Simplifying Differential Privacy for Non-Experts

The ENCRYPT Project Approach

Enhancing Data Security and Utility Across Federated Data Spaces

encrypt

02/09/2024

Overview of Data Privacy Challenges

- **Data Explosion**: Massive amounts of data driving research and innovation
- **Privacy Risks**: Cybersecurity threats and data misuse
- **Regulatory Compliance**: Importance of adhering to GDPR and other regulations
- **Public Concerns**: Growing demand for stronger privacy measures
- **ENCRYPT Project**: Aims to enhance data security and privacy across federated data spaces.

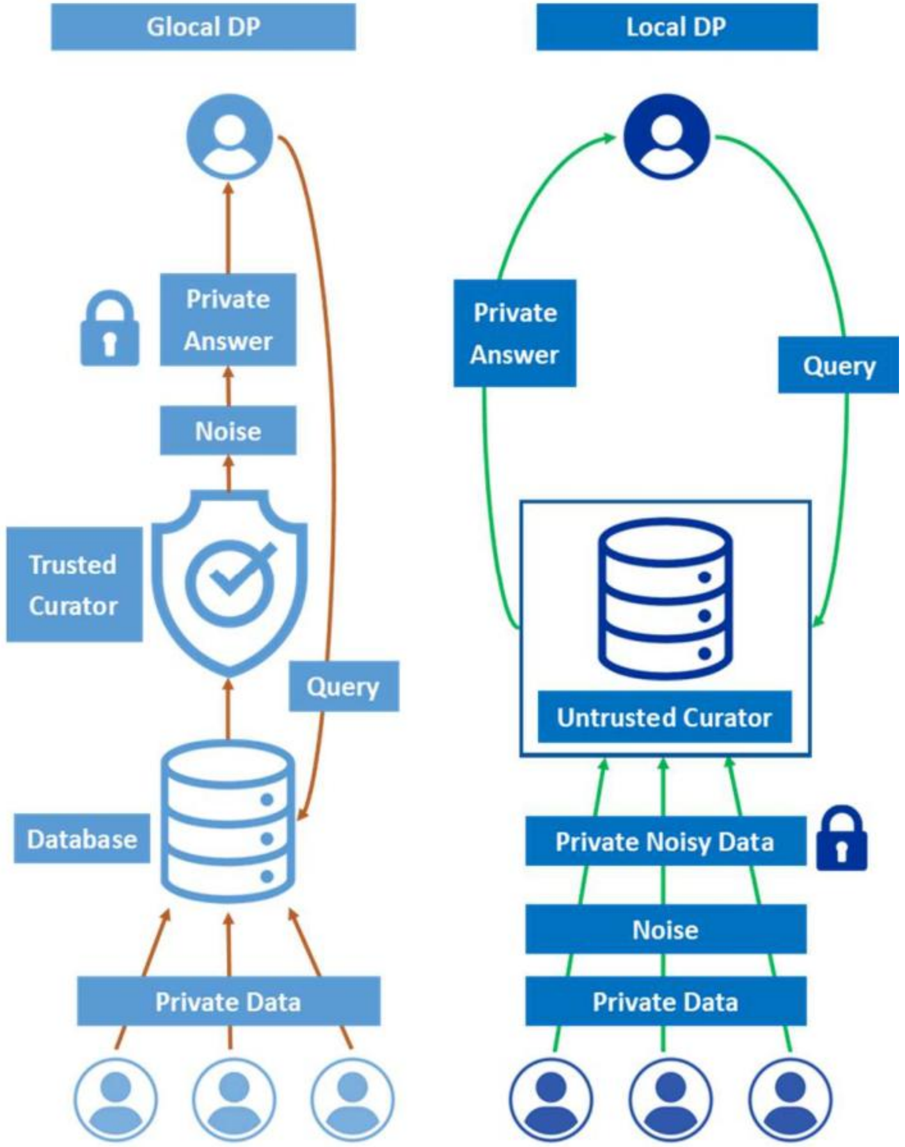
What is Differential Privacy?

