Report on Deliverable Number D10.3

Strategic Analysis of the Supported Topics 2020

Workpackage		10		
Task		10.3		
Date of delivery	**Contractual**	Month 32 (July 2020)		
	Actual	Month 36 (November 2020)		
Code name		D10.3	Version 1	Draft ☐ Final ☒
Type of deliverable		Report		
Dissemination level		Public		
Contact(s)		Florence Quist	florence.quist@frs-fnrs.be	
WP/Task leader		Florence Quist	florence.quist@frs-fnrs.be	
EC project officer		Julian Ellis		
Publishable abstract		The report presents the analysis of the outcome of the funded projects in the Call 2015 topics: • User-Centric Security, Privacy and Trust in the Internet of Things (SPTIoT) • Terahertz Band for Next-Generation Mobile Communication Systems (TCMS) It also gives insight into the evolution of those topics.		
Keywords		Strategic analysis, supported topics, Call 2015		

Content Table

1. Overview of CHIST-ERA III Task Related to D10.3

The task (T 10.2) related to the deliverable 10.3 covers the strategic analysis for the topics funded by CHIST-ERA calls. This task entails an analysis of the results obtained by on-going projects and aims at the definition of suitable criteria for the identification of emerging research communities and their maturity. In addition, an analysis of the needs and opportunities of research projects for specifically identified topics is conducted in order to determine their compatibility with possible future ICT programmes. Deliverables of this task, D10.3 and following, will be made available to the FET community and other fora.

2. Analysis and recommendation for the process

a. Scope of Deliverable 10.3

In order to allow for maturation of both funded projects and topic, deliverable 10.3 focuses on the topics of the Call 2015:

- User-Centric Security, Privacy and Trust in the Internet of Things (SPTIoT)
- Terahertz Band for Next-Generation Mobile Communication Systems (TCMS)

Indeed, projects of the Call 2015 finished in 2020. During their lifetime, the corresponding research communities could form, exchange and present their vision of the future of their topics thanks to three editions of the CHIST-ERA yearly Projects Seminar[1].
This deliverable draws on the work performed in task 9.1 Project Follow-up and Monitoring (for projects from all calls except Call 2017) and in task 10.1 Projects Seminar Organisation.

b. Analysis of the Topic *User-Centric Security, Privacy and Trust in the Internet of Things (SPTIoT)*

i. Evolution of the Funded Projects

The CHIST-ERA consortium funded six projects in the SPTIoT topic. The table below details the specific scope of each project.

Name	Project goals
Cocoon	***Emotion psychology meets cyber security in IoT smart homes*** Innovative approaches in emotion psychology and cyber security, to understand and improve security of home IoT technology, in an attempt to recast the user as an integral part of the entire security system. The objectives are twofold: 1. To examine the users' emotional investment and their psychology in the context of the smart home, during both periods of normal use and, importantly, in periods when they experienced what they perceived as sporadic attack of their home IoT network. 2. To put mainstream IoT technology to the test, and prototype a network-wide intrusion detection system that leveraged the heterogeneity of protocols and traces of behaviour in the network. We combined several analytical techniques to detect characteristic features in network data.

[1] The project seminar 2020 planned in May 2020 had to be cancelled due to the Covid19 pandemic

ID_IOT	***IDentification for the Internet Of Things*** Generation of a general security and privacy toolbox for the IoT: • The handling of PUF data captured by IoT sensors, in particular for authentication and identification purposes • Privacy-preserving databases with good scaling behaviour • Mass deployment of Quantum-Readout PUFs (QRPUFs) a.k.a. Quantum-Secure Authentication (QSA) • Group membership verification
SPIRIT	***Security and PrIvacy foR the Internet of Things*** Investigation of the Proof-of Concept of employing novel secure and privacy-ensuring techniques in services set-up in the Internet of Things (IoT) environment, aiming to increase the trust of users in IoT-based systems. The system will address distinct issues related to security and privacy, hence, overcoming the lack of user confidence, which inhibits utilisation of IoT technology.
SUCCESS	***SecUre aCCESSibility for the internet of things*** Use methods and tools with a proven track-record to provide more transparency of security risks for people in given IoT scenarios. Extension of well-known industry-strength methods in priority areas. Technological innovation to provide adequate tools to address risk assessment and adaptivity within IoT in healthcare environments and an open source repository to foster future reuse, extension and progress in this area. Validation of the scientific and technological innovation through pilots, one of which will be in collaboration with a hospital and will allow all stakeholders (e.g. physicians, hospital technicians, patients and relatives) to enjoy a safer system capable to appropriately handle highly sensitive information on vulnerable people while making security and privacy risks understandable and secure solutions accessible.
UPRISE-IoT	***User-centric PRivacy & Security in the IoT*** Provide users with the control of data generated and collected by the IoT devices surrounding them. This project will take a fresh look at the IoT privacy space from a user-centric perspective. More specifically, users' behaviours and context will be considered in the implementation of security-compliant and privacy-preserving strategies for IoT data collection and processing. As a result, data transparency and control will be improved.
USEIT	***User empowerment for Security and prIvacy in Internet of Things*** Design and development of security and privacy mechanisms, so that users can control disclosure and usage of their personal data when they interact with IoT services. In particular, USEIT focuses on the design of new cryptographic schemes that are sufficiently efficient to be easily deployed in constrained IoT environments.

