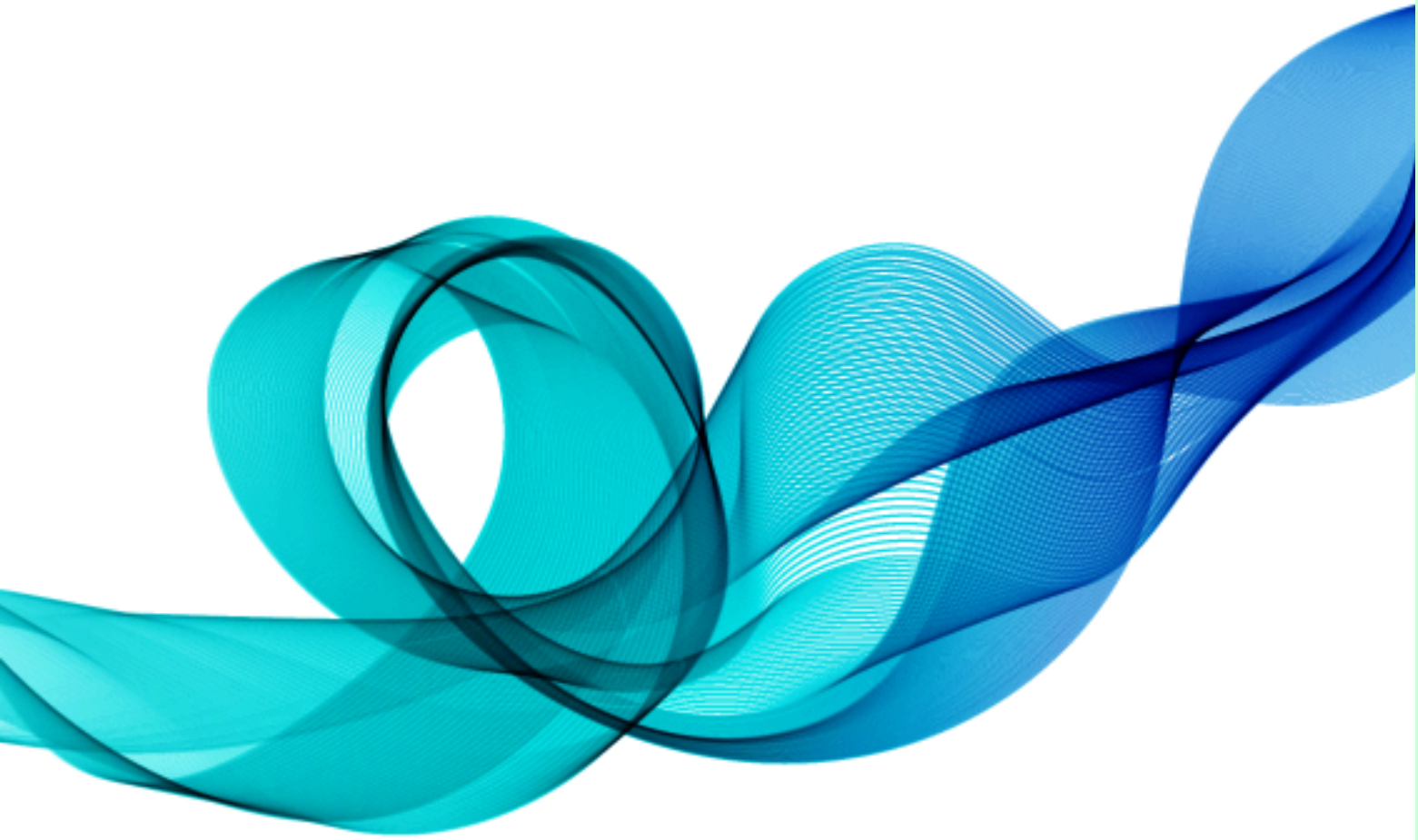
HARPOCRATES

Technischer Bericht zu HARPOCRATES

Datenschutzfreundliche Analysen für Cybersicherheit und Gesundheit



Inhaltsverzeichnis

Einleitung

Projektübersicht HARPOCRATES ist ein von Horizon Europe finanziertes Forschungsprojekt mit 13 Partnern aus 9 Ländern. Ziel des Projekts ist es, sichere Datenverarbeitungstools zu entwerfen und zu validieren, die es Organisationen ermöglichen, sensible Informationen zu analysieren und auszutauschen, ohne die Rohdaten offenzulegen.

Das Projekt wendet fortschrittliche Kryptografie und datenschutzfreundliches maschinelles Lernen auf zwei zentrale Demonstratoren an:

- **Bedrohungsinformationsaustausch für öffentliche Verwaltungen**
- **Schlafdatenanalyse zur klinischen Entscheidungsunterstützung**

Die Tools und Methoden sind modular aufgebaut, DSGVO-konform und auf Bereiche wie Mobilität, Energie und Finanzen übertragbar.

Projektziele

Projektziele Das Projekt HARPOCRATES zielt darauf ab, datenschutzfreundliche Analysen in sensiblen Bereichen zu ermöglichen.

Diese Ziele leiten die technische und praktische Arbeit im Projekt und stellen sicher, dass Vertraulichkeit gewahrt bleibt, ohne analytische Fähigkeiten einzuschränken:

- Analyse verschlüsselter Daten ohne Offenlegung
- Kombination von Kryptografie und Differential Privacy
- Modelltraining ohne Datenaustausch
- Robustheit gegenüber böswilligen Eingaben
- Validierung in Cybersicherheit und Gesundheit
- DSGVO-konforme modulare Tools bereitstellen
- Automatisierung von Datenschutzgarantien
- Umsetzung wissenschaftlicher Forschung in praxisnahe Lösungen

Projektkonzept

HARPOCRATES basiert auf der Idee, dass Datenschutz und Datenverwendbarkeit koexistieren können. Organisationen verlassen sich zunehmend auf sensible Daten – wie Gesundheitsakten oder Systemprotokolle – für Analysen, doch rechtliche und ethische Vorgaben schränken den Datenaustausch ein.

HARPOCRATES begegnet dieser Herausforderung, indem es Analysen verschlüsselter Daten mithilfe fortschrittlicher kryptografischer Methoden wie homomorpher und funktionaler Verschlüsselung, föderiertem Lernen und Differential Privacy ermöglicht.

Anstelle eines Einheitsansatzes verfolgt das Projekt eine modulare Architektur, die unterschiedliche Datentypen, Betriebsumgebungen und Bedrohungsszenarien unterstützt. Komponenten wie verschlüsselte ML-Modelle, Werkzeuge zur Anomalieerkennung und DSGVO-Module sind interoperabel und lassen sich leicht integrieren.

Kerninnovationen

Eine Reihe kryptografischer und datenschutzfördernder Techniken wurde entwickelt und integriert, um sichere Datenanalysen in verschiedenen Szenarien zu ermöglichen.

Homomorphe Verschlüsselung (HE):
Datenverarbeitung ohne Entschlüsselung

Homomorphe Verschlüsselung (HE):
Datenverarbeitung ohne Entschlüsselung

Föderiertes Lernen (FL):
Dezentralisiertes Modelltraining

Differential Privacy (DP):
Statistischer Schutz personenbezogener Daten

Anomalie-Erkennungspipelines:
Datenschutzfreundliche Detektion

Verschlüsselte ML-Modelle:
Klassifikation sensibler Signale

DEMONSTRATOR 1

Bedrohungsinformationsaustausch

Sichere Erkennung von Cyberangriffen durch öffentliche Stellen

Ziel: Lokale Behörden sollen gemeinsam koordinierte Angriffe erkennen können, ohne Rohdaten offenzulegen.

Datenquellen:

- Windows Sysmon-Protokolle
- Prozesse wie `powershell.exe` `cmd.exe` `explorer.exe`

Ablauf:

- Strukturelle Merkmalsextraktion aus Systemlogs
- Lokales Modelltraining je Institution
- Anomalieerkennung pro beobachtetem Prozess
- Verschlüsselter Austausch von Warnungen mittels FE
- Korrelation über Institutionen hinweg zur Erkennung koordinierter Kampagnen

Ergebnisse:

- ✓ Sicherer Signalaustausch
- ✓ DSGVO-konforme Bedrohungsinformationen
- ✓ Skalierbarkeit für nationale CSIRT-/CERT-Strukturen

DEMONSTRATOR 2

Schlafanalyse in der Medizin

Verschlüsselte klinische Analyse zur Schlafstadienklassifikation

Ziel: Multiinstitutionelle Forschung zu Schlafdaten ermöglichen, ohne Patientendaten offenzulegen.

Datenquellen:

- Aus dem Schlaf-EEG abgeleitete Hypnogramme
- Annotierte Schlafstadien: Wake REM N1 N2 N3

Ablauf:

- Lokale Merkmalsextraktion aus Zeitreihendaten
- Verschlüsselung mit HE und FE
- Training von Klassifikatoren auf verschlüsselten Daten
- Inferenz auf verschlüsselten Daten
- Ergebnisweitergabe ohne Offenlegung der Eingabedaten

Ergebnisse:

✓ Klassifikationsgenauigkeit bis zu 87,55 %
✓ Wahrung medizinischer Vertraulichkeit
✓ Skalierbarkeit für Forschung und Klinik

Tools und Komponenten

Zur Unterstützung der Demonstratoren wurden modulare Tools entwickelt, die Kryptografie, maschinelles Lernen und Datenschutz kombinieren. Sie sind leicht integrierbar und erfüllen DSGVO-Anforderungen.

SPADE Engine: Anomalieerkennung in Systemprotokollen

ML Wrapper für HE/FE: Training und Inferenz mit verschlüsselten Modellen

Privacy-preserving ML Pipelines: Datenschutzfreundliche Workflows

Testumgebungen und Bewertungsrahmen

DSGVO-Mapping-Module

Technische Wirkung

Die entwickelten Technologien sind für den praktischen Einsatz in sensiblen Bereichen ausgelegt.

Sichere Analysen in kritischen Bereichen

↓

Umsetzung akademischer Kryptografie in der Praxis

↓

Angewandte Demonstration von verschlüsseltem ML

↓

***Ergebnisse:** Das Projekt liefert wiederverwendbare Open-Source-Tools, Anleitungen zur Integration und Berichte zu Genauigkeit und Skalierbarkeit.*

Kontakt

Gesamtkoordination: Tampere University, Tampere, Finland

Technische Koordination: University of Westminster, London, United Kingdom

Scannen Sie diesen QR-Code, um sich mit HARPOCRATES zu verbinden

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.