

ENCRYPT Newsletter Issue #4

Contents

1. Brief Summary
- 2-3. Project Achievements
4. Scientific Publications
4. Events
5. Learn more

We are pleased to announce the publication of the 4th issue of the ENCRYPT newsletter!

ENCRYPT is a 3-year Research and Innovation Action which began in July 2022, and is funded under Horizon Europe. The Consortium consists of 14 experienced and committed partners, namely 2 industrial partners, 3 SMEs, 1 start-up, and 8 research centers universities, spread around 8 EU countries.

ENCRYPT will develop a scalable, practical, and adaptable privacy preserving framework which allows researchers and developers to process data stored in federated cross-border data spaces in a GDPR compliant way. Within this framework, a recommendation engine for citizens and end-users will be developed, providing them with personalised suggestions on privacy preserving technologies based on the sensitivity of data and the trade-off between the degree of security and the overall system performance.

The ENCRYPT framework will consider the needs and preferences of the relevant actors, and will be validated in a comprehensive, 3-phase validation campaign. Those 3 phases are i) in-lab validation tests; ii) use cases provided by consortium partners in three sectors, namely the health sector, the cybersecurity sector, and the finance sector, that include cross-border processing of data; and iii) external use cases including privacy preserving computations on federated medical datasets.

Our newsletter is published twice a year, offering updates on the latest news and advances of the project!

Follow us on online media to be kept up to date with ENCRYPT.



[encrypt-project](https://www.linkedin.com/company/encrypt-project)



[@encrypt_project](https://twitter.com/encrypt_project)



encrypt-project.eu



encrypt

A scalable and practical
privacy-preserving framework

Project Achievements

This fourth issue of the ENCRYPT newsletter covers a period of 6 months from January to June 2024. Activities on all technical Work Packages have continued in this period. An account per active Work Package of the project, and their achievements based on the progress of initial work is summarised below.

Privacy-preserving computation technologies [WP3]

Our project has made significant progress in Work Package 3, focusing on "Privacy-Preserving Computation Technologies". As part of our collaborative efforts, in the 6 months period from January to June 2023, we improved the workflow design to address all use-cases. All partners have also made substantial advancements in implementing and integrating privacy-preserving tools tailored to the project's specific use-cases. These tools encompass Homomorphic Encryption, Trusted Execution Environments, Differential Privacy and Hardware Acceleration, as well as a hybrid tool which uses homomorphic encryption combined with the trusted environment

Each of these tools plays a crucial role in ensuring privacy while enabling efficient computation:

- **Homomorphic Encryption** is a cryptographic technique that allows computations to be performed directly on encrypted data, ensuring confidentiality throughout the process.
- **Trusted Execution Environments** provide secure enclaves where sensitive computations can be executed, protecting data from unauthorized access.
- **Differential Privacy** ensures that statistical analysis on datasets does not reveal individual-level information, striking a balance between data utility and privacy.
- **Hardware Acceleration** techniques optimize the performance of privacy-preserving operations.

Through the collaborative efforts of all partners, our project is achieving significant milestones in the implementation and integration of these tools. In particular, functional tools are now implemented to address the FinTech use-case with all of these privacy-preserving technologies. An effort has also been made by all partners to progress in integrating these tools. For instance, The FHE tool is integrated with the hardware accelerator, and work has begun to optimize the acceleration of FHE in the context of the FinTech use-case. Finally, the TEE-based tool is fully integrated in the main platform of the project.

These advancements pave the way for robust privacy-preserving computation technologies, enabling secure and efficient processing of sensitive data in various real-world use-cases.



Funded by
the European Union

Disclaimer: Views and opinions expressed are those of the ENCRYPT consortium authors only and do not necessarily reflect those of the European Union or its delegated Agency DG CNECT. Neither the European Union nor the granting authority can be held responsible for them.

Privacy-supporting technologies [WP4]

In WP4, between January 2024 to June 2024, significant progress was made in evolving and updating technologies and methodologies aimed at supporting the ENCRYPT project, focusing on user-friendliness. More specifically:

- Different pre-processing techniques such as data reduction were implemented, tested and fine-tuned across all datasets. Detailed tests on Named Entity Recognition (NER), Nerpii, and Large Language Models (LLMs) were conducted to improve the identification and extraction of Private Identifiable Information (PII). Additionally, internal testing, fine-tuning and updates were performed to ensure optimal performance.
- Significant progress was made developing and integrating ontology alignment solutions to improve the precision and usefulness of the Knowledge Graph tools. The initial technology, BERTMap, provided a robust foundation for ontology class alignment. However, it had limitations in terms of accuracy and performance. To address these, we transitioned to using Large Language Models (LLMs), which significantly improved both the performance and accuracy of our results. This transition has been a critical step in enhancing the capabilities of our Knowledge Graph tools. As such, we improved the model performance by utilizing LLMs and Few-Shot Learning techniques. Vector databases were also used to improve the generation process and lessen data distortion, producing outputs that were more accurate and dependable. KPIs have been already met, achieving over 95% coverage of modelling requirements, ensuring 100% consistency in domain models.
- Several updates have been made on the privacy risk assessment tool. The main one involves the definition of the taxonomy for the Fintech domain. A new procedure was also established that allows the compilation of privacy and a vulnerability assessment. Lastly a summary of what has been compiled along with the impact, vulnerability and risk scores was introduced as a new functionality.
- The AI-based recommendation engine can successfully select between the basic privacy preserving technologies offered by the ENCRYPT platform, and now provides a justification that accompanies the selected technology. The justification explains why the technology was selected and is tailored to the knowledge of the data owner, providing more detail when it is appropriate and less when the data owner is not familiar with data privacy and protection.
- New functionalities were identified for the front-end tool and these have been implemented, to enhance the user experience and allow more users to use the functionalities of the ENCRYPT platform in an easier manner.

Integration, validation, and evaluation [WP5]

Following the conclusion of the first successful integration of the components that make up the ENCRYPT platform, partners have continued to work on their components during the first 6 months of 2024. Specifically, we are preparing for the second full integration of the ENCRYPT platform that will take place in September 2024. This second integration will test the compatibility of the enhanced versions of the platform's subcomponents - the User Interface, the pre-processing tool, the knowledge graphs, the recommendation engine, and the platform backend - and will also see more privacy-preserving technologies deployed through the platform which are the Trusted Execution Environment, Differential Privacy, and Fully Homomorphic Encryption.

The development of the use cases to test the ENCRYPT platform also began in June 2024. Three use cases in three different domains - health care, cybersecurity, and fintech - will incorporate ENCRYPT into their work flow, which will protect the sensitive data involved in each domain.

The use cases provide the opportunity not only to test the work done by the partners developing the privacy-preserving technologies, but also to test the recommendation engine, pre-processing tool and knowledge graphs in a variety of scenarios, which will be used to improve their outputs.



Scientific publications

Although no papers which carry acknowledgement of the ENCRYPT project were accepted during the period January to June 2024, a fair number of papers have been submitted to various conferences and these will appear in the next Newsletter.

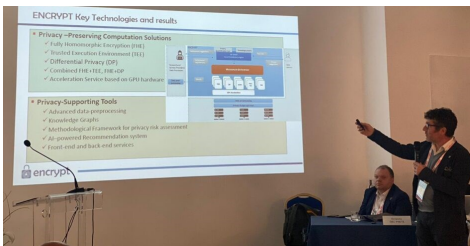
For the complete list of research papers, please visit:

<https://encrypt-project.eu/downloads/publications/> or the [ENCRYPT community page](#) directly at ZENODO.

Events

Check out all ENCRYPT project updates at <https://encrypt-project.eu/communication/encrypt-news/>

ENCRYPT presented at a ITASEC 2024 Conference Workshop



On April 8th 2024 Salvatore D'Antonio and Chiara Feoli participated in the "Protection from Cybersecurity-induced Safety Threats" workshop at ITASEC 2024 in Salerno, Italy. The event explored safety risks from cybersecurity incidents and strategies for mitigation. Salvatore presented ENCRYPT's privacy-preserving solutions for medical data, while Chiara discussed cybersecurity challenges in healthcare, particularly in diagnostic imaging and radiation oncology.

Read more: <https://encrypt-project.eu/communication/news/encrypt-presented-at-a-itasec-2024-conference-workshop/>

ENCRYPT Project Joins CPDP 2024: Spotlight on Fundamental Rights and AI

The ENCRYPT project partnered with the 17th CPDP International Conference in Brussels, held on May 22-24, 2024. ENCRYPT organized the panel "Fundamental Rights Protection and Artificial Intelligence," featuring experts such as Dr. Marco Bassini of ENCRYPT. The panel discussed AI's role in enhancing fundamental rights protection, with a focus on privacy-enhancing technologies and the EU's forthcoming AI Act. Bassini highlighted ENCRYPT's privacy-preserving technology and related use cases.



Read more: <https://encrypt-project.eu/communication/news/encrypt-project-joins-cdpd-2024-spotlight-on-fundamental-rights-and-ai/>

Other Activities

- In January 2024, Salvatore D'Antonio from TRUSTUP presented ENCRYPT at the workshop on Security Services for Connected Devices, organised by the CROSSCON project. More details of the event can be found here: <http://2024.necs-winterschool.disi.unitn.it/>
- In February 2024, Sotiris Diamantopoulos appeared at an "Innovation Talk Podcast" where he presented and discussed with the presented about the ENCRYPT Project. The podcast is in Greek and can be found here: <https://open.spotify.com/episode/5tM5IAyp1v8S3m15w9MEX5>
- In May 2024, Marco Bassini from TiU organised a panel devoted to AI and fundamental rights on the role of privacy preserving technology in the ENCRYPT project. Marco was also a speaker on this panel. More details of this event can be found here: <https://www.cdpdconferences.net/CPDP2024.pdf>
- In May 2024, Irene Kamara from TiU spoke at a panel on data security in dataspace organised by the European Agency for Cybersecurity (ENISA). The talk included insights from the ENCRYPT health use case, challenges of data security in common dataspace, and technical standardisation.



encrypt

A scalable and practical
privacy-preserving framework

ENCRYPT project in a nutshell

Fact sheet

Project Title	A scalable and practical privacy-preserving framework
Acronym	ENCRYPT
GA No	101070670
Start	01 July 2022
End	30 June 2025
Budget	4.392.540 €
EU Funding	4.392.540 €
Call	HORIZON-CL3-2021-CS-01
Funding	RIA - Research and Innovation action
Topic	HORIZON-CL3-2021-CS-01-04

Consortium




CERTH
CENTRE FOR
RESEARCH & TECHNOLOGY
HELLAS



UNIVERSITÄTSmedizin.
MAINZ



Stay in touch!

 <https://encrypt-project.eu>

 [encrypt-project](https://www.linkedin.com/company/encrypt-project)

 [@encrypt_project](https://twitter.com/encrypt_project)

*Our newsletter is published twice a year,
offering updates on the latest news and advances of the project!
[Subscribe here](#) to receive ENCRYPT newsletter at your inbox.*