Together, those 6 projects address issues on:

1. Methods for data anonymization;
2. Technical mechanisms to increase trustworthiness when data is shared between different providers;
3. Intrusion detection methods;
4. Authentication using trusted computing (lightweight hardware and software security);
5. Dynamic security to allow systems to adapt to varying users;
6. Data visualization for increasing user awareness of privacy issues;
7. Empowering users with risk evaluation tool for their data and contacts;
8. Assistive technology/techniques to encourage more secure behaviour and awareness of users.

From the project progress reports by the participating teams and the review reports by the scientific experts appointed by CHIST-ERA, we can conclude that in general the projects progressed according to the initial plan and generated relevant results, as detailed in the table below:

Name	Major project outcomes
Cocoon	• 2000 Participants took part in series of studies to understand experience of victims of cybercrime • Characterisation of the psychology of IoT users • Characterisation of the landscape of IoT technologies • Development a device that permits the monitoring of network activity across the wide range of protocols used by IoT devices – Cocoon node
ID_IOT	• Sparse Ternary Coding with Ambiguation (STCA) seems to have privacy properties comparable to Zero Leakage Quantization + Code Offset Method • STCA applied to synthetic data achieves the claimed theoretical performance • It is possible to do Quantum Key Recycling without a rate loss even when Alice sends qubits only, i.e. no classical ciphertext. Furthermore, it is possible to combine Quantum Key Recycling and Unclonable Encryption without suffering a rate loss • Compact group representation method for speckle-PUFs • Results obtained lead to 1 follow up project.
SPIRIT	• Development of a new hashing method based on perceptual information that outperforms related methods. The new hashing method is robust to content preserving operations (compression, scaling etc.) and sufficiently sensitive to content-changing operations such as tampering or splicing • Development of a method for making automatically annotated datasets • Use of sensor data as a time series and viewing it as mean reverting, such that its time-based variance (high/low) and return to a centre line (Bollinger bands) can infer a binary string fingerprint that can also be error corrected • Use of Voronoi Diagrams to generate digital fingerprints from sensor data (visuals) that can be image processed to identify devices, K-Means and Bi-Clustering mapping techniques

	• Use of the hidden states of HMMs and restricted Boltzmann machines to derive meaning from sensor data. To improve accuracy or to generate "clean" synthetic distributions from physically generated distributions i.e., decoupling. • Design, implementation and integration of complete hardware and software platform based on the Raspberry PI, QT framework and cloud backend, which is capable of mapping all components of the project together into one demonstrator
SUCCESS	• Fully functional pilot (Isabelle) infrastructure framework and Risk-Refinement Loop applied to IoT Healthcare scenario • Security Enforcement in Model-based Systems Using Attack-Trees • Development of a new version of SBIP that generalises the current stochastic modelling formalism
UPRISE-IoT	• Study on the perception of privacy in users of mobile smart devices • Method to further enhance transparency and allow data subjects to make better informed choices of privacy settings • Development of a privacy-preserving Reinforcement Learning algorithm that allows several entities to perform a global optimization without requiring the exposition of sensitive data.
USEIT	• Users empowerment through the use of encryption based selective disclosure and policy based approaches • Production of a secure and efficient version of the proof-of-concept implementations of the pairings • Design of flexible and scalable cryptographic mechanisms to enable a secure IoT enabled data sharing platform • Proxy based Attribute based re-encryption approach • Providing advanced and lightweight cryptographic schemes to be used in C ITS scenarios • Privacy friendly authentication when entering a new zone & receiving zone key • Integration between the IDS and CP-ABE re-keying with the policy-based orquestration for incident identification on IoT systems

ii. Evolution of the Topic

As part of the projects seminar's format, the projects in the same topic were invited each year to reflect on their progress and on the key challenges that still need to be tackled in their specific field. They produced presentations that are made public and available from the CHIST-ERA website (http://www.chistera.eu/funded-topics). The following challenges were identified during the 2019 project seminar[2] and consolidated during and additional and *ad hoc* 2020 projects webinar:

- To reach out to the stakeholders to validate our visions;
- Certified code generation for IoT devices from component specifications;

[2] Project Seminar 2020 was cancelled due to the Covid19 pandemic. As a replacement, a virtual projects webinar dedicated to both topics was organized in October 2020.

