encrypt

A scalable and practical privacy-preserving framework

Brief Summary

We are pleased to announce the publication of the 6th issue of the ENCRYPT newsletter!

ENCRYPT Newsletter Issue #6

Contents

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 across 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! This is the final newsletter of the ENCRYPT Project—thanks for your support!

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

encrypt-project

@encrypt_project

encrypt-project.eu

Funded by the European Union

encrypt

A scalable and practical privacy-preserving framework

Project Achievements

This sixth and final issue of the ENCRYPT newsletter covers a period of 6 months from January to June 2025. 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, we finalized the implementation and the integration of the tools. Due to substantial effort from all the partners, our privacy-preserving tools are now finalized and available through the main platform of the project for usage in the context of all the 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.

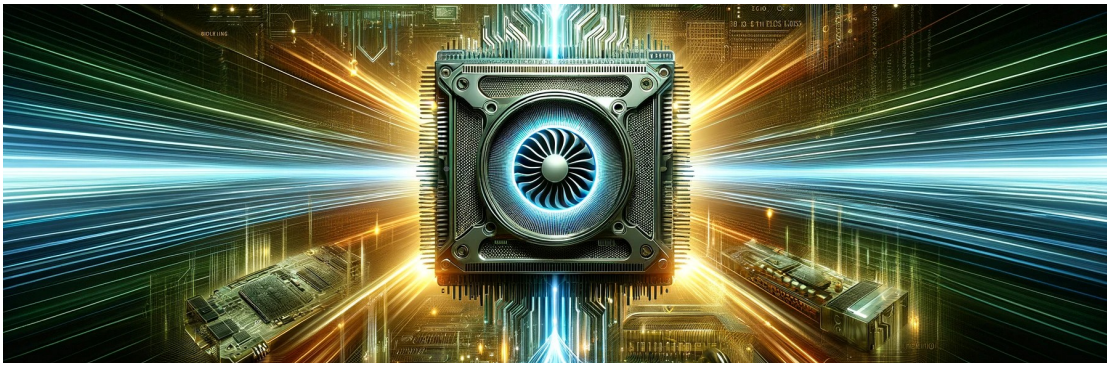
Each of these tools plays a crucial role in ensuring privacy while enabling efficient computation:

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

Through the collaborative efforts of all partners, our project is achieving the implementation and integration of these tools, including variants of the previous tools adapted to other use-cases, and various additional client-side tools for completing use-case workflows.

In particular, HE is now available for all the three use-cases of the project, as well as its combination with TEE, from revisited solutions according to the requirements of the use-cases. DP is now available for the health use-case, and a new optimized version of DP for the FinTech use-case has been developed, based on repeated trainings of models over several hyperparameters. The hardware acceleration tool has also been migrated in a cloud-based environment and optimized with parallelism. A performance analysis has been made on accelerated HE based on setup cryptographic parameters. An effort has also been made for optimizing these tools and adapting them to the specificities of the use-cases, for instance the HE algorithm chosen in CTI context has allowed the use of a non-LWE based HE scheme for security in a stronger model and potentially easier standardization.

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

encrypt

A scalable and practical privacy-preserving framework

Project Achievements

Privacy-supporting technologies [WP4]

In WP4, significant progress was made in evolving and updating technologies and methodologies aimed at supporting the ENCRYPT project. More specifically:

- During this period, the Data Preprocessing and Preparation tool was further updated to align with the requirements of the tool's owner and the different use cases. Furthermore, regarding the identification of Private Identifiable Information (PII), new assessments of the identification procedures were made.
- During the first half of 2025, the ENCRYPT project made significant progress in refining and expanding its Knowledge Graph (KG) infrastructure, with a continued emphasis on semantic alignment, interoperability, and scalable integration of real-world domain data. Efforts focused on enhancing LLM-powered ontology alignment techniques—particularly through fine-tuning and adaptive, few-shot learning—resulted in improved contextual understanding across domains such as cybersecurity and MIRACUM healthcare datasets. Domain-specific modules matured, with MIRACUM ontologies further validated across federated healthcare data and the CTI module (using MITRE ATT&CK) providing richer graph-based threat intelligence. The KG infrastructure also began integrating data from the GLACIATION project, showcasing the pipeline's flexibility with SCADA and energy datasets. Finally, optimizations to the vector-based querying backend improved real-time, cross-domain semantic search, ensuring timely and relevant access to actionable insights, especially for healthcare and cybersecurity use cases.
- Regarding the recommendation engine, the final updates and refinements to the rule base of the tool were completed as the task and the project come to an end. These refinements were based on the testing of the recommendation engine on real-world use cases from WP5 and the MIRACUM use case. In addition, the output of the Risk Assessment tool was incorporated into the justification of the recommendation engine, urging the data owner to consider how any risks identified in their system might affect the use case before they proceed to share the data with the researcher.
- With regard to the ENCRYPT User Interface, various changes have been made to both the functional and aesthetic aspects of the UI. These include updating the interface to align with the requirements of the Use Cases, as well as additional adjustments to colors and fonts. In addition, the backend was updated to facilitate the incorporation of the risk assessment outputs in the justification of the recommendation engine, deepening the connection between WP4 tasks.

Funded by the European Union

encrypt

A scalable and practical privacy-preserving framework

Project Achievements

Integration, validation, and evaluation [WP5]

During the final six months of the ENCRYPT project in the first half of 2025, all components have been completed and extensively tested in real-world scenarios across multiple use cases. The platform's core elements, including the user-friendly UI, pre-processing tool, knowledge graphs, recommendation engine, and platform backend, have been fully refined and deployed. Advanced privacy-preserving technologies like TEE, DP and FHE have been successfully implemented, with comprehensive testing conducted in healthcare, cybersecurity, and fintech environments to validate the platform's capabilities in diverse operational contexts.

The platform features secure identity management through Keycloak, providing seamless user authentication and role-based access control across all components. The orchestrator operates with enhanced flexibility, efficiently managing complex workflows and adapting to various deployment scenarios, including geo-localized computations and on-demand resource allocation. Recent updates to the UI have focused on maximizing user friendliness to ensure optimal usability across all use cases.

In the Fintech use case, the platform supports model training (using DP or TEE) and inference (using DP or FHE with acceleration and TEE), with FHE integration demonstrating significant reductions in processing time when combined with the acceleration service. The risk assessment tool has been fully integrated, with its results incorporated into the justification of the recommendation engine for improved security, demonstrating how ENCRYPT effectively lowers risks for data owners and integrates with other WP4 tools.

The Health use case focuses on secure patient data management in cancer oncology using FHE for encrypted data analysis. Following successful single-machine testing, comprehensive in-lab validation with realistic data has been completed.

For the CTI use case, FHE serves as a robust privacy-preserving solution, enabling data owners to encrypt their data after establishing a secure communication with a TEE. The encrypted data is then correlated with external threat information collected through MISP channels (i.e. blacklists), using a PIR protocol. TEE ensures secure data analysis and pattern identification, keeping the data concealed from service providers while still allowing them to retrieve and utilize the results.

The MIRACUM use case has successfully implemented scenarios such as polypharmacy analysis and privacy-preserving record linkage between hospitals. These use cases demonstrate ENCRYPT's proven capabilities in handling sensitive data across different domains, with TEE and DP ensuring privacy during data analysis and linkage. TEE and DP have both been thoroughly evaluated and validated for securing the linkage of datasets from different sources.

As the ENCRYPT project draws to a close, the comprehensive testing across diverse use cases has demonstrated the platform's robustness and effectiveness in real-world applications. The successful deployment and validation of privacy-preserving technologies across healthcare, cybersecurity, and fintech domains confirms the platform's readiness for broader adoption, with all components fully integrated and tested in a variety of operational situations. Additionally, testing with an external use case has provided valuable insights into the platform's adaptability and performance beyond the core project scenarios, offering an independent evaluation mechanism that further validates ENCRYPT's versatility and real-world applicability.

Funded by the European Union

Scientific publications

We present a list of papers submitted and accepted during the period January 2025 to June 2025 that carry acknowledgement of ENCRYPT project. For the complete list of research papers, please visit https://encrypt-project.eu/downloads/publications/ or the ENCRYPT community page directly at ZENODO.

- Maria Papoutsoglou, Apostolos Mavridis, Stergios Tegos, Christos Anastasiou, Georgios Meditskos. LLM-Based Ontology Mapping for Privacy-Preserving Healthcare Data Management. Semantic Web Applications and Tools for Health Care and Life Science (SWAT4HCLS).
  Download from Zenodo
- Luigi Coppolino, Salvatore D'Antonio, Giovanni Mazzeo, Luigi Romano. An Experimental Evaluation of TEE technology: Benchmarking Transparent Approaches based on SGX, SEV and TDX. Computers & Security, 154, 104457.
  Download from Zenodo
- Apostolos Mavridis, Stergios Tegos, Christos Anastasiou, Maria Papoutsoglou, Georgios Meditskos. Large language models for intelligent RDF knowledge graph construction: results from medical ontology mapping. Frontiers in Artificial Intelligence, 8, 1546179.
  Download from Zenodo
- Apostolos Mavridis, Stergios Tegos, Christos Anastasiou, Maria Papoutsoglou, Georgios Meditskos. Integrating AI and Knowledge Graphs with MITRE ATT&CK.
  Download from Zenodo
- Apostolos Mavridis, Stergios Tegos, Christos Anastasiou, Maria Papoutsoglou, Georgios Meditskos. Ontology Alignment and PII for Financial Knowledge Graph Construction.
  Download from Zenodo
- Orion Papadakis, Michail Papadimitriou, Athanasios Stratikopoulos, Maria Nektaria Xekalaki, Juan Fumero, Christos Kotselis. Offloading Key Switching on GPUs: A Path towards Seamless Acceleration of FHE. Frontiers in Artificial Intelligence, 8, 1546179.
  Download from Zenodo
- Athanasios Dimitriadis, Angelos Papoutsis, Dimitrios Kavalieros, Theodora Tsikrika, Stefanos Vrochidis and Ioannis Kompatsiaris. EVACTI: Evaluating the actionability of cyber threat intelligence. International Journal of Information Security (2025) 24:123.
- Irene Kamara and Marco Bassini. The cybersecurity and AI nexus in the EU digital acquis. Rivista di diritto dei media, 1, 2025.

Funded by the European Union

Events

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

ENCRYPT Hackathon: Data Readiness for Privacy-Preserving Technologies

In March and June 2025, ENCRYPT ran an online hackathon titled "Data Readiness for Privacy‑Preserving Technologies". The event featured hands‑on workshops where participants learned to anonymize datasets, preprocess data for privacy‑preserving technologies (PPTs), and address GDPR compliance and ethical data sharing, including introductions to differential privacy. A use‑case example allowed attendees to apply these skills, with the ENCRYPT team presenting their PPTs and discussing their practical applications. The hackathon targeted professionals and researchers in fields managing sensitive data.

Read more: https://encrypt-project.eu/communication/news/encrypt-hackathon-data-readiness-for-privacy-preserving-technologies/

Final Event – "Encrypting Europe: Towards Secure and Federated Data Use"

To celebrate and disseminate the results of the project, the ENCRYPT consortium hosted its final public event on 17 June 2025 in Athens. Titled "Encrypting Europe: Towards Secure and Federated Data Use", the event brought together researchers, industry representatives, policymakers and stakeholders in the data privacy and cybersecurity domains.
The agenda featured:

- Keynotes from leading data privacy experts. These were given by:
  - Dr. Andreas Mitrakas, Head of Unit at the "Executive Director's Office" in the European Union Agency for Cybersecurity (ENISA)
  - Professor Emanuele Bellini, University of Roma Tre
- Presentation of the ENCRYPT platform and its enabling technologies
- Panel discussions on the future of privacy-preserving computation in Europe

Read more: https://encrypt-project.eu/communication/news/encrypt-final-event-encrypting-europe-towards-secure-and-federated-data-use/

As we approach the project's conclusion, today at the end of June 2025, we would like to take this moment to thank our consortium members and the broader community for their efforts and support over the past three years.

The ENCRYPT project's results and platform stands as a testament to what collaborative European research can achieve.

Funded by the European Union

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

EXUS · ENGINEERING THE DIGITAL TRANSFORMATION COMPANY · CERTH CENTRE FOR RESEARCH & TECHNOLOGY HELLAS · EIGHTBELLS Independent Research & Consultancy · cea

TrustUP A PARTHENOPE UNIVERSITY SPIN-OFF · ARISTOTLE UNIVERSITY OF THESSALONIKI · DBC EUROPE S.A. · TILBURG UNIVERSITY Understanding Society · UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

BANK OF EPIRUS COOPERATIVE YOUR LOCAL BANK · GOETHE UNIVERSITÄT FRANKFURT AM MAIN · JG|U UNIVERSITÄTSmedizin. MAINZ · MANCHESTER 1824 The University of Manchester

Stay in touch!

https://encrypt-project.eu

encrypt-project

@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.

Funded by the European Union