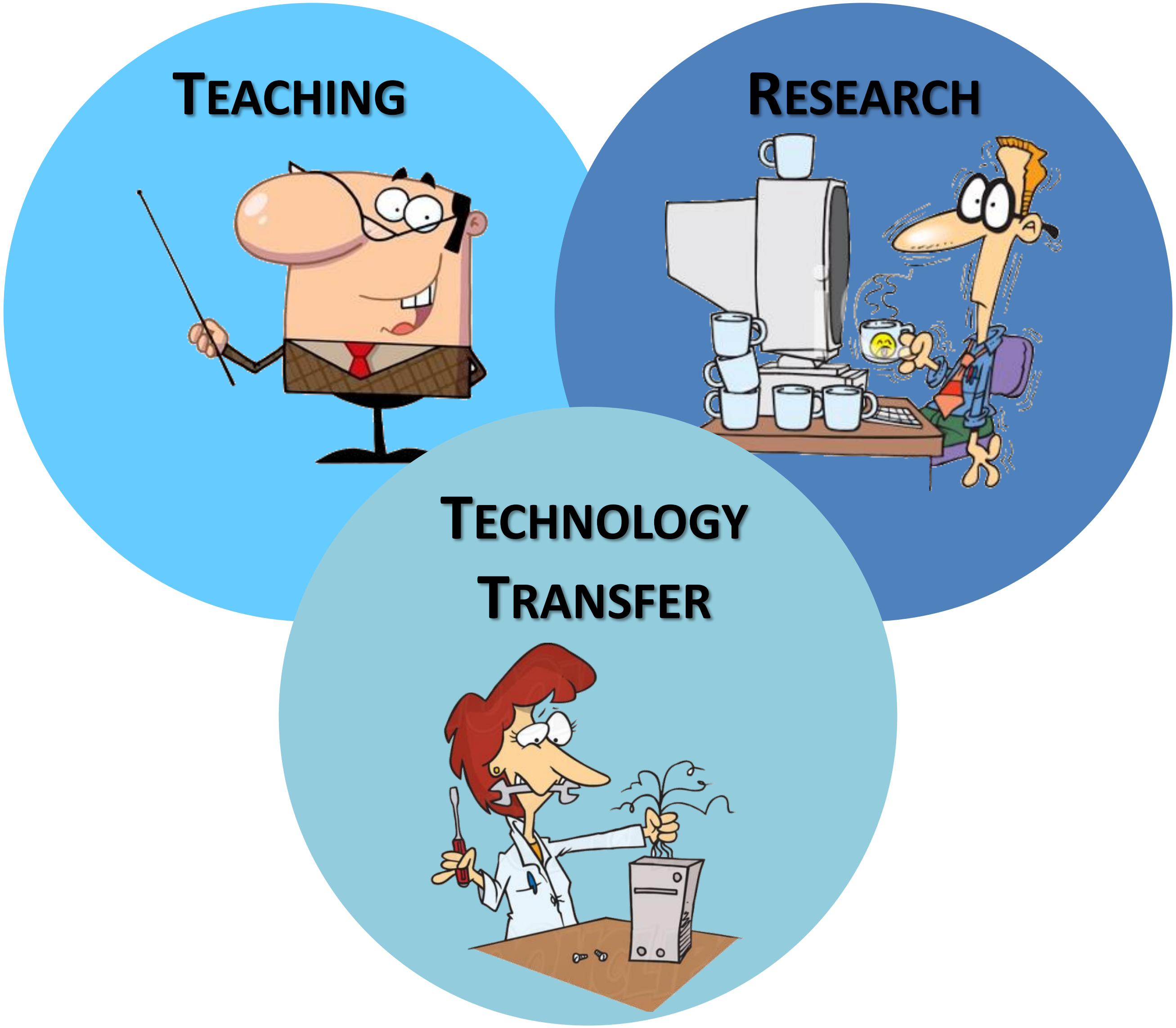
- Federica Pascucci

- Laura Torsello

- Maria Gabriella Ceravolo

- Fiorenzo Conti

# ACTIVITIES



TEACHING

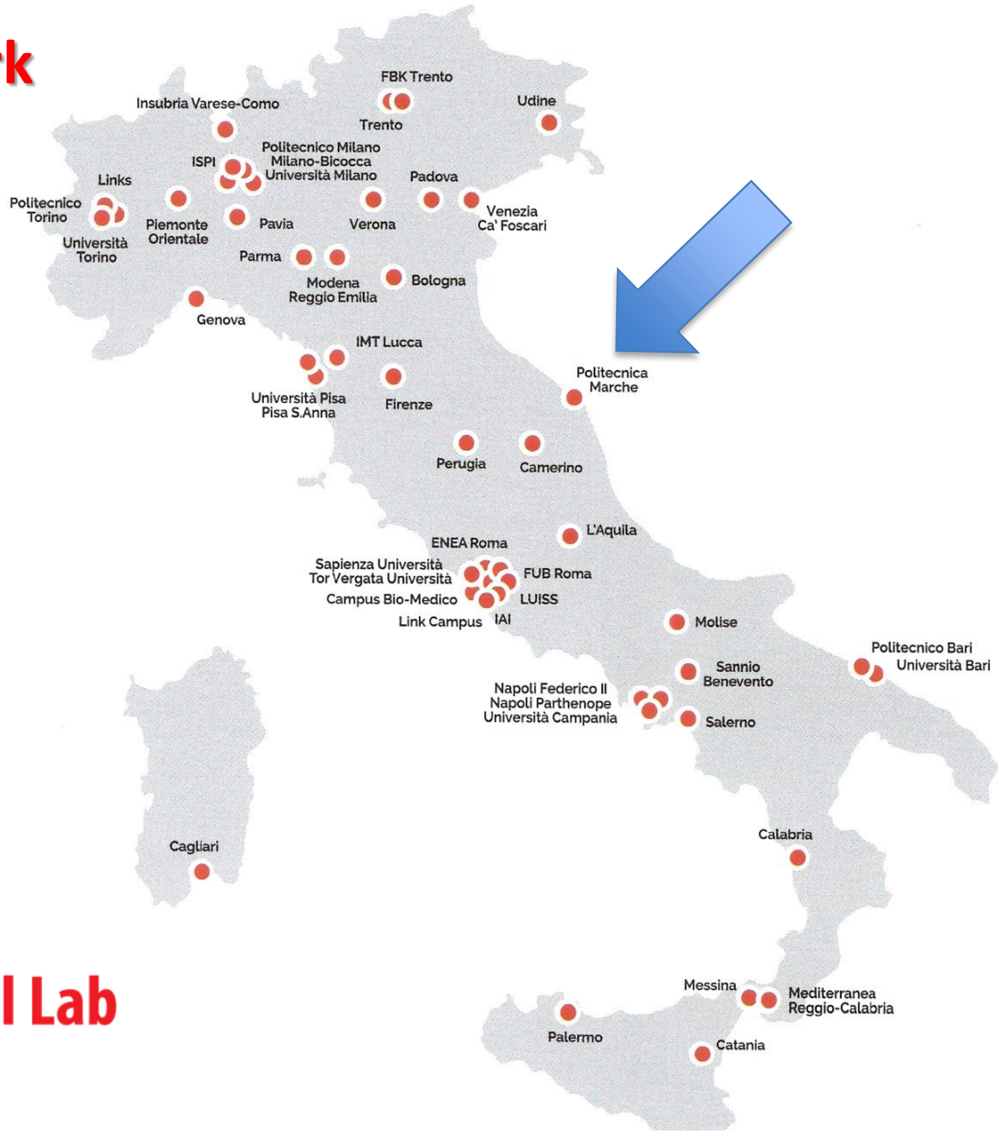
RESEARCH

TECHNOLOGY TRANSFER

# CINI - Cyber Security National Lab

## Italian excellence network on cybersecurity

- 240 Faculties
  - 68 Full Prof
  - 57 Ass. Prof
  - 100 Researchers
- 178 PhD students
- 76 postdocs
- 51 Experts



cini
Cyber Security National Lab

# CINI - Cyber Security National Lab

cini
Cyber Security National Lab

- **Scopes**:
  - – Increase national resilience to cyber threats
  - – Increase service continuity of critical systems
  - – Increase society awareness
  - – Enhance protection measures against cyber attacks by public administration and companies
  - – Support the development of national standards and frameworks

# ITALIAN CYBERSECURITY STRATEGY

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 gennaio 201

Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale. (13A02504)

(GU n.66 del 19-3-2013)

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

[illegible]

Decree Law 24/1/2013

Presidenza del Consiglio dei Ministri

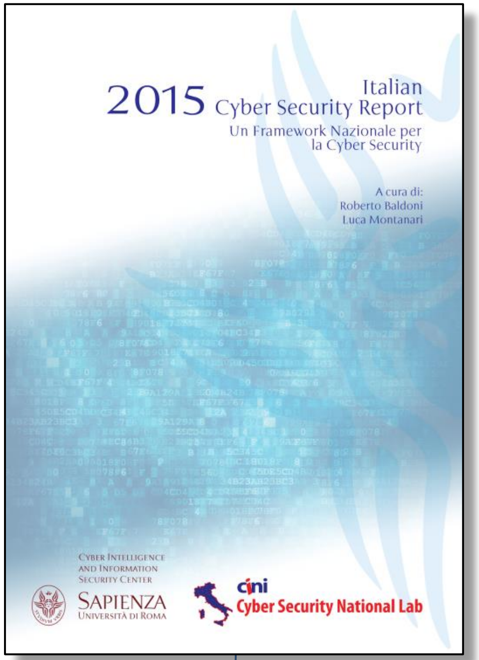
RNETICA
ATICA

Presidenza del Consiglio dei Ministri

QUADRO STRATEGICO NAZIONALE
PER LA SICUREZZA
DELLO SPAZIO CIBERNETICO

Dicembre 2013

National Strategy 27/12/2013



2015 Italian
Cyber Security Report
Un Framework Nazionale per
la Cyber Security

A cura di:
Roberto Baldoni
Luca Montanari

CYBER INTELLIGENCE
AND INFORMATION
SECURITY CENTER
SAPIENZA
UNIVERSITÀ DI ROMA

cini
Cyber Security National Lab

National Framework 4/2/2016

2016 Italian
Cybersecurity Report
Controlli Essenziali di Cybersecurity

a cura di:
Roberto Baldoni
Luca Montanari
Leonardo Querzoni

CYBER INTELLIGENCE
AND INFORMATION
SECURITY CENTER
SAPIENZA
UNIVERSITÀ DI ROMA

cini
Cybersecurity
National Lab

Essential Controls (Report 2016)

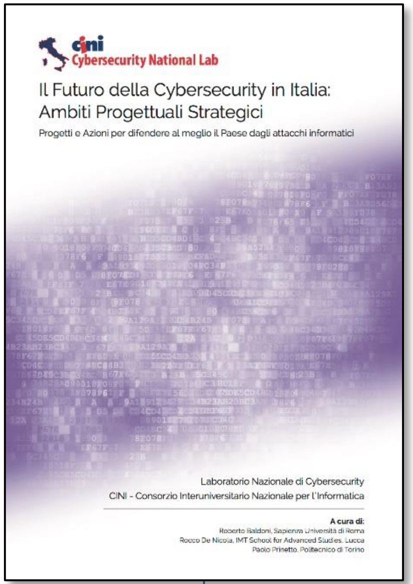
Presidenza del Consiglio dei Ministri

PIANO NAZIONALE
PER LA PROTEZIONE CIBERNETICA
E LA SICUREZZA INFORMATICA

Marzo 2017

Updating of the National Strategy (March 2017)

# ITALIAN CYBERSECURITY STRATEGY



cini
Cybersecurity National Lab

Il Futuro della Cybersecurity in Italia:
Ambiti Progettuali Strategici

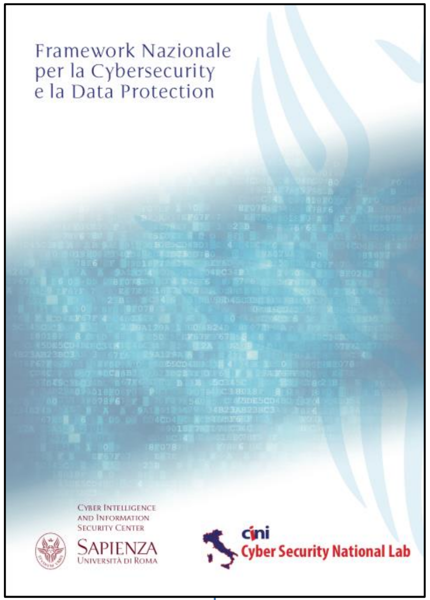
Progetti e Azioni per difendere al meglio il Paese dagli attacchi informatici

Laboratorio Nazionale di Cybersecurity
CINI - Consorzio Interuniversitario Nazionale per l'Informatica

**A cura di:**
Roberto Baldoni, Sapienza Università di Roma
Rocco De Nicola, IMT School for Advanced Studies, Lucca
Paolo Prinetto, Politecnico di Torino

White Book
(January 2018)

…



Framework Nazionale
per la Cybersecurity
e la Data Protection

CYBER INTELLIGENCE
AND INFORMATION
SECURITY CENTER

SAPIENZA
UNIVERSITÀ DI ROMA

cini
Cyber Security National Lab

National
Framework v2
(February 2019)

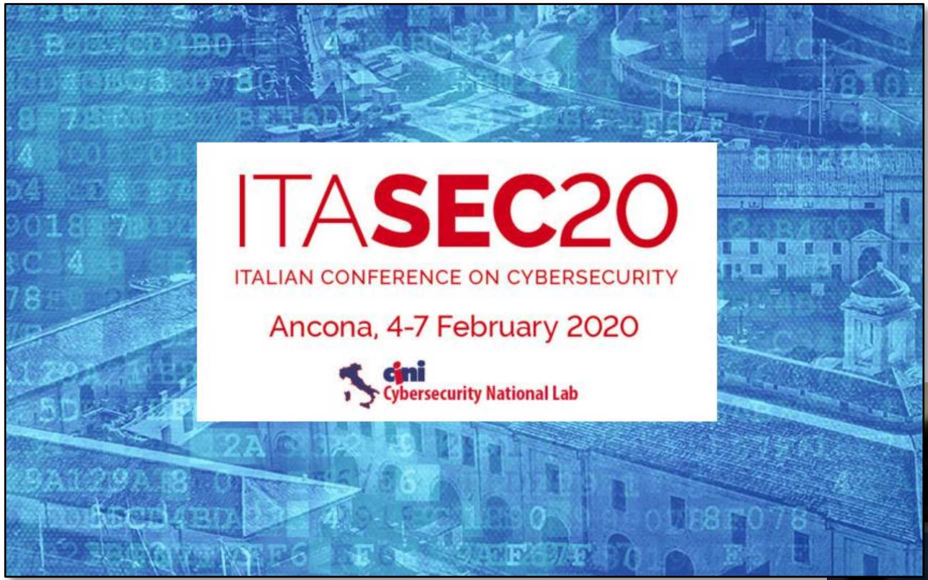
# CYBERCHALLENGE.IT

CYBER
CHALLENGE
CyberChallenge.IT

- National **ethical hacking** training and selection program

- **2020 (4th) edition**:
  - 4000+ candidates between 16 and 23 years old
  - 28 local nodes
  - 518 students selected
  - Italian Cyberdefender Team formed for the **European Cyber Security Challenge** (ECSC) organized by ENISA

# ITALIAN CYBERSECURITY CONFERENCE



ITASEC20

ITALIAN CONFERENCE ON CYBERSECURITY

Ancona, 4-7 February 2020

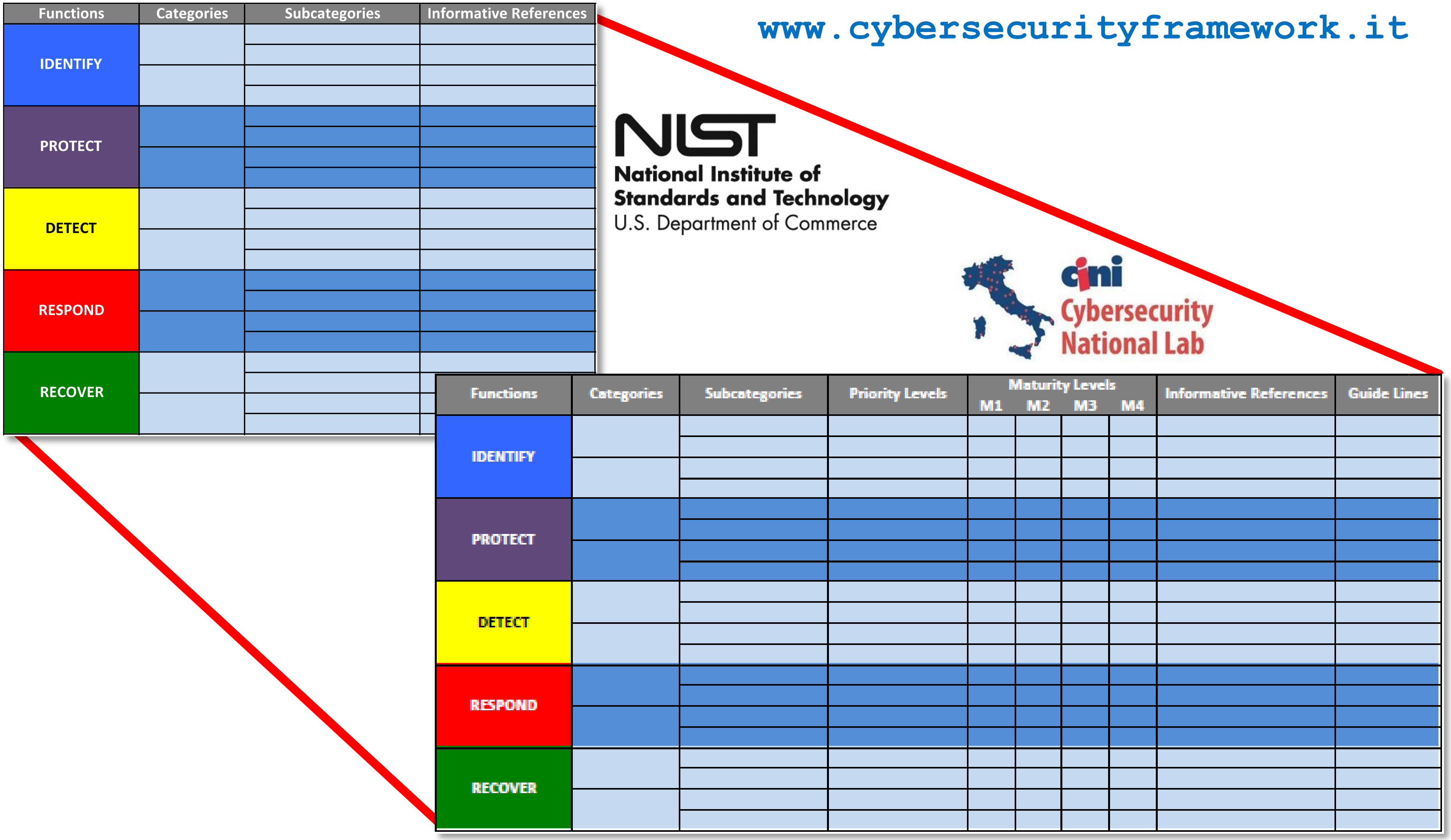
cini
Cybersecurity National Lab

# NATIONAL FRAMEWORK FOR CYBERSECURITY AND DATA PROTECTION

www.cybersecurityframework.it

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

cini
Cybersecurity National Lab



| Functions | Categories | Subcategories | Informative References |
|---|---|---|---|
| IDENTIFY | | | |
| | | | |
| | | | |
| | | | |
| PROTECT | | | |
| | | | |
| | | | |
| | | | |
| DETECT | | | |
| | | | |
| | | | |
| | | | |
| RESPOND | | | |
| | | | |
| | | | |
| | | | |
| RECOVER | | | |
| | | | |
| | | | |
| | | | |

| Functions | Categories | Subcategories | Priority Levels | Maturity Levels | | | | Informative References | Guide Lines |
|---|---|---|---|---|---|---|---|---|---|
| | | | | M1 | M2 | M3 | M4 | | |
| IDENTIFY | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| PROTECT | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| DETECT | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| RESPOND | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| RECOVER | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

# TOWARDS PRACTICAL QUANTUM COMPUTERS

- ***2017:***
  Google develops a 72-qubit quantum computer that reveals too difficult to control.

- ***January 2019:***
  IBM announces its Q System One with 20 qubits.

- ***October 2019:***
  Google announces that its Sycamore system with 53 qubits can perform in 200 seconds a computation that would require 10’000 years if executed over the world’s most powerful supercomputer.

- ***October 2020:***
  The IonQ startup announces a quantum computer with 32 qubits characterized by low error rates, which are needed for the technology to scale.

# QUANTUM-VULNERABLE CRYPTOGRAPHY

- The most widespread asymmetric cryptographic systems rely on mathematical problems that can be solved through **Shor's quantum algorithm**:

  - ***RSA***

    *(asymmetric cryptosystem based on integer factorization, used in SSL/TLS, online banking, ATM,…)*

  - ***ElGamal***

    *(asymmetric cryptosystem based on discrete logarithms, used in SSL/TLS,…)*

  - ***Diffie-Hellman***

    *(key exchange protocol based on discrete logarithms, used in SSL/TLS, NFC/contactless,…)*

  - ***ECC, DSA, ECDSA,…***

# POST-QUANTUM CRYPTOGRAPHY

- ***Asymmetric Cryptosystems:***
  - Based on lattices
  - Based on codes
  - Based on multivariate polynomials
  - Based on hash functions
  - Others (isogenies…)
- ***Symmetric Cryptosystems:***
  - Symmetric encryption schemes (AES…)
  - Hash functions (SHA…)

*Can still be used by taking into account* ***Grover's quantum algorithm***

# NIST PQcrypto Project

NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PROJECTS

Post-Quantum Cryptography

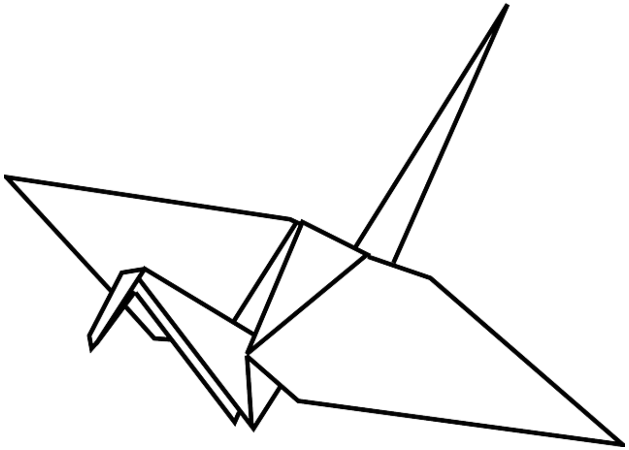
Since 2016, ***NIST*** has launched a standardization process for the definition of one or more asymmetric cryptographic algorithms to enrich:

- The ***FIPS 186-4*** recommendation (Digital Signature Standard - DSS)
- The ***SP 800-56A Rev 2*** special publication (key establishment systems based on the discrete logarithm)
- The ***SP 800-56B*** special publication (key establishment systems based on integer factorization)

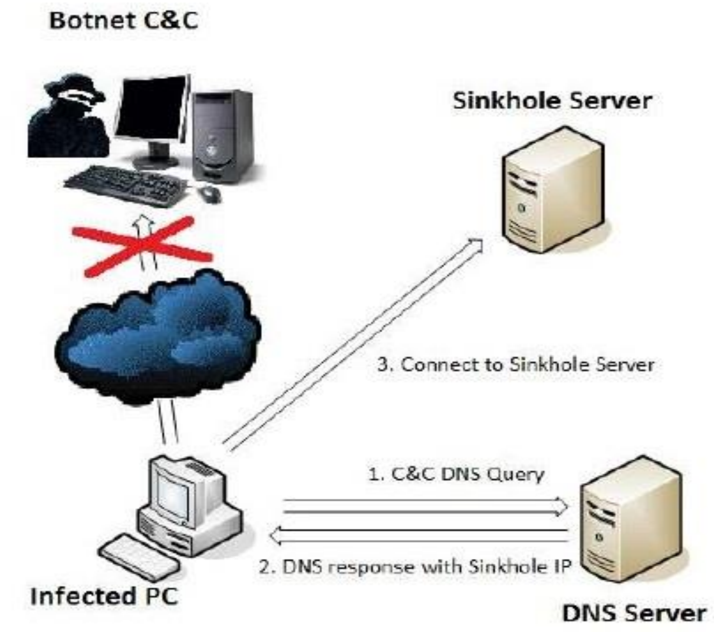
# LEDACRYPT

- The **UnivPM research unit** has been the first one to introduce post-quantum cryptosystems based on **QC-LDPC codes** in 2007/2008.

- **LEDAcrypt** (Low-dEnsity parity-check coDe-bAsed cryptographic systems) proposed by UnivPM jointly with PoliMI:
  - Suite of low-density parity-check code-based cryptosystems.
  - Among the ***26 second round candidates*** of the NIST competition.
  - Proposing team:
    - Marco Baldi (Univpm, Italy)
    - Alessandro Barenghi (Polimi, Italy)
    - Franco Chiaraluce (Univpm, Italy)
    - Gerardo Pelosi (Polimi, Italy)
    - Paolo Santini (Univpm, Italy)
  - Official website: https://www.ledacrypt.org/
  - Full ANSI-C99 codebase.



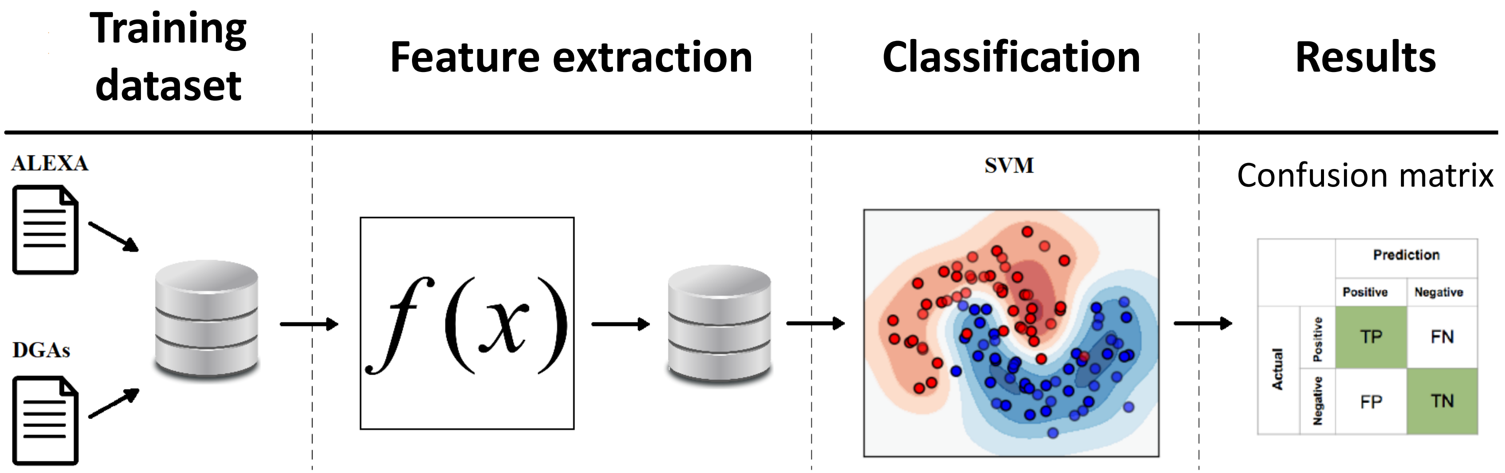
# RESEARCH ON MALWARE DETECTION



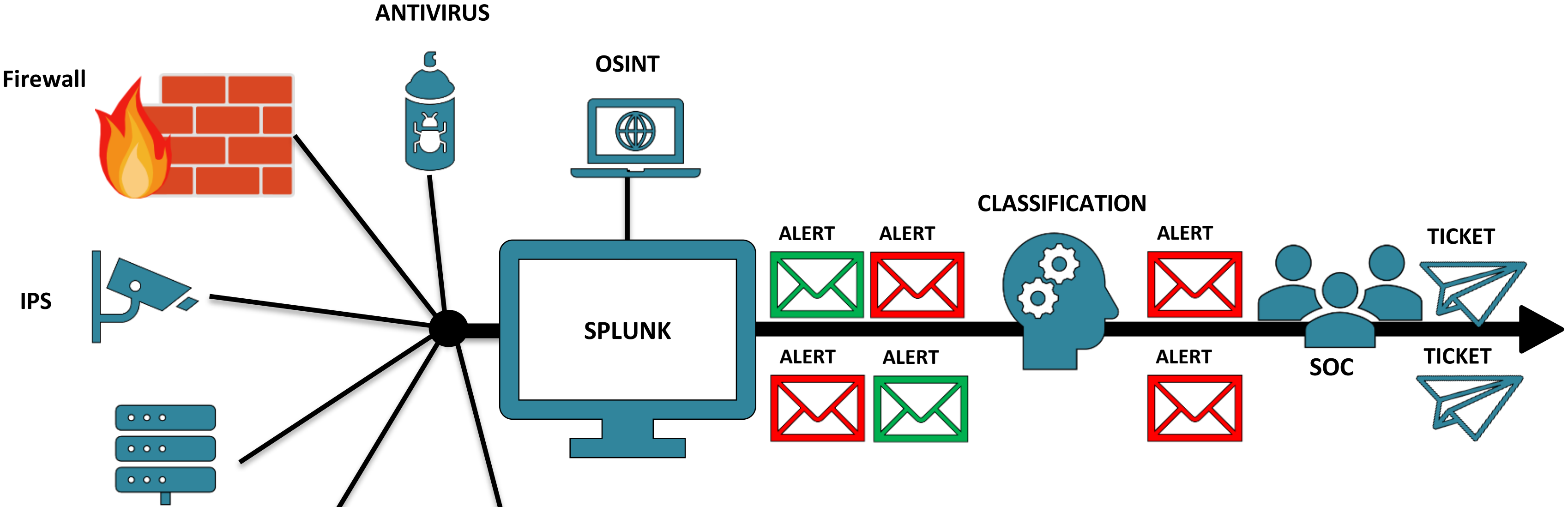
**Domain Generation Algorithm:**

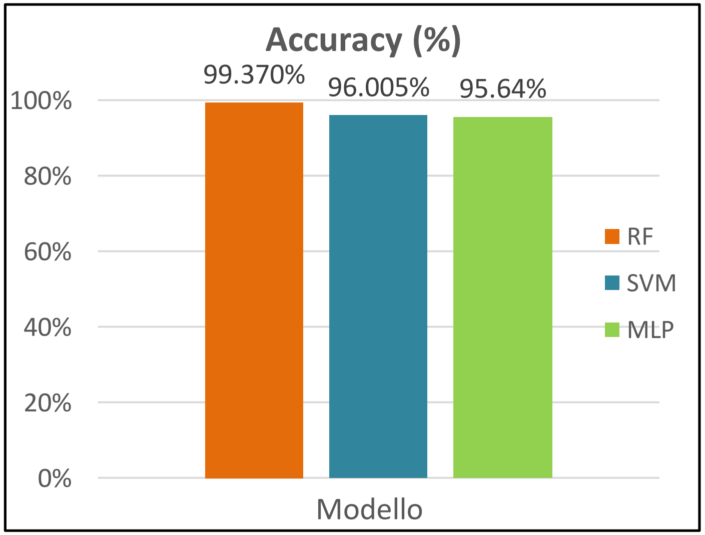
«ghrfkpaacxctha.com»
«bilabavemieqiq.net»
«tapigipjs.it»

**Analysis of DNS logs to identify DGA-created domains**



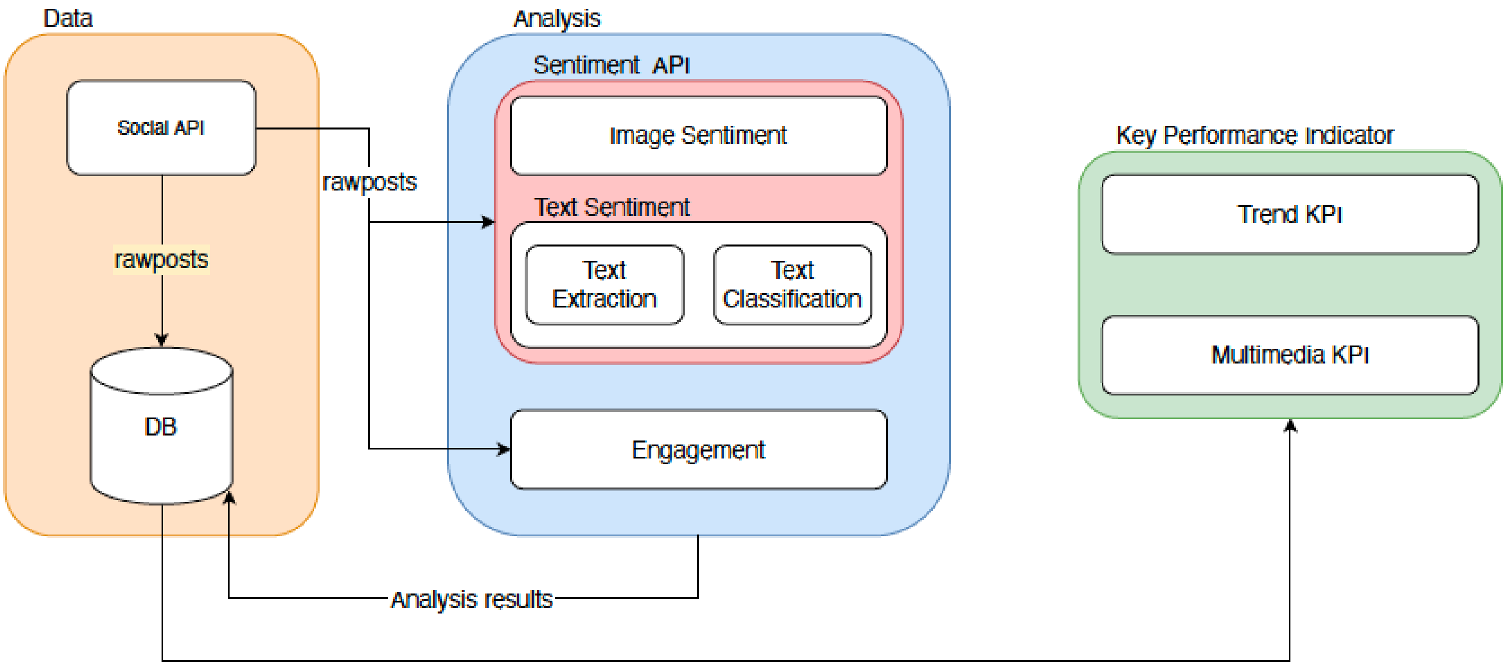
# Research on Incident Detection





Joint work with **Alessandro Cucchiarelli** and **Christian Morbidoni**

# Research on Social Media Intelligence



Data

Social API

rawposts

DB

rawposts

Analysis

Sentiment API

Image Sentiment

Text Sentiment

Text Extraction

Text Classification

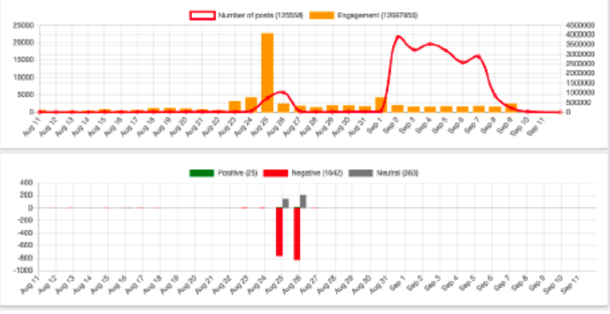
Engagement

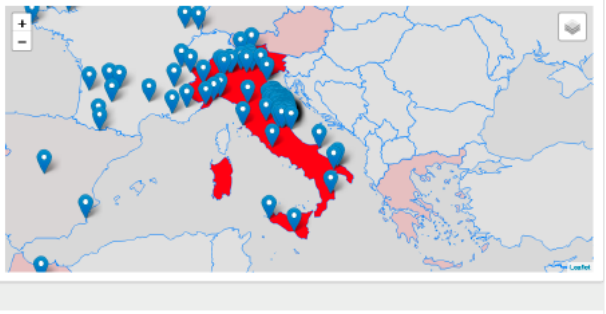
Analysis results

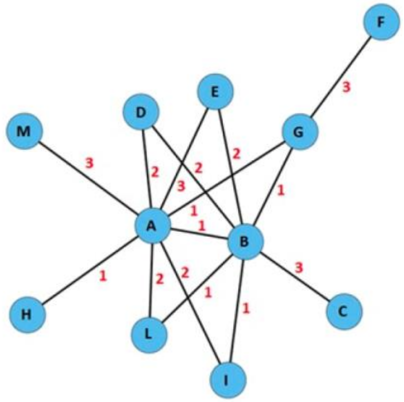
Key Performance Indicator

Trend KPI

Multimedia KPI

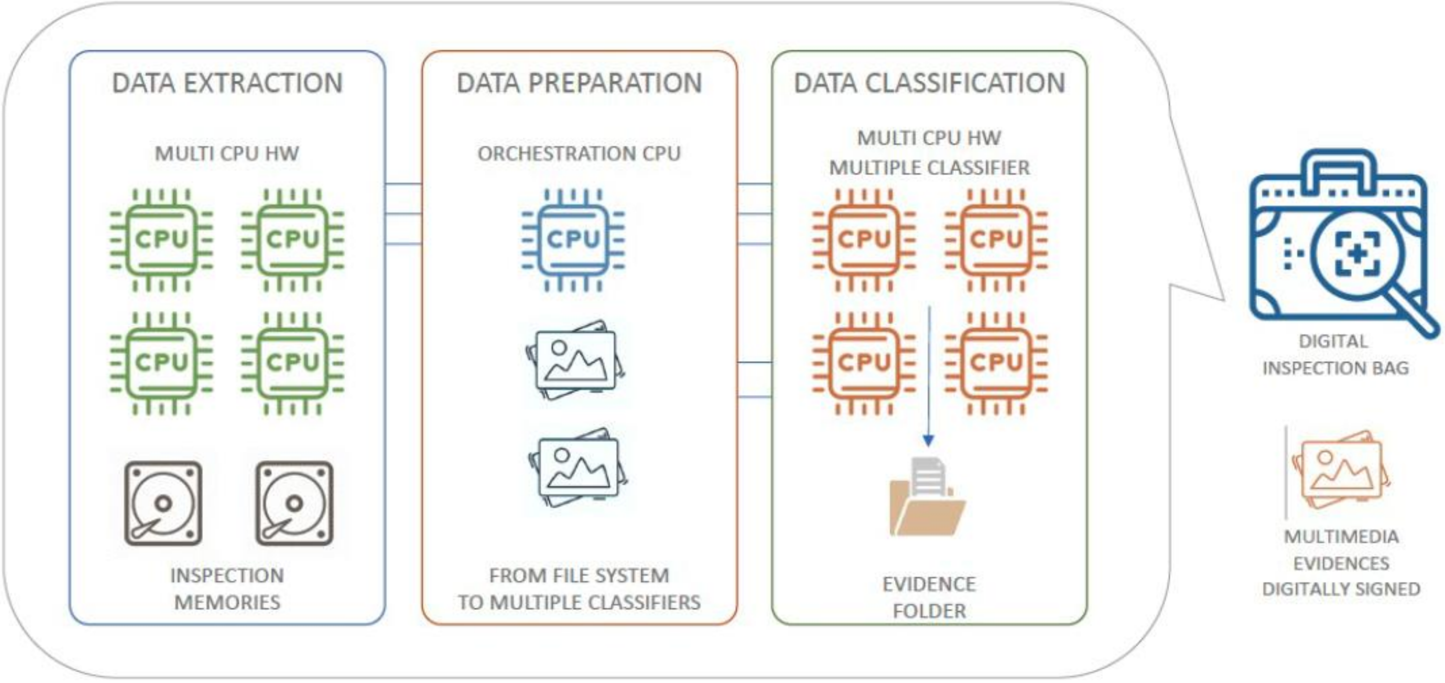






UNIVERSITÀ POLITECNICA DELLE MARCHE

# RESEARCH ON FORENSIC MULTIMEDIA CLASSIFICATION BASED ON AI & ML



DATA EXTRACTION

MULTI CPU HW

INSPECTION MEMORIES

DATA PREPARATION

ORCHESTRATION CPU

FROM FILE SYSTEM TO MULTIPLE CLASSIFIERS

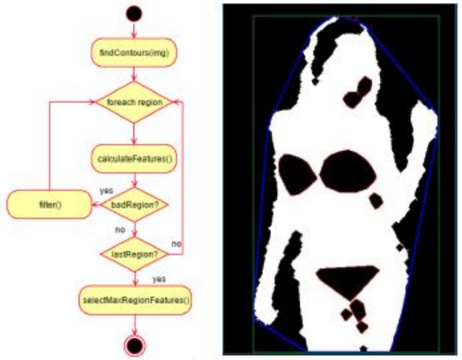
DATA CLASSIFICATION

MULTI CPU HW MULTIPLE CLASSIFIER

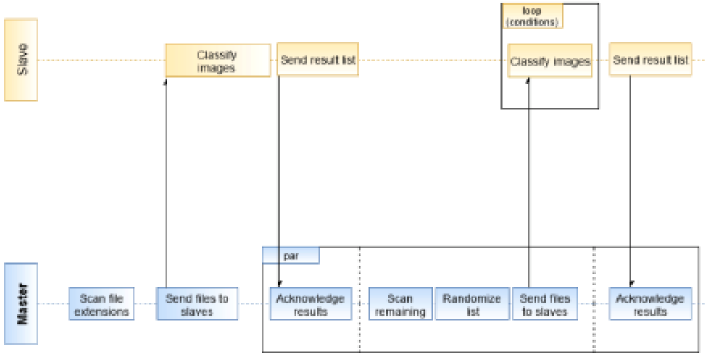
EVIDENCE FOLDER

DIGITAL INSPECTION BAG

MULTIMEDIA EVIDENCES DIGITALLY SIGNED

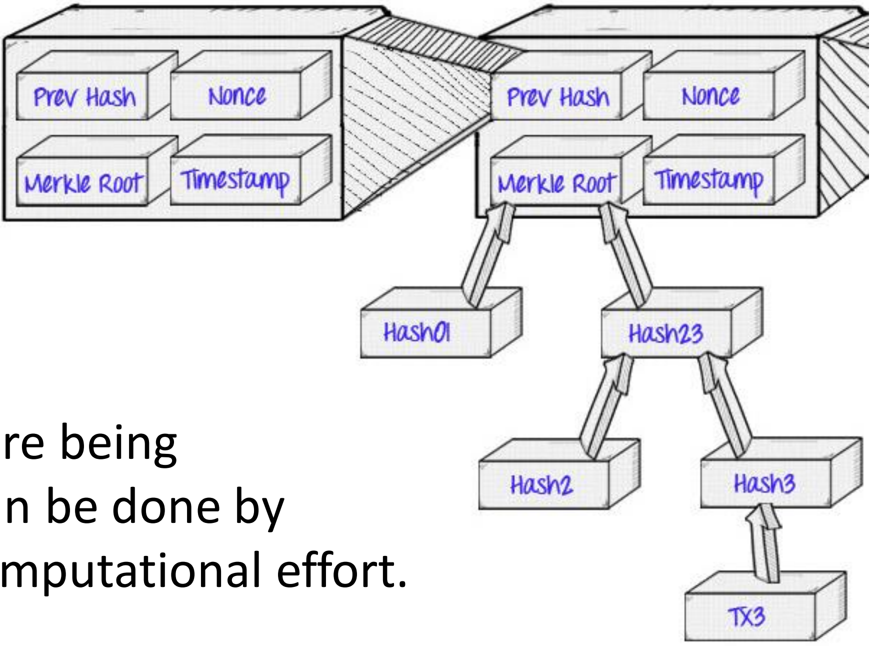


ML approach



Distributed architecture

# RESEARCH ON BLOCKCHAIN TECHNOLOGY



- Blockchains are **decentralized registers** created for cryptocurrencies, where data are written sequentially and immutably.

- Each added block **must be verified** before being appended to the blockchain, and this can be done by each user on the network with some computational effort.

- This makes blockchains new important tools for many applications where a **decentralized and immutable data infrastructure** is needed.

- **UnivPM** is working on the use of blockchain technology for user **authentication** and **security of biomedical data**.