- Quality and instability of data;
- Need to define guidelines for common strategy on data generation and metrics;
- Need for new lightweight cryptography for constrained small devices;
- Synergy between IDS and reaction system;
- Empower users ability to effectively control their data;
- Advanced techniques for pre-computation and re-encryption in IoT for reducing computation and energy cost;
- Privacy attributed based credential systems (p-ABC) integration with IoT solutions for increasing usability.

The scientific experts in charge of following up on projects progress noted that the latter should have taken greater consideration of the impact of the GDPR.

c. Analysis of the Topic *Terahertz Band for Next-Generation Mobile Communication Systems (TCMS)*

i. Evolution of the Funded Projects

The CHIST-ERA consortium funded two projects in the TCMS topic. The table below details the specific scope of each project.

Name	Project goals
TERALINKS	***TERAhertz high power LINKS using photonic devices, tube amplifiers and Smart antennas*** Demonstration of a real-time THz communication system, with the 200-300 GHz bandwidth, in an operational environment for point-to-point links. The TERALINKS consortium targeted to integrate three key enabling technologies and demonstrated the state of the art system with industrial relevance: THz sources, THz power generation using travelling wave tubes and advanced THz antennas.
WISDOM	***Wideband Low-Cost Smart Passive and Active Integrated Antennas for THzWireless Communications*** Advance towards the design and fabrication of smart, wideband and low-cost low-THz antennas and circuits. Such a frequency range is expected to be highly important for the 6th generation mobile communications (6G) and the internet of things (IoT). Use 3D techniques for fast fabrication THz passive/ active antennas. Combination of 3D and CMOS devices toward power combining antenna arrays.

Together, those projects address the following issue:

- Demonstration of the use of terahertz ' band for higher capacity (data rate);
- Developments at components and system level.

From the progress reports by the participating teams and the review reports by the scientific experts appointed by CHIST-ERA, we can conclude that projects progressed generally according to the initial plan and generated relevant results, as detailed in the table below:

Name	Major project outcomes
TERALINKS	• THz sources achieved • Tube amplifier designed for 240 GHz • Many types of antenna fabricated & characterized • 50 Gbps system in the lab demonstrated with silicon photodiodes • 100 Gbps system in the lab demonstrated with III V photodiodes
WISDOM	• 3 types of antennas fabricated and measured up to 300 GHz • CMOS transceiver integrated with horn see figures), IMS 2018 • Novel design on metamaterial based lens • Design of compact 300 GHz antennas (initial prototype validated at 140 GHz)

ii. Evolution of the topic

As part of the Projects Seminar's format, the projects in the same topic were invited each year to reflect on their progress and on the key challenges that still need to be tackled in their specific field. They produced presentations that are made public and available from the CHIST-ERA website (http://www.chistera.eu/funded-topics). The following challenges were identified in 2019:

- Testing in «real life » increased TRL of the system;
- Accurate characterization benches, methods and suitable metrics towards system level measurements (cross-comparison of data , reproducibility...).

3. General comments

Based on the scope of the supported topics and the progress and analysis of the funded projects about what still needs to be investigated, certain future calls from the ICT Work Programme 2018-2020 and EIC pilot Work Programme 2018-2020 are identified as being of interest to the CHIST-ERA Call 2014 research communities. The identified specific calls come in complement to the FETOPEN-01-2020 call.

Topic	Relevant Horizon Europe Work programme : ICT, EIC other relevant topics of WP 2021-2022
SPTIoT	• **EIC Pathfinder open** Scope: Support from EIC Pathfinder Open to realise an ambitious vision for radically new technology, with potential to create new markets and/or to address global challenges. EIC Pathfinder Open supports early-stage development of such future technologies (e.g. various activities at low Technology Readiness Levels 1-4), based on high-risk/high-gain science-towards-technology breakthrough research (including 'deep-tech'). This research must provide the foundations of the technology that is envisioned. Proposal must meet all the following essential characteristics ('Gatekeepers'): - Convincing long-term vision of a radically new deep-tech that has the potential to have a transformative positive effect to our economy and society; - Concrete, novel and ambitious science-towards-technology breakthrough, providing advancement towards the envisioned technology;

