encrypt
A scalable and practical privacy-preserving framework

Brief Summary

ENCRYPT Newsletter Issue #5

Contents

We are pleased to announce the publication of the 5th 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 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!

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

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.

Project Achievements

This fifth issue of the ENCRYPT newsletter covers a period of 6 months from July to December 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, we finalized 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 (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 significant milestones in the implementation and integration of these tools. In particular, TEE is now available for all the three use-cases through the main platform of the project. DP and HE tools for the FinTech use-case have also been integrated in this platform, and the FinTech HE tool has been integrated with HA in parallel, and successfully tested on the accelerated version of the HE library. Another HE tool for the medical use-case has also been implemented, and an effort started for implementing a DP tool for the medical use-case as well. Finally, an effort has also been made for optimizing and generalizing these HE and DP tools.

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, significant progress was made in evolving and updating technologies and methodologies aimed at supporting the ENCRYPT project, with a focus on making the ENCRYPT platform more user-friendly. More specifically:

- During this period, the data preprocessing and preparation tool was updated to align with the requirements of the tool's owner. Specifically, various techniques were removed or added to address the needs related to Fully Homomorphic Encryption (FHE) and Differential Privacy (DP). Furthermore, with regards to Private Identifiable Information (PII) identification, the NERPII library was tested and evaluated across the project's datasets. Lastly, with the aim of extracting PII from the pixel level of DICOM (Digital Imaging and Communications in Medicine) files, Optical Character Recognition (OCR) was utilized. The extracted PII is then processed by an LLM to categorize it and determine whether it is PII or not.
- During the second half of 2024, the Knowledge Graphs were refined to improve accuracy, scalability and interoperability across multiple domains. Major enhancements included integrating Large Language Models for more precise ontology alignment, employing context-aware alignment techniques for specialized datasets and utilizing Few-Shot Learning for efficient introduction of new concepts. Domain-specific modules were expanded in the Cyber Threat Intelligence (CTI) and MIRACUM use cases, incorporating the MITRE ATT&CK framework as well as SNOMED CT and HL7 FHIR standards to enrich threat intelligence and clinical/genomic data modeling. The supporting vector database also gained dynamic indexing and optimized query performance, enabling complex, real-time information retrieval in healthcare, finance, cybersecurity and MIRACUM contexts.
- The recommendation engine and its justifications have been refined over the past few months. It now offers more robust recommendations by incorporating geolocation requirements and the type of data uploaded to the platform. Justifications for recommendations explicitly reference relevant legal frameworks, including GDPR and the AI Act. Additionally, the engine can now suggest hybrid technologies, such as a combination of TEE and FHE, or FHE with the TornadoVM acceleration service developed by the University of Manchester. An LLM-based variant of the recommendation engine was developed and tested to assess its potential to enhance the current solution. While the current approach remains more suitable for now, because the output is clearly understood and the results are deterministic, this avenue shows promise for future iterations.
- With regards to the ENCRYPT User Interface, various changes and updates took place during this period. These changes affected both the functional aspects of the UI - such as adding justification to the available configurations for the user, and aesthetic aspects, including adjustments to colors and fonts. On the backend, the platform was continuously monitored using the installed monitoring tools. The backend has been updated to align with changes in outputs and message structures from other tasks, particularly those involving the knowledge graphs and user interface. These updates also address the new information requirements of the platform orchestrator, ensuring proper integration and functionality.

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.

Integration, validation, and evaluation [WP5]

Following the successful second integration of the ENCRYPT platform in September 2024, significant progress has been made in refining its components, including the UI, pre-processing tool, knowledge graphs, recommendation engine and platform backend. Advanced privacy-preserving technologies like TEE, DP and FHE were deployed, and use cases in healthcare, cybersecurity, and fintech were launched to test and validate the platform's capabilities. These use cases aim to demonstrate the effectiveness of ENCRYPT's tools while providing insights into further improvements.

Key advancements include the successful setup of Keycloak for secure identity management, enabling seamless user authentication and role-based access control across the platform. Additionally, the new orchestrator has been implemented with enhanced flexibility, allowing it to efficiently manage complex workflows and adapt to various deployment scenarios, including geo-localized computations and on-demand resource allocation.

In the Fintech use case, the platform supports model training (using DP and TEE) and inference (using FHE with acceleration and TEE), with FHE integration showing promising reductions in processing time. The risk assessment tool is being explored to demonstrate how ENCRYPT can lower risks for data owners and integrate with other WP4 tools.

The Health use case focuses on secure patient data management in cancer oncology using FHE for encrypted data analysis. After successful single-machine testing, future steps include in-lab validation with realistic data and further integration into clinical workflows.

For the CTI use case, FHE will serve as a privacy-preserving option, enabling data owners to encrypt their data before sharing it or after establishing secure communication with a TEE. The encrypted data is then correlated with external threat intelligence collected through MISP channels, 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 explores scenarios such as polypharmacy analysis and privacy-preserving record linkage between hospitals. These use cases demonstrate ENCRYPT's capabilities in handling sensitive data across different domains, with FHE and DP ensuring privacy during data analysis and linkage.

The Risk Assessment Tool is being considered to evaluate process improvements, while TEE and FHE are both under evaluation for securing the linkage of datasets from different sources.

Overall, the second integration highlights ENCRYPT's progress in deploying and testing privacy-preserving technologies across diverse use cases, with ongoing efforts to refine components and ensure seamless integration. The integration of Keycloak and the new orchestrator has further strengthened the platform's security, flexibility, and scalability, paving the way for broader adoption and real-world applications.

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.

Scientific publications

We present a list of papers submitted and accepted during the period July 2024 to December 2024 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.

- Stelios Erotokritou, Ioannis Giannoulakis, Emmanouil Kafetzakis, Konstantinos Kaltakis, Ettore Etenzi, Sotiris Diamantopoulos, Giovanni Mazzeo, Salvatore D'Antonio, Jean-Paul Bultel, Athanasios Stratikopoulos, Angelos Papoutsis, James Lloyd, Georgios Meditskos, Vincenzo Napolitano. *Revolutionizing Data Privacy: The ENCRYPT Project's Innovations and Applications*. 2024 European, Mediterranean and Middle Eastern Conference on Information Systems.
  Download from Zenodo
- Stelios Erotokritou, Ioannis Giannoulakis, Emmanouil Kafetzakis, Konstantinos Kaltakis. *Simplifying Differential Privacy for Non-Experts: The ENCRYPT Project Approach*. 2024 IEEE International Conference on Cyber Security and Resilience.
  Download from Zenodo
- Christina Karalka, Georgios Meditskos, Maria Papoutsoglou, Nick Bassiliades. *Towards a Generic Knowledge Graph Construction Framework for Privacy Awareness*. 2024 IEEE International Conference on Cyber Security and Resilience.
  Download from Zenodo
- Maria Papoutsoglou, Georgios Meditskos, Nick Bassiliades, Efstratios Kontopoulos, Stefanos Vrochidis. *Mapping the Current Status of CTI Knowledge Graphs through a Bibliometric Analysis*. 13th Conference on Artificial Intelligence (SETN 2024).
  Download from Zenodo
- Salvatore D'Antonio, Jonah Giglio, Federica Uccello, Giovanni Mazzeo. *Enhancing Healthcare Data Confidentiality through Decentralized TEE Attestation*. 2024 IEEE International Conference on Cyber Security and Resilience.
  Download from Zenodo
- Orion Papadakis, Michail Papadimitriou, Athanasios Stratikopoulos, Maria Xekalaki, Juan Fumero, Nikos Foutris, Christos Kotselidis. *Towards GPU Accelerated FHE Computations*. 2024 IEEE International Conference on Cyber Security and Resilience.
  Download from Zenodo
- Marina Checri, Renaud Sirdey, Aymen Boudguiga and Jean-Paul Bultel. *On the practical CPAD security of "exact" and threshold FHE schemes and libraries*. Advances in Cryptology – CRYPTO 2024. CRYPTO 2024. Lecture Notes in Computer Science, vol 14922.
  Download from Zenodo

Events

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

ENCRYPT Organises two September Workshops

IEEE CSR
Cyber Security and Resilience
2024 IEEE International Conference on Cyber Security and Resilience
2024 IEEE CSR Workshop on Privacy-Preserving Data Processing and Analysis
Supported by: encrypt

In September 2024, the ENCRYPT project hosted two key workshops on privacy-preserving technologies. On September 2, at the IEEE International Conference on Cyber Security and Resilience ENCRYPT researchers presented four papers on securing federated learning, enhancing healthcare data confidentiality, simplifying differential privacy and accelerating fully homomorphic encryption. On September 3, at the 21st EMCIS Conference (Athens), ENCRYPT showcased its latest innovations in data privacy and their practical applications. These workshops highlight ENCRYPT's commitment to advancing secure data processing and fostering knowledge exchange in the field.

Read more: https://encrypt-project.eu/communication/news/encrypt-organises-two-september-workshops/ and https://encrypt-project.eu/communication/news/encrypt-paper-presentations-september-2024/

1st EASiNet Scientific Remote Meeting

On September 13, 2024, the first EASiNet Scientific Remote Meeting convened 25 consortium members to discuss the progress of EASiNet projects. Professor Salvatore D'Antonio from the University of Naples Parthenope presented the ENCRYPT Project during this session.

Read more: https://encrypt-project.eu/communication/news/1st-easinet-scientific-remote-meeting/

ENCRYPT Project at GLACIATION Dissemination Event: Privacy-Preserving Technologies in Smart Environments

High-level discussion
Harmonising Privacy-Preservation and Interoperability in Smart Environments
10th October,2024
From 17:00 to 19:00
Leibniz University Hannover: TIB Library - Vortragsraum
https://glaciation-project.eu/
GLACIATION

On October 10, 2024, Marco Bassini represented the ENCRYPT project at the GLACIATION Horizon-funded dissemination event hosted by Leibniz University Hannover, discussing privacy-preserving technologies in smart environments.

Read more: https://encrypt-project.eu/communication/news/encrypt-project-at-glaciation-dissemination-event-privacy-preserving-technologies-in-smart-environments/

Other Activities

- On October 16-17, 2024, the ENCRYPT project participated in the RISE-SD conference in Chalkidiki, Greece, featuring a dedicated booth to showcase its advancements in privacy-preserving technologies.
  Read more: https://encrypt-project.eu/communication/news/encrypt-presence-at-the-rise-sd-conference/
- On October 22, 2024, the European AI Security Network (EASiNet) hosted a CrossTalk event at the Delegation of the European Union to Japan, bringing together ten EU-funded projects and European authorities to discuss AI and cybersecurity solutions. The ENCRYPT project was among the participants, contributing to dialogues on advancing AI in healthcare.
  Read more: https://encrypt-project.eu/communication/news/european-ai-security-network-crosstalk-event-leading-the-future-of-ai-in-healthcare/

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.

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

JGU 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

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.