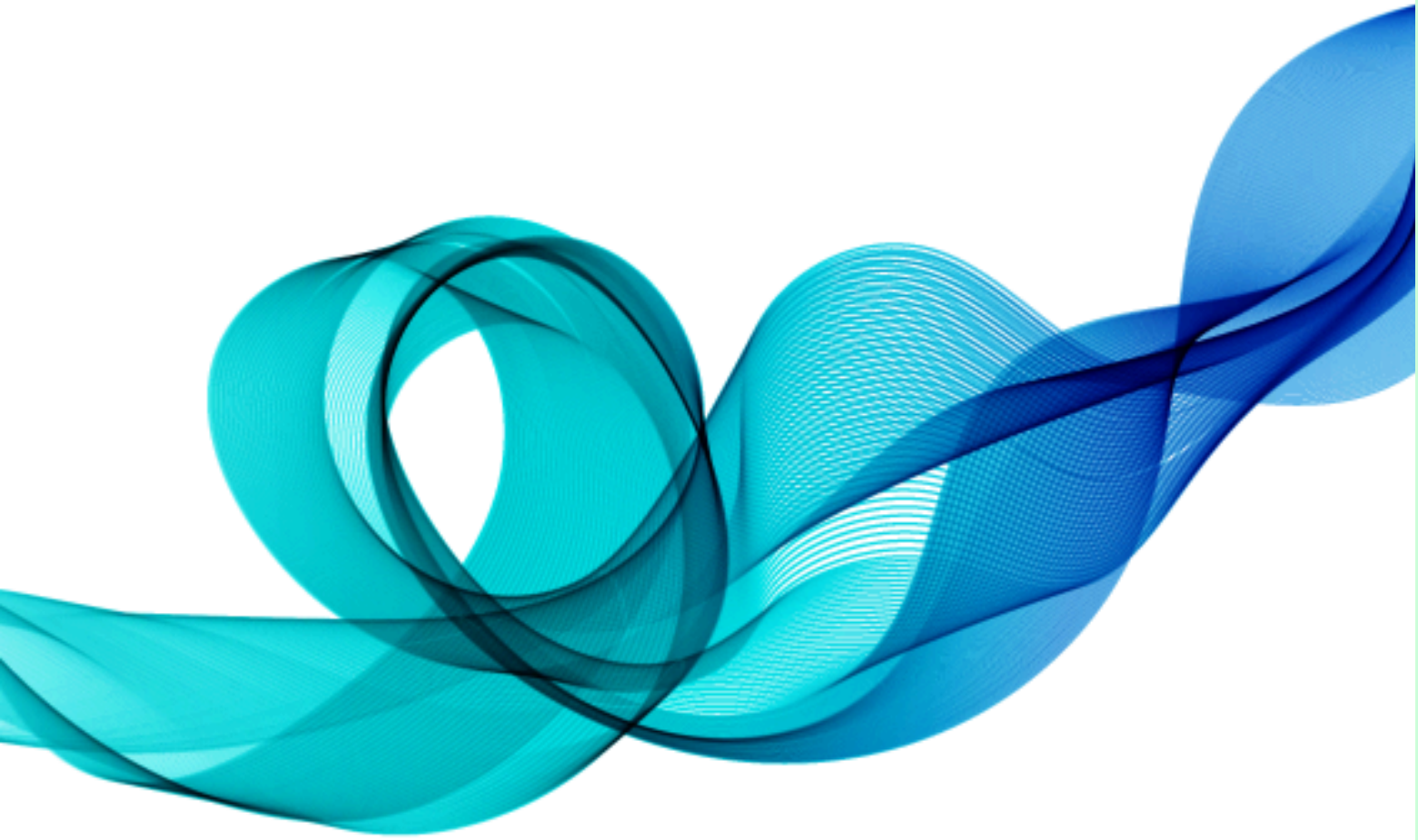
HARPOCRATES

Informe Técnico de HARPOCRATES

Análisis con Preservación de Privacidad para Ciberseguridad y Salud



Contenido

Introducción

HARPOCRATES es un proyecto de investigación financiado por el programa Horizon Europe, con la participación de 13 socios de 9 países. El proyecto desarrolla y valida herramientas de procesamiento de datos seguras que permiten a las organizaciones analizar y compartir información sensible sin revelar los datos originales.

Aplica criptografía avanzada y aprendizaje automático con preservación de la privacidad en dos demostradores principales:

- **Compartición de Inteligencia de Amenazas entre Administraciones Públicas**
- **Análisis del Sueño para el Soporte a la Toma de Decisiones Clínicas en Medicina del Sueño**

Las herramientas y métodos desarrollados son modulares, conformes al reglamento RGPD y adaptables a otros sectores como movilidad, energía y finanzas.

Objetivos del Proyecto

El proyecto HARPOCRATES surge de la necesidad de habilitar análisis de datos seguros y respetuosos de la privacidad en sectores sensibles.

Estos objetivos guían el trabajo técnico y aplicado del proyecto, garantizando la confidencialidad sin comprometer la capacidad analítica:

- Capacidad de análisis de datos cifrados
- Aplicación de criptografía y privacidad diferencial
- Entrenamiento de modelos sin necesidad de compartición de datos
- Desarrollo de sistemas robustos frente a datos de entrada maliciosos
- Validación de casos de uso en sectores de ciberseguridad y salud
- Desarrollo de herramientas conformes al reglamento RGPD
- Automatización de las garantías de privacidad
- Transformación de los resultados de investigación en soluciones aplicables en el mercado

Concepto del Proyecto

El proyecto HARPOCRATES se basa en la idea de que la privacidad de los datos y su utilidad pueden coexistir. Las organizaciones dependen cada vez más de la disponibilidad de datos sensibles — para poder llevar a cabo el análisis de los mismos historiales clínicos o registros del sistema — para poder llevar a cabo el análisis de los mismos, pero las restricciones legales y éticas a menudo limitan el intercambio de estos datos.

HARPOCRATES aborda este desafío habilitando el análisis de datos cifrados mediante técnicas criptográficas avanzadas como los ciffrados homomórfico y funcional, el aprendizaje federado y la privacidad diferencial.

En lugar de aplicar un enfoque único para todos los casos, el proyecto adopta una arquitectura modular que contempla distintos tipos de datos y entornos operativos, al tiempo que contempla diferentes escenarios de amenaza. Los diferentes componentes de la arquitectura -modelos de cifrado para el aprendizaje automático, herramientas para la detección de anomalías y herramientas para el cumplimiento del reglamento RGPD- están diseñados para ser fácilmente interoperables e integrables.

Principales Innovaciones Técnicas

Se han desarrollado e integrado una serie de técnicas criptográficas y de mejora de la privacidad para permitir el análisis seguro de datos potencialmente sensibles en distintos entornos.

Cifrado Homomórfico (HE): Procesamiento de datos sin descifrado

Cifrado Funcional (FE): Divulgación controlada de los resultados

Aprendizaje Federado (FL): Entrenamiento sin centralizar los datos

Privacidad Diferencial (DP): Protección estadística de los datos personales

Pipelines de Detección de Amenazas: Detección de anomalías con privacidad

Modelos de ML Cifrados: Clasificación de señales sensibles

DEMOSTRADOR 1

Compartición de Inteligencia de Amenazas

Compartición segura de inteligencia de amenazas entre autoridades públicas que colaboran para la detección de ciberamenazas.

Objetivo: Permitir que autoridades locales colaboren en la detección de ciberataques-coordinados o no-sin exponer los registros originales de la actividad de sus usuarios.

Fuente de Datos:

- Registros de actividad en el sistema operativo Windows
- Procesos comunes como `powershell.exe` `cmd.exe` `explorer.exe`

Flujo de Trabajo:

- Extracción estructurada de características de registros del sistema
- Entrenamiento local de modelos en cada institución
- Detección de anomalías por proceso monitorizado
- Intercambio cifrado de alertas mediante HHE
- Correlación entre instituciones para detectar campañas distribuidas

Resultados:

✓ Compartición segura de ciberinteligencia
✓ Inteligencia de amenazas conforme al reglamento RGPD
✓ Escalable a contextos nacionales tipo CSIRT/CERT

DEMOSTRADOR 2

Análisis del Sueño en Entorno Médico

Análisis clínico cifrado para clasificación de etapas del sueño

Objetivo: Facilitar la investigación multiinstitucional de datos del sueño sin comprometer la privacidad del paciente.

Fuente de Datos

- Hipnogramas derivados de EEG
- Etapas etiquetadas: Wake REM N1 N2 N3

Flujo de Trabajo:

- Extracción local de características de datos de series temporales
- Cifrado utilizando HE y FE
- Entrenamiento de clasificadores sobre datos cifrados
- Inferencia sobre datos cifrados
- Compartición de resultados sin revelar los datos de entrada

Resultados:

✓ Precisión de hasta 87.55%
✓ Preserva la confidencialidad médica
✓ Soporta escalabilidad clínica y de investigación

Herramientas y Componentes

Para respaldar los demostradores, HARPOCRATES desarrolló herramientas modulares que combinan criptografía, aprendizaje automático y protección de datos. Estas herramientas están diseñadas para integrarse fácilmente y cumplir con el reglamento RGPD.

Motor SPADE: Detección de anomalías en registros del sistema

Wrappers de ML Cifrados: Entrenamiento e inferencia con HE/FE

Pipelines con Preservación de Privacidad: Para flujos de trabajo de ML

Bancos de pruebas y marcos de evaluación

Módulos de mapeo de cumplimiento con RGPD

Impacto Técnico

Las tecnologías desarrolladas en HARPOCRATES están diseñadas para su aplicación real en sectores sensibles.

Permite el análisis seguro en entornos críticos

Aplica la investigación criptográfica académica a contextos operativos

Demuestra el uso aplicado de ML cifrado

***Resultados:** El proyecto proporciona herramientas de código abierto reutilizables, junto con guías de despliegue e integración, y reportes sobre precisión y escalabilidad.*

Contacto

Coordinador General: Tampere University, Tampere, Finland

Coordinador Técnico: University of Westminster, London, United Kingdom

Escanee este código QR para conectarse con HARPOCRATES

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101069535.

UK Research and Innovation

UK participant in Horizon Europe Project HARPOCRATES is supported by UKRI grant number 10048312.