- **Core Concept**: Protects individual privacy by adding noise to data
- **Mathematical Foundation**: Balances privacy with data utility using the privacy loss parameter (ε)
- **Key Feature**: Ensures statistical analysis results are consistent whether or not a specific individual's data is included
- **Real-World Applications**: Used by companies like Apple, Google, and in the U.S. Census

encrypt

Local vs. Global Differential Privacy

- Local Differential Privacy (LDP):
  - ✓**Privacy at the Source**: Noise added before data leaves the user’s device
  - ✓**Use Case**: Ideal when users don’t fully trust the data collector (e.g., Apple iOS)
- Global Differential Privacy (GDP):
  - ✓**Privacy at the Server**: Noise added at a centralized database
  - ✓**Use Case**: Suitable for large-scale analysis with a trusted central entity (e.g., U.S. Census)
- ENCRYPT's Choice:
  - ✓Focuses on LDP to empower user control over data privacy



Differential Privacy in the ENCRYPT Project

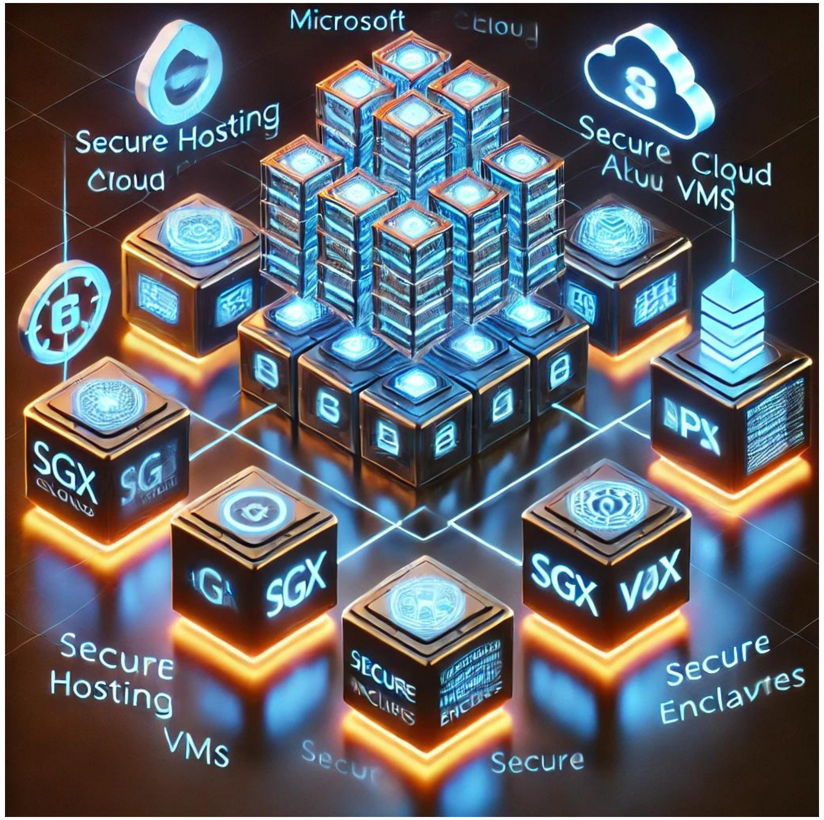
- **Key Application**: Focus on the fintech sector for secure data sharing
- **Collaboration Example**: EXUS as service provider and EPIBANK as data steward
- **Main Objective**: Enable secure machine learning model training with anonymized data
- **User-Centric Approach**: Simplifies DP usage for non-experts through automated recommendations

The ENCRYPT Platform Architecture

- **Modular Design**: Flexible and scalable structure for integrating various technologies
- Key Components:
  - ✓ **User Interface**: Accessible design for non-experts
  - ✓ **Secure Hosting**: Microsoft Azure Cloud with SGX-enabled VMs for secure enclaves
  - ✓ **APIs and Communication**: Ensures reliable and consistent interaction between components
- **Purpose**: Facilitates secure, efficient, and GDPR-compliant data processing

Making DP Accessible with the Recommendation Engine

- **AI-Driven Recommendations**: Suggests appropriate privacy-preserving technologies
- **Customizable**: Tailored suggestions based on user's data and privacy needs
- **Continuous Updates**: Adapts to new research, technologies, and regulations
- **User-Centric Design**: Provides explanations to build trust and understanding



User Interaction and Workflow in ENCRYