INSTITUTE FOR SYSTEMS
AND COMPUTER ENGINEERING,
TECHNOLOGY AND SCIENCE

INESCTEC

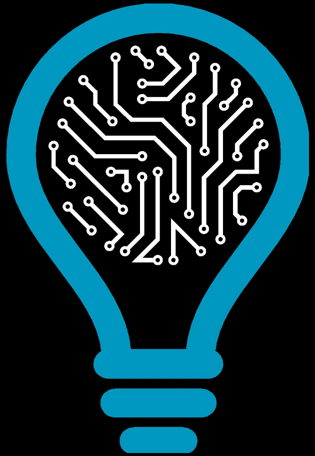
HIGH-ASSURANCE SOFTWARE LABORATORY

JANUARY 2022

from knowledge
generation to
science-based
innovation

- HASLab in brief
- Facts and figures
- CLOUDinha laboratory
- What we are doing now

HASLAB
IN BRIEF



WHAT WE DO

HASLab is focused on the **design and implementation of high-assurance software systems**: software that is correct by design and resilient to environment faults and malicious attacks

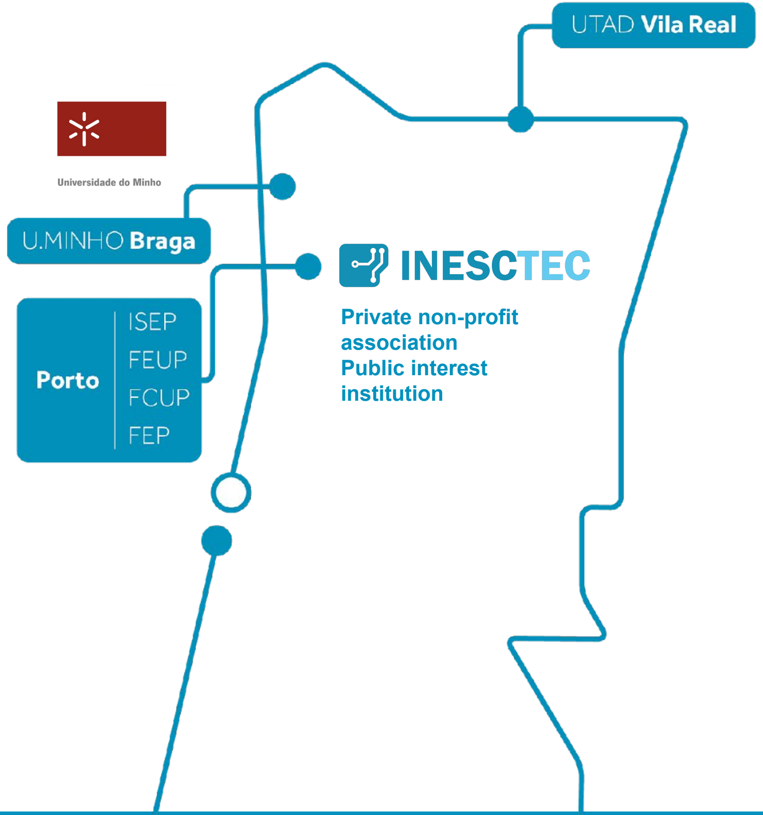
To accomplish this mission, HASLab covers three main research areas:

- **Distributed Systems**
- **Software Engineering**
- **Cyber Security**

The contributions of HASLab to these three main areas range **from fundamental research on formal methods and algorithms, to applied research on developing tools and middleware that address real-world demands stemming** from long-term collaborations with industry

WHERE WE ARE

HASLab is a research center of INESC TEC and the University of Minho - located at U,Minho, Braga



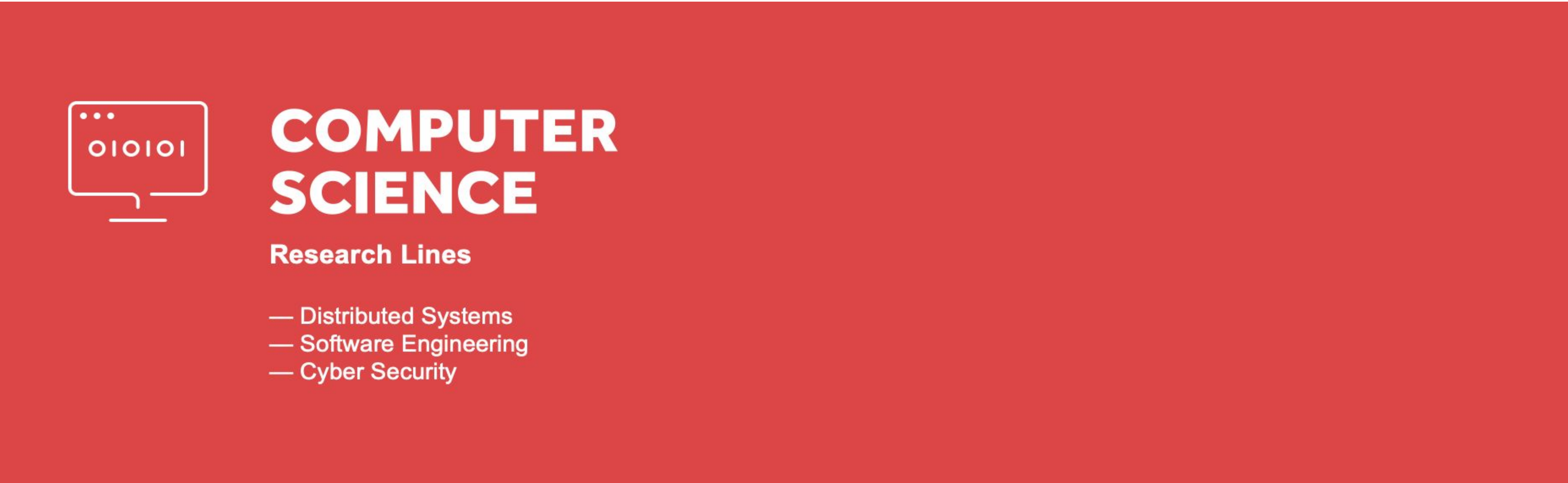
Private non-profit association
Public interest institution

WHO WE ARE

107	68	15	4
TOTAL MEMBERS	INTEGRATED RESEARCHERS	EXTERNAL RESEARCHERS	NATIONALITIES

RESEARCH LINES

To accomplish its mission, HASLab covers three main research lines within INESC TEC Computer Science domain



COMPUTER SCIENCE

Research Lines

— Distributed Systems
— Software Engineering
— Cyber Security

DISTRIBUTED SYSTEMS

- Efficient data management
- Large scale data storage and processing
- Distributed systems monitoring and benchmarking
- Secure data storage and processing

Target

- Cloud computing
- High-Performance computing
- Big Data applications: data analytics; machine/deep learning
- Blockchain

SOFTWARE ENGINEERING

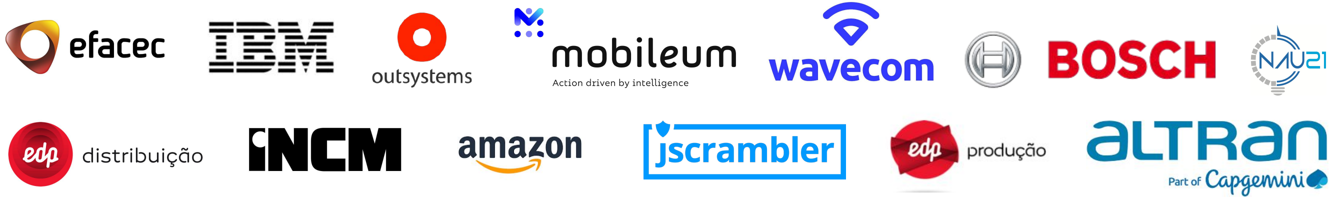
- Formal design and analysis of complex systems
- Static analysis and program verification
- Automatic testing and fault localisation
- Green computing
- Quantum computing
- Interface and usability

CYBER SECURITY

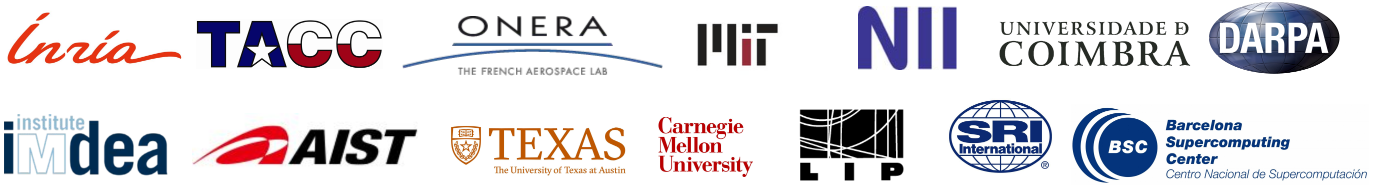
- Provable security
- Efficient and secure implementation of cryptographic software
- Formal verification of cryptography proofs and implementations
- Domain-specific software development tools for cryptography
- Privacy-enhancing data-management technologies

SOME OF OUR PARTNERS

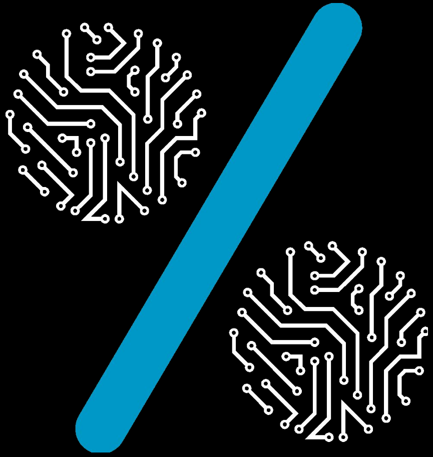
Industry



Academia


Inria
TACC
ONERA
THE FRENCH AEROSPACE LAB
MIT
NII
UNIVERSIDADE D COIMBRA
DARPA
institute IMdea
AIST
TEXAS
The University of Texas at Austin
Carnegie Mellon University
LIP
SRI International
BSC
Barcelona Supercomputing Center
Centro Nacional de Supercomputación

FACTS
AND FIGURES



R&D PROJECTS | 2021

National R&D Programmes | **11**
EU Programmes | **5**
R&D Services & Consulting | **10**
Other Funding Programmes | **3**

> 25 Ongoing R&D Projects

INDEXED PUBLICATIONS | 2021

INDEXED PUBLICATIONS

> 5 conference papers were published in CORE 2021 A* conference
> 4 journal publications were published in Quartile 1

15 Indexed Journal Papers
30 Indexed Conference Articles
3 Concluded PhD Theses – Supervised
21 Ongoing PhD Theses - Supervised

SHARING R&D RESULTS

4 Conferences, workshops and scientific sessions
2 Advanced training courses organised
5 Editorial roles in journals
21 Participation in program committees
5 Participation in fairs and industrial events

INNOVATION

1

PATENT GRANTED
IN 2019

2

INVENTION DISCLOSURES
IN 2020

keyruptive

Keyruptive Technologies

Mobile app solution for secure cloud storage and management of digital assets such as cryptocurrency.

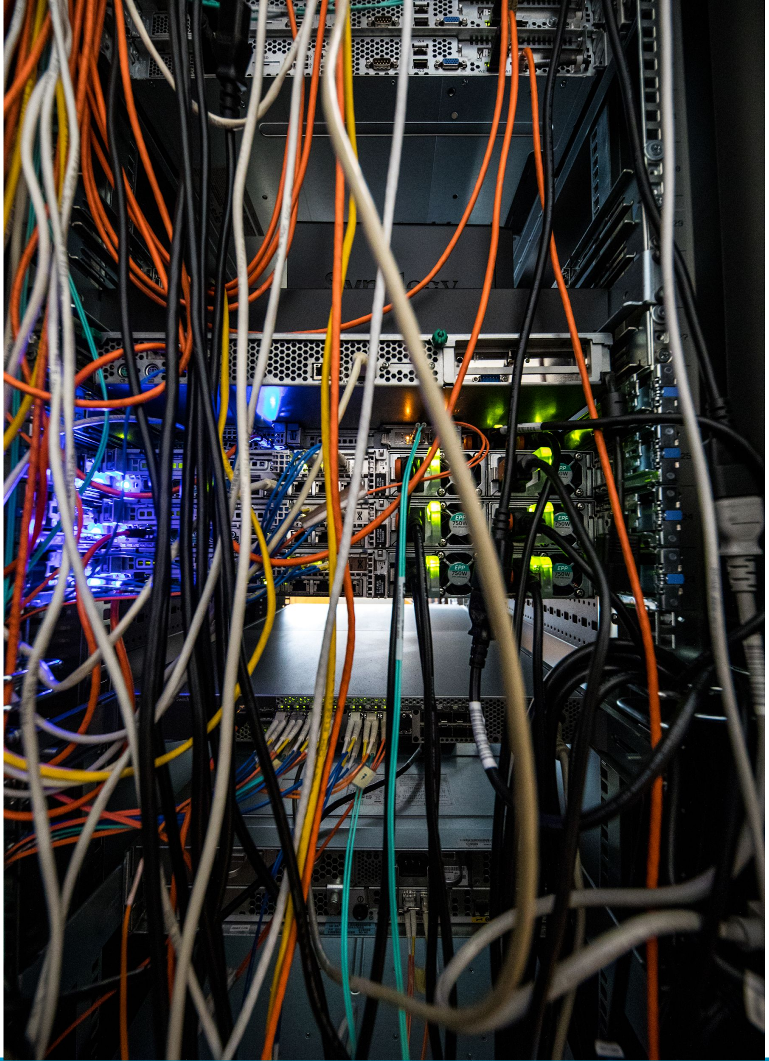
Keyruptive obtained a software patent in the United States of America

CLOUDINHA LABORATORY

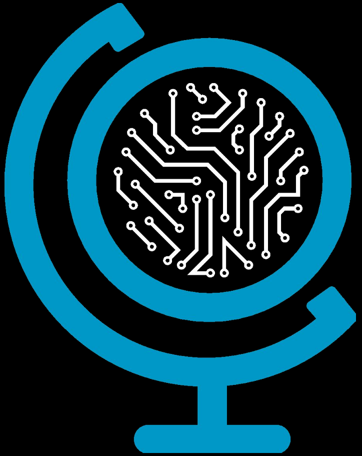
CLOUDINHA LABORATORY

CLOUDInha is a cluster of servers that provides **computational and storage support for research, development and education** conducted at INESC TEC and University of Minho

Users have access to a bare-metal infrastructure composed by more than **100 servers**, connected through a **10 Gb network**, and with an aggregated computational power of **290 computing cores, 1.8 TB of RAM, and 41.28 TB of storage**



WHAT WE ARE DOING NOW



BIGHPC PROJECT
DISTRIBUTED SYSTEMS

- Improve the monitoring of heterogeneous HPC infrastructures
  - Large-scale setup
  - Unified framework and metrics (jobs, compute nodes, storage nodes)

- Improve the deployment of Big Data applications and the management of HPC computational resources
  - Containerization technologies (e.g., singularity, charlie cloud)

- Improve storage performance and management for HPC services
  - Alleviate I/O pressure at the shared parallel file system
  - Improve Quality of Service

- https://bighpc.wavecom.pt

Partners:

INESCTEC

LIP

TEXAS
The University of Texas at Austin

MACC Minho Advanced Computing Center

TACC

wavecom

Funding:

Cofinanciado por:
COMPETE 2020

Lisb@20²⁰

PORTUGAL 2020

UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

FCT Fundação para a Ciência e a Tecnologia

UTAustin Portugal

PASTOR PROJECT
DISTRIBUTED SYSTEMS

- Improve storage performance for AI frameworks
    - E.g., TensorFlow, Pytorch, …
- Novel Software-Defined Storage (SDS) solution
    - reusable storage optimizations for AI applications (e.g., caching, tiering, QoS)
    - holistic visibility and automatic configuration of storage resources
    - easy integration with existing HPC software and hardware
- https://pastor-project.github.io

Partners

INESCTEC

TACC

MACC Minho Advanced Computing Center

HOOD COLLEGE

Funding

FCT Fundação para a Ciência e a Tecnologia

UTAustin Portugal

GOVERNO DE PORTUGAL

CENTRA
DISTRIBUTED SYSTEMS

- CENTRA - Collaborations to Enable Transnational Cyberinfrastructure Applications
- Partners from Europe, US and Asia
- Efficient and Secure Data Management for HPC and Cloud Computing
  - Optimize the performance and dependability of data-centric applications (e.g., databases, data analytics, ML)
  - Privacy-by-design approach for storing and processing data at third-party infrastructures
  - https://www.globalcentra.org/projects/#prv

AIDA PROJECT
DISTRIBUTED SYSTEMS

AIDA will provide **highly-configurable and rich data collection** and **monitoring, while preserving the current real-time, security and dependability** guarantees of the RAID platform:

https://aida.inesctec.pt/

DATA PRIVACY AND CONFIDENTIALITY

EDGE COMPUTING AND 5G

RESILIENCE TO INTRUSION

FEDERATED MACHINE LEARNING

Partners:

mobileum

INESCTEC

1 2 9 0

UNIVERSIDADE Ð COIMBRA

Carnegie Mellon University

Funding:

Cofinanciado por:

COMPETE 2020

PORTUGAL 2020

UNIÃO EUROPEIA
Fundo Europeu
de Desenvolvimento Regional

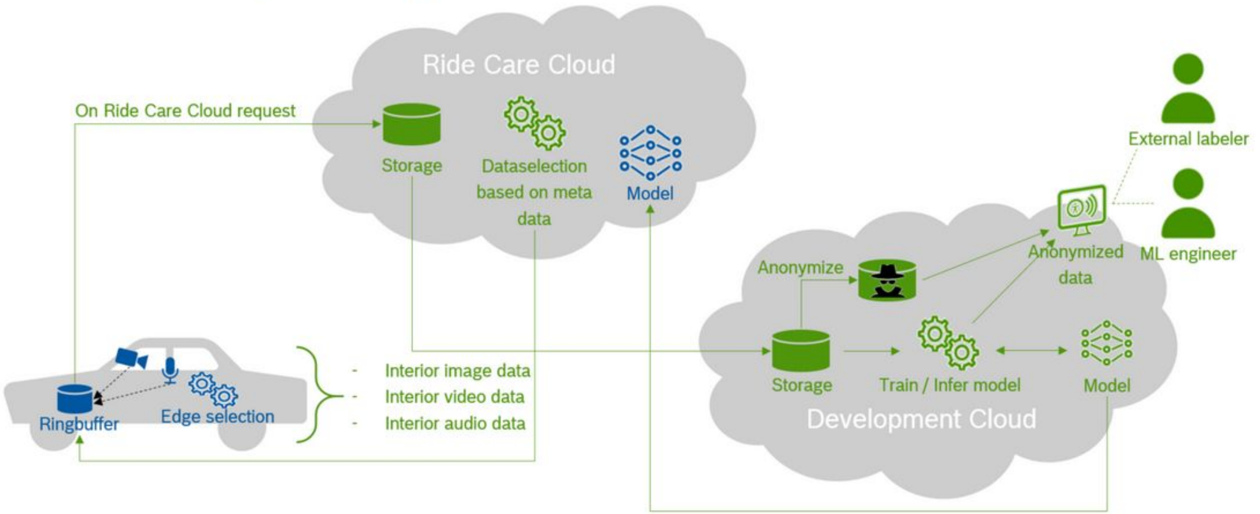
FCT Fundação para a Ciência e a Tecnologia

Carnegie Mellon Portugal

AURORA PROJECT
DISTRIBUTED SYSTEMS

Universidade do Minho

- Data management optimization, in the car itself and in the cloud.
    - In the cloud focus on data management and optimization in generic workloads and in optimizations for ML/DL workloads.
    - Privacy-preserving data management and processing.



SUSTAINABLE PROJECT
DISTRIBUTED SYSTEMS

SUSTAINABLE
HPC

- National project to develop and testing innovative solutions to enable maximizing the sustainability of operating facilities for advanced computing and data centers
  - taking advantage of the Deucalion supercomputer
- Laboratory with a diverse set of energy conversion sources (electricity and thermal) both from the point of view of generation and storage
- Reduction of electric energy consumption by using predictive management algorithms and implementation of different energy efficiency measures

INTERCONNECT PROJECT
DISTRIBUTED SYSTEMS

- Cross-domain interoperability with semantic data exchange for IoT
- Neutral Data Marketplaces and Hubs for data exchange
- Blockchain-based solutions to assist data management
- Applied data management and privacy preserving capabilities to high TRL solutions and very large-scale demonstrations

interconnect

MACC
DISTRIBUTED SYSTEMS

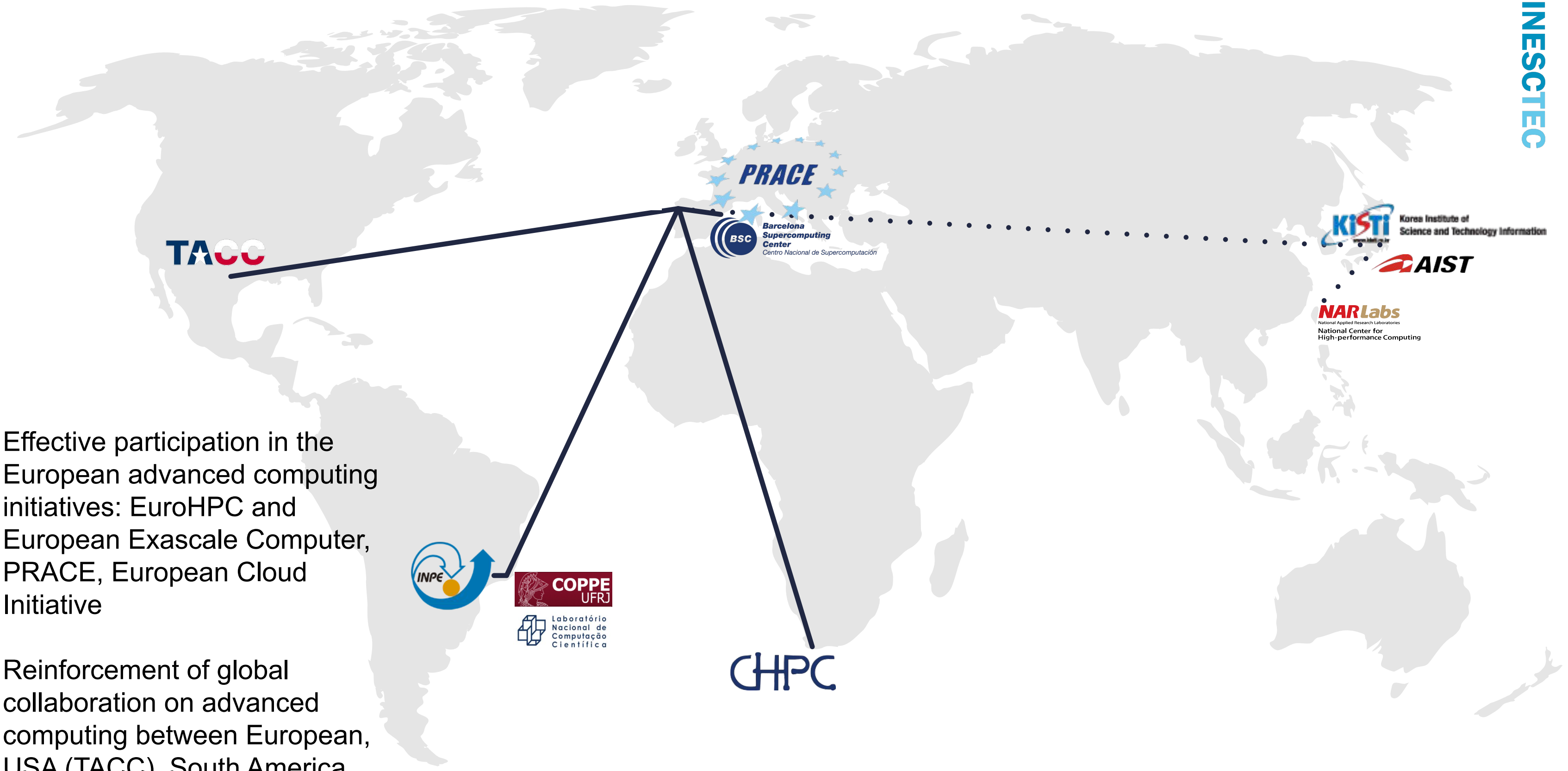
Minho
Advanced
Computing
Center

- National collaborative infrastructure to promote and support Open Science initiatives on supercomputing, data science and visualization;

- Sustainable computing and data infrastructure catering to national scientific and industrial communities and complementary to international partners;

- https://macc.fccn.pt/

- RNCA, https://rnca.fccn.pt


TACC
PRACE
BSC
Barcelona Supercomputing Center
Centro Nacional de Supercomputación
KISTI
Korea Institute of Science and Technology Information
AIST
NARLabs
National Applied Research Laboratories
National Center for High-performance Computing
INPE
COPPE UFRJ
Laboratório Nacional de Computação Científica
CHPC

- Effective participation in the European advanced computing initiatives: EuroHPC and European Exascale Computer, PRACE, European Cloud Initiative

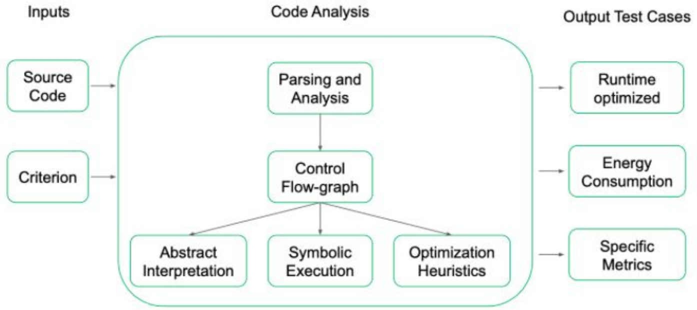
- Reinforcement of global collaboration on advanced computing between European, USA (TACC), South America (LNCC) and Asia (PRAGMA) facilities

SOFTWARE QUALITY
SOFTWARE ENGINEERING

- Green Computing:
  - Measure/estimate energy consumption;
  - Detect energy smells;
  - Recommend energy-friendly software practices;

- Software Testing and Analysis:
  - Fault Localization;
  - Program repair;
  - Automatic Generation of Program Executions;
  - Software Metrics.

Automatic Generation of Program Executions



GREEN COMPUTING

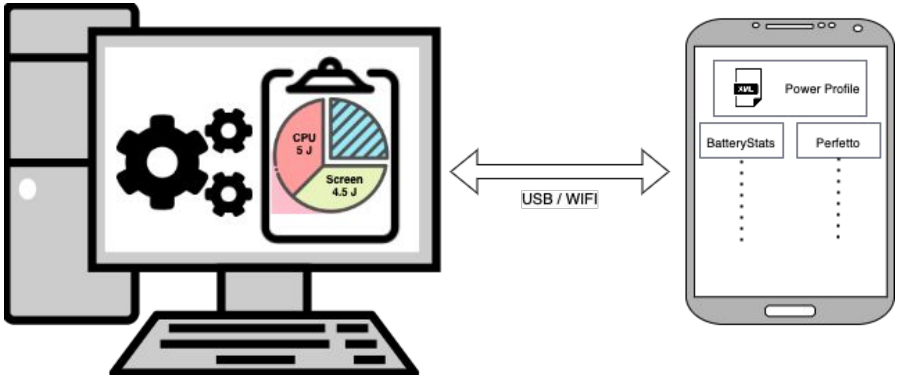
Measure/Estimate Energy Consumption

E-MANAFA: Energy Monitor and ANAlyzer For Android

- Compatible with any Android device;

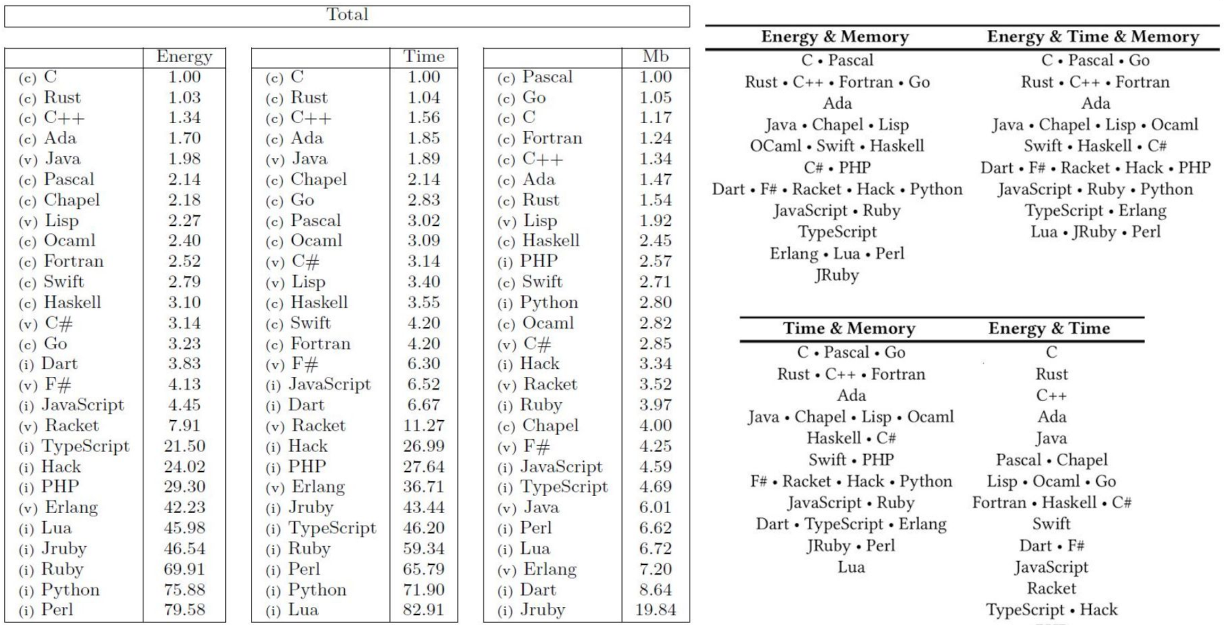
- Fine-grained component-level energy measurements;

https://github.com/RRua/e-manafa



GREEN COMPUTING

Energy Efficiency Across Programming Languages



Total

	Energy		Time		Mb
(c) C	1.00	(c) C	1.00	(c) Pascal	1.00
(c) Rust	1.03	(c) Rust	1.04	(c) Go	1.05
(c) C++	1.34	(c) C++	1.56	(c) C	1.17
(c) Ada	1.70	(c) Ada	1.85	(c) Fortran	1.24
(v) Java	1.98	(v) Java	1.89	(c) C++	1.34
(c) Pascal	2.14	(c) Chapel	2.14	(c) Ada	1.47
(c) Chapel	2.18	(c) Go	2.83	(c) Rust	1.54
(v) Lisp	2.27	(c) Pascal	3.02	(v) Lisp	1.92
(c) Ocaml	2.40	(c) Ocaml	3.09	(c) Haskell	2.45
(c) Fortran	2.52	(v) C#	3.14	(i) PHP	2.57
(c) Swift	2.79	(v) Lisp	3.40	(c) Swift	2.71
(c) Haskell	3.10	(c) Haskell	3.55	(i) Python	2.80
(v) C#	3.14	(c) Swift	4.20	(c) Ocaml	2.82
(c) Go	3.23	(c) Fortran	4.20	(v) C#	2.85
(i) Dart	3.83	(v) F#	6.30	(i) Hack	3.34
(v) F#	4.13	(i) JavaScript	6.52	(v) Racket	3.52
(i) JavaScript	4.45	(i) Dart	6.67	(i) Ruby	3.97
(v) Racket	7.91	(v) Racket	11.27	(c) Chapel	4.00
(i) TypeScript	21.50	(i) Hack	26.99	(v) F#	4.25
(i) Hack	24.02	(i) PHP	27.64	(i) JavaScript	4.59
(i) PHP	29.30	(v) Erlang	36.71	(i) TypeScript	4.69
(v) Erlang	42.23	(i) Jruby	43.44	(v) Java	6.01
(i) Lua	45.98	(i) TypeScript	46.20	(i) Perl	6.62
(i) Jruby	46.54	(i) Ruby	59.34	(i) Lua	6.72
(i) Ruby	69.91	(i) Perl	65.79	(v) Erlang	7.20
(i) Python	75.88	(i) Python	71.90	(i) Dart	8.64
(i) Perl	79.58	(i) Lua	82.91	(i) Jruby	19.84

Energy & Memory	Energy & Time & Memory
C • Pascal	C • Pascal • Go
Rust • C++ • Fortran • Go	Rust • C++ • Fortran
Ada	Ada
Java • Chapel • Lisp	Java • Chapel • Lisp • Ocaml
OCaml • Swift • Haskell	Swift • Haskell • C#
C# • PHP	Dart • F# • Racket • Hack • PHP
Dart • F# • Racket • Hack • Python	JavaScript • Ruby • Python
JavaScript • Ruby	TypeScript • Erlang
TypeScript	Lua • JRuby • Perl
Erlang • Lua • Perl	
JRuby	

Time & Memory	Energy & Time
C • Pascal • Go	C
Rust • C++ • Fortran	Rust
Ada	C++
Java • Chapel • Lisp • Ocaml	Ada
Haskell • C#	Java
Swift • PHP	Pascal • Chapel
F# • Racket • Hack • Python	Lisp • Ocaml • Go
JavaScript • Ruby	Fortran • Haskell • C#
Dart • TypeScript • Erlang	Swift
JRuby • Perl	Dart • F#
Lua	JavaScript
	Racket
	TypeScript • Hack
	PHP
	Erlang
	Lua • JRuby
	Ruby

- sites.google.com/view/energy-efficiency-languages

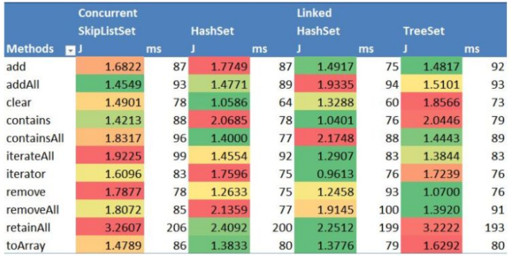
or

- greenlab.di.uminho.pt

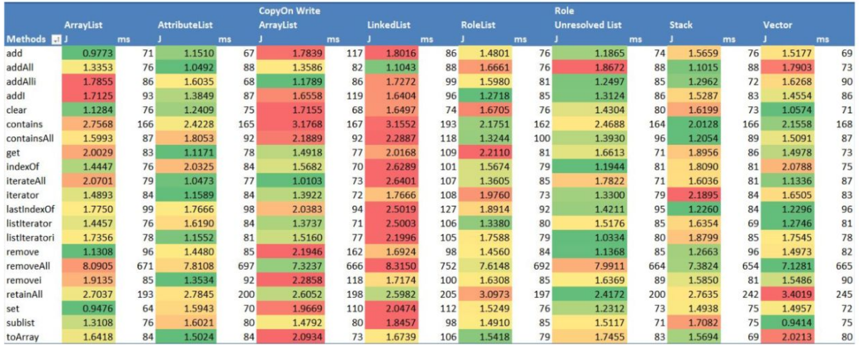
GREEN COMPUTING

Energy Efficiency of Programming Practices

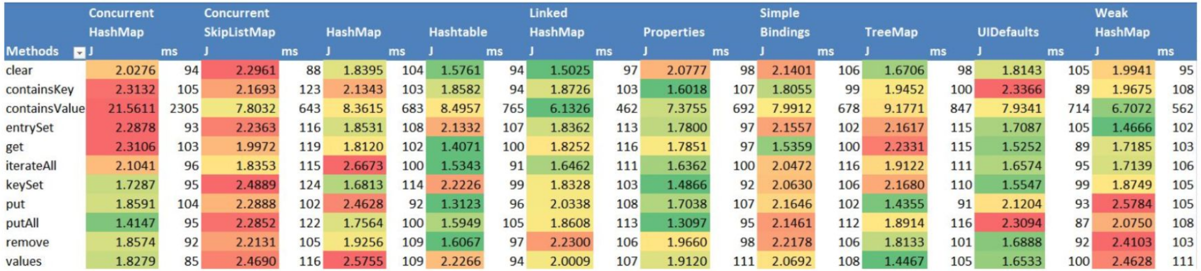
Results (25k pop)



	Concurrent				Linked			
	SkipListSet		HashSet		HashSet		TreeSet	
Methods	J	ms	J	ms	J	ms	J	ms
add	1.6822	87	1.7749	87	1.4917	75	1.4817	92
addAll	1.4549	93	1.4771	89	1.9335	94	1.5101	93
clear	1.4901	78	1.0586	64	1.3288	60	1.8566	73
contains	1.4213	88	2.0685	78	1.0401	76	2.0446	79
containsAll	1.8317	96	1.4000	77	2.1748	88	1.4443	89
iterateAll	1.9225	99	1.4554	92	1.2907	83	1.3844	83
iterator	1.6096	83	1.7596	75	0.9613	76	1.7239	76
remove	1.7877	78	1.2633	75	1.2458	93	1.0700	76
removeAll	1.8072	85	2.1359	77	1.9145	100	1.3920	91
retainAll	3.2607	206	2.4092	200	2.2512	199	3.2222	193
toArray	1.4789	86	1.3833	80	1.3776	79	1.6292	80



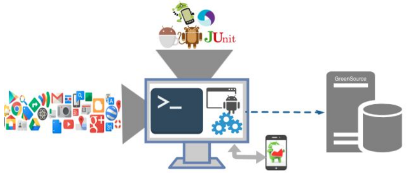
					CopyOn Write						Role					
	ArrayList		AttributeList		ArrayList		LinkedList		RoleList		Unresolved List		Stack		Vector	
Methods	J	ms	J	ms	J	ms	J	ms	J	ms	J	ms	J	ms	J	ms
add	0.9773	71	1.1510	67	1.7839	117	1.8016	86	1.4801	76	1.1865	74	1.5659	76	1.5177	69
addAll	1.3353	76	1.0492	88	1.3586	82	1.1043	88	1.6661	76	1.8672	88	1.1015	88	1.7903	73
addAlli	1.7855	86	1.6035	68	1.1789	86	1.7272	99	1.5980	81	1.2497	85	1.2962	72	1.6268	90
addI	1.7125	93	1.3849	87	1.6558	119	1.6404	96	1.2718	85	1.3124	86	1.5287	83	1.4554	86
clear	1.1284	76	1.2409	75	1.7155	68	1.6497	74	1.6705	76	1.4304	80	1.6199	73	1.0574	71
contains	2.7568	166	2.4228	165	3.1768	167	3.1552	193	2.1751	162	2.4688	164	2.0128	166	2.1558	168
containsAll	1.5993	87	1.8053	92	2.1889	92	2.2887	118	1.3244	100	1.3930	96	1.2054	89	1.5091	87
get	2.0029	83	1.1171	78	1.4918	77	2.0168	109	2.2110	81	1.6613	71	1.8956	86	1.4978	73
indexOf	1.4447	76	2.0325	84	1.5682	70	2.6289	101	1.5674	79	1.1944	81	1.8090	81	2.0788	75
iterateAll	2.0701	79	1.0473	77	1.0103	73	2.6401	107	1.3605	85	1.7822	71	1.6036	81	1.1336	87
iterator	1.4893	84	1.1589	84	1.3922	72	1.7666	108	1.9760	73	1.3300	79	2.1895	84	1.6505	83
lastIndexOf	1.7750	99	1.7666	98	2.0383	94	2.5019	127	1.8914	92	1.4211	95	1.2260	84	1.2296	96
listIterator	1.4457	76	1.6190	84	1.3737	71	2.5003	106	1.3380	80	1.5176	85	1.6354	69	1.2746	81
listIteratori	1.7356	78	1.1552	81	1.5160	77	2.1996	105	1.7588	79	1.0334	80	1.8799	85	1.7545	78
remove	1.1308	96	1.4480	85	2.1946	162	1.6924	98	1.4560	84	1.1368	85	1.2663	96	1.4973	82
removeAll	8.0905	671	7.8108	697	7.3237	666	8.3150	752	7.6148	692	7.9911	664	7.3824	654	7.1281	665
removei	1.9135	85	1.3534	92	2.2858	118	1.7174	100	1.6308	85	1.6369	89	1.5850	81	1.5486	90
retainAll	2.7037	193	2.7845	200	2.6052	198	2.5982	205	3.0973	197	2.4172	200	2.7635	242	3.4019	245
set	0.9476	64	1.5943	70	1.9669	110	2.0474	112	1.5249	76	1.2312	73	1.4938	75	1.4957	72
sublist	1.3108	76	1.6021	80	1.4792	80	1.8457	98	1.4910	85	1.5117	71	1.7082	75	0.9414	75
toArray	1.6418	84	1.5024	84	2.0934	73	1.6739	106	1.5418	79	1.7455	83	1.5694	69	2.0213	80



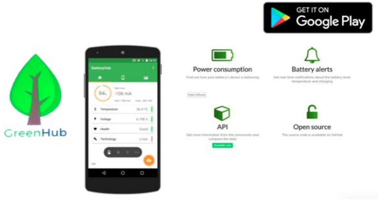
	Concurrent		Concurrent						Linked				Simple						Weak	
	HashMap		SkipListMap		HashMap		Hashtable		HashMap		Properties		Bindings		TreeMap		UIDefaults		HashMap	
Methods	J	ms	J	ms	J	ms	J	ms	J	ms	J	ms	J	ms	J	ms	J	ms	J	ms
clear	2.0276	94	2.2961	88	1.8395	104	1.5761	94	1.5025	97	2.0777	98	2.1401	106	1.6706	98	1.8143	105	1.9941	95
containsKey	2.3132	105	2.1693	123	2.1343	103	1.8582	94	1.8726	103	1.6018	107	1.8055	99	1.9452	100	2.3366	89	1.9675	108
containsValue	21.5611	2305	7.8032	643	8.3615	683	8.4957	765	6.1326	462	7.3755	692	7.9912	678	9.1771	847	7.9341	714	6.7072	562
entrySet	2.2878	93	2.2363	116	1.8531	108	2.1332	107	1.8362	113	1.7800	97	2.1557	102	2.1617	115	1.7087	105	1.4666	102
get	2.3106	103	1.9972	119	1.8120	102	1.4071	100	1.8252	116	1.7851	97	1.5359	100	2.2331	115	1.5252	89	1.7185	103
iterateAll	2.1041	96	1.8353	115	2.6673	100	1.5343	91	1.6462	111	1.6362	100	2.0472	116	1.9122	111	1.6574	95	1.7139	106
keySet	1.7287	95	2.4889	124	1.6813	114	2.2226	99	1.8328	103	1.4866	92	2.0630	106	2.1680	110	1.5547	99	1.8749	105
put	1.8591	104	2.2888	102	2.4628	92	1.3123	96	2.0338	108	1.7038	107	2.1646	102	1.4355	91	2.1204	93	2.5784	105
putAll	1.4147	95	2.2852	122	1.7564	100	1.5949	105	1.8608	113	1.3097	95	2.1461	112	1.8914	116	2.3094	87	2.0750	108
remove	1.8574	92	2.2131	105	1.9256	109	1.6067	97	2.2300	106	1.9660	98	2.2178	106	1.8133	101	1.6888	92	2.4103	103
values	1.8279	85	2.4690	116	2.5755	109	2.2266	94	2.0009	107	1.9120	111	2.0692	108	1.4467	105	1.6533	100	2.4628	111

SOFTWARE QUALITY
SOFTWARE ENGINEERING

Green Computing
Benchmarking/Data collection

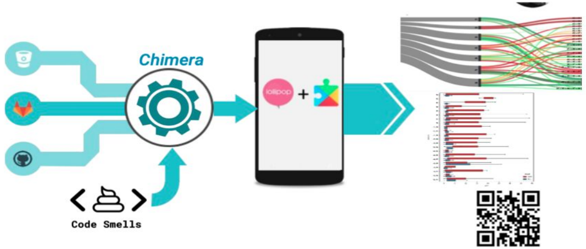


PyAnadroid



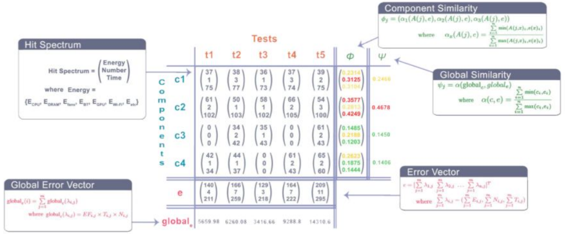
GreenHub

Green Computing
Energy Impact of Android Code Smells



Full Study Results

Green Computing
Spectrum-Based Energy Leak Localization



Hit Spectrum = (Energy, Number, Time) where Energy = $\{E_{CPU}, E_{DRAM}, E_{fans}, E_{BT}, E_{GPU}, E_{Wi\text{-}Fi}, E_{etc}\}$

Component Similarity: $\phi_j = (\alpha_1(A(j),e), \alpha_2(A(j),e), \alpha_3(A(j),e))$ where $\alpha_x(A(j),e) = \frac{\sum_{i=1}^{m} \min(A(j,x)_i, e(x)_i)}{\sum_{i=1}^{m} \max(A(j,x)_i, e(x)_i)}$

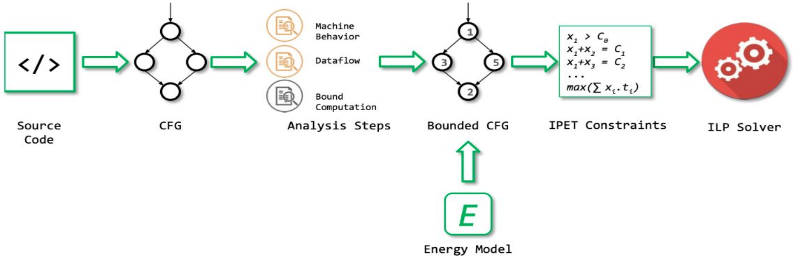
Global Similarity: $\psi_j = \alpha(global_c, global_e)$ where $\alpha(c,e) = \frac{\sum_{i=1}^{m} \min(c_i,e_i)}{\sum_{i=1}^{m} \max(c_i,e_i)}$

Error Vector: $e = [\sum_{j=1}^{m} \lambda_{1,j}\ \sum_{j=1}^{m} \lambda_{2,j} \dots \sum_{j=1}^{m} \lambda_{n,j}]^T$ where $\sum_{j=1}^{m} \lambda_{i,j} = (\sum_{j=1}^{m} E_{i,j}, \sum_{j=1}^{m} N_{i,j}, \sum_{j=1}^{m} T_{i,j})$

Global Error Vector: $global_e(i) = \sum_{j=1}^{m} global_e(\lambda_{i,j})$ where $global_e(\lambda_{i,j}) = EF_{i,j} \times T_{i,j} \times N_{i,j}$

	t1	t2	t3	t4	t5	Φ	Ψ
c1	37 1 75	38 3 77	36 1 73	37 3 74	39 2 75	0.2314 0.3125 0.3104	0.2466
c2	61 2 102	50 1 103	58 1 102	66 2 105	54 3 100	0.3577 0.2813 0.4249	0.4678
c3	0 0 0	34 2 42	35 1 43	0 0 0	61 2 43	0.1485 0.2188 0.1203	0.1450
c4	42 1 34	44 1 37	0 0 0	61 2 43	65 2 60	0.2623 0.1875 0.1444	0.1406
e	140 4 211	166 7 259	129 3 218	164 7 222	209 11 295		
$global_e$	5659.98	6260.08	3416.66	9288.8	14310.6		

Green Computing
Static Energy Analysis in Software Product Lines



$x_1 > C_0$
$x_1+x_2 = C_1$
$x_1+x_3 = C_2$
...
$max(\sum x_i \cdot t_i)$

Source Code

CFG

Analysis Steps

Bounded CFG

IPET Constraints

ILP Solver

Energy Model

SOFTWARE QUALITY
SOFTWARE ENGINEERING

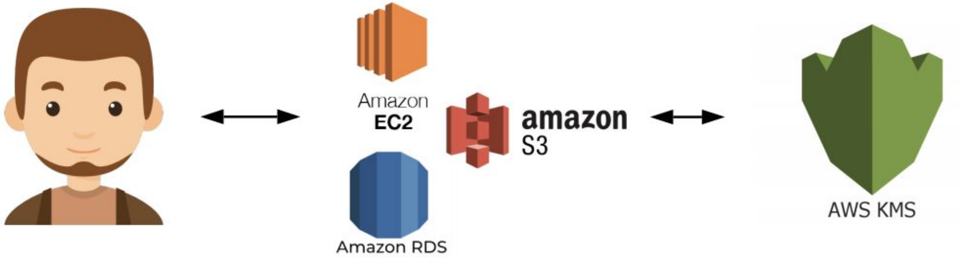
Wanna know more?

Group's Page

Git Repositories

PROJECT CYBER SECURITY

- Collaboration with amazon
- Formalize the security of AWS **Key Management Service**
- **Decentralized** system for protecting crypto keys of AWS users
    - Hardware Security Modules
    - Amazon operators
    - Front-end hosts

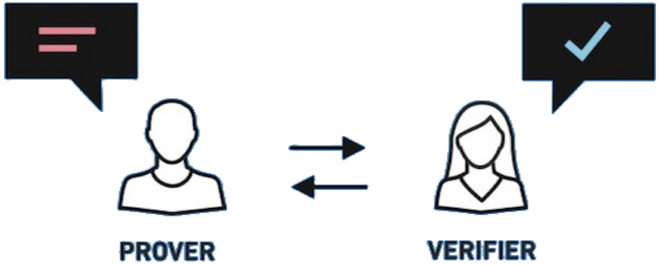


- A **machine-checked** cryptographic proof of protocol security
    - Largest machine-checked proof to date using EasyCrypt

EC-ZK PROJECT
CYBER SECURITY

- Collaboration with SRI International, part of DARPA **SIEVE** Zero-Knowledge Proof Research Program

ZKP: *prover* convinces a *verifier* that it knows a secret belonging to some relation



- **Machine-checked proof** of “MPC-in-the-Head” using EasyCrypt
  - modular construction to build ZKP for generic relations
  - used in modern quantum-secure signature schemes
- **Verified implementation** obtained via code synthesis
  - automatically extracted executable code
  - verified high-speed assembly operations

HADES PROJECT
CYBER SECURITY

NOVALINCS
LABORATORY FOR COMPUTER SCIENCE AND INFORMATICS

INESCTEC

FCT (2018-2021)

Goals

- Secure, efficient, and scalable approach to building completely **decentralized systems** for society critical applications
- Build on emerging technologies for **trusted execution environments**:
  - Intel SGX
  - ARM TrustZone
- **Reducing** computational and communicational costs of expensive cryptographic protocols used today in secure **decentralized** systems
- A new toolbox of **hardware-backed** abstractions and new protocols for decentralized **storage** and processing applications

THEIA PROJECT
CYBER SECURITY

Ongoing (2021-2023)

Goal: Develop and apply intelligent perception algorithms to support autonomous driving

Challenges (GDPR compliance)

- secure machine learning for connected vehicles
- secure inter-vehicle data communication
- secure in-vehicle data processing
- secure in-vehicle data storage

Other (non-THEIA) Automotive Partners

IDINA **PROJECT**
CYBER SECURITY

INCLUSIVE NON-AUTHORITATIVE DIGITAL IDENTITY

The project aims to create an effective and inclusive identification platform open to all citizens, in countries that do not have central identification systems (civil registration infrastructures).

The innovative nature of IDINA will help exploring the potential of **institutions and other agents** that work in the field, as **sources of reliable information** about citizens, with whom they have direct contact (non-governmental entities, for instance). In this sense, it will be possible to validate the data provided by the different entities about each citizen, and improve them throughout their life events.

Goals

- Design and implementation of a non-authoritative digital identity system filling the void stemming from a non-existent or incomplete State-managed legal identity system
- Inclusive solution enabling individuals to prove their identities to entities they regularly interact with, requiring no tech or low
- A stepping stone leading to a future full-fledge, State-managed legal identity authoritative system

INSTITUTE FOR SYSTEMS
AND COMPUTER ENGINEERING,
TECHNOLOGY AND SCIENCE

INESCTEC

THANK YOU!

HASLab

Campus de Gualtar
Universidade do Minho
4710-053 BRAGA
PORTUGAL

+351 253 604 440
haslab@inesctec.pt
www.inesctec.pt/en/centres/haslab

INESCTEC