	- High-risk/high-gain research approach and methodology, with concrete and plausible objectives. • **HORIZON-CL4-2021-HUMAN-01-01: Verifiable robustness, energy efficiency and transparency for Trustworthy AI: Scientific excellence boosting industrial competitiveness** Scope: Scientific proposals are expected to focus on advancing the state of the art in one of the major research areas below: 1. Novel or promising learning (such as unsupervised, self-supervised, representational learning capable of contextualization, transfer learning, life-long and continual learning, etc.) as well as symbolic and hybrid approaches. The objective is to advance "intelligence" and autonomy of AI-based systems, essential to scale-up deployment, in solving a wider set of more complex problems, adapting to new situations (making them "smarter", more accurate, robust, dependable, versatile, reliable, secured, safer, etc.), and addressing real-time performance requirements, where relevant, for both robotics and non-embodied AI systems. This will include a.o. integration of both learning and reasoning, combining data-driven and knowledge-based models, causality, contextualization and knowledge discovery. Approaches can build on simulation and digital twins, or include data augmentation, knowledge modelling, federation of AI systems – including the use of distributed data – federated learning, and new AI methods ensuring scalability and re-usability. This topic also supports innovative or promising approaches addressing functional and performance guarantees; 2. Advanced transparency in AI, including advances in explainability, in transparency (with guaranteed/verifiable levels of performance, confidence levels, etc), investigating novel or improved approaches increasing user's understanding of AI system behaviour, and therefore increasing trust in such systems; 3. Greener AI, increasing data and energy efficiency. This covers research towards lighter, less data-intensive and energy-consuming models, optimized learning processes to require less input (frugal AI), or optimized models, data augmentation, synthetic data, transfer learning, one-shot learning, continuous / lifelong learning, and optimized architectures for energy-efficient hardware, framework that optimises calculations for energy reduction in big data analytics. This also build on latest results in self-configuring, low-power or energy harvesting capable sensor devices, and low power data transmission and energy reduction in big data analytics (e.g. a framework that optimises calculations, leading to decreasing use of energy, etc.); 4. Advances in edge AI networks, bringing intelligence near sensors, in embedded systems with limited computational, storage and communication resources, as well as the integration of advanced and adaptive sensors and perception (including multi-modal sensing and active perception, distributed sensing, etc.), but also optimising edge vs cloud AI to maximise the capabilities of the

	overall system (both globally and for individual users). This builds on latest hardware development but does not cover such hardware developments; 5. Complex systems & socially aware AI: Able to anticipate and cope with the consequences of complex network effects in large scale mixed communities of humans and AI systems interacting over various temporal and spatial scales. This includes the ability to balance requirements related to individual users and the common good and societal concerns, including sustainability, non-discrimination, equity, diversity etc. • **HORIZON-CL4-2021-DATA-01-01: Technologies and solutions for compliance, privacy preservation, green and responsible data operations** Scope: Digital technologies, methods, architectures and processes for safe, trustworthy, compliant, fair, transparent, accountable and environmentally sustainable collection, storage, processing, querying, analytics and delivery of data. The technologies shall facilitate sharing and manipulation of data in compliance with prevailing and emerging legislation (e.g. GDPR) for data processors and data subjects/rightholders and other stakeholders. The technologies and solutions shall enable safe data handling, sharing and re-use in the context of common European data spaces in various situations and application areas. The scope also includes technologies and solutions that enable environmentally sustainable data operations (e.g. by optimising/minimising/de-centralising processing, transfer and storage of data and avoiding unnecessary data manipulations, using energy-harvesting sensors/devices etc.), as well as technologies and solutions for ensuring human, fair and ethically sound collection, processing and manipulation of data, in line with the principles of responsible/trustworthy AI.
TCMS	• **EIC Pathfinder open** Scope: Support from EIC Pathfinder Open to realise an ambitious vision for radically new technology, with potential to create new markets and/or to address global challenges. EIC Pathfinder Open supports early-stage development of such future technologies (e.g. various activities at low Technology Readiness Levels 1-4), based on high-risk/high-gain science-towards-technology breakthrough research (including 'deep-tech'). This research must provide the foundations of the technology that is envisioned. Proposal must meet all the following essential characteristics ('Gatekeepers'): - Convincing long-term vision of a radically new deep-tech that has the potential to have a transformative positive effect to our economy and society; - Concrete, novel and ambitious science-towards-technology breakthrough, providing advancement towards the envisioned technology; - High-risk/high-gain research approach and methodology, with concrete and plausible objectives.

	• **HORIZON-CL4-2021-DIGITAL-EMERGING-01-06: Advanced optical communication components** Scope: Projects to develop ultra-dynamic photonic components and subsystems for data communication, using for example new optical wavelength bands, space division multiplexing, new integration schemes, optical switching and new switching paradigms, as solutions for time-deterministic and time-sensitive networks. They should also enable ultra-dynamic reconfiguration on the optical layer and mitigate amplifier power transients, while saving energy, improving bandwidth efficiency, and guaranteeing low deterministic latencies across the network. Advances will cover a range of use cases for example from optical switching in commercial applications to optical flow or packet switching approaches that would become practical for the industrial Internet. Where relevant for the application, devices should be able to work in a harsh environment such as within a wide temperature operating range, or in high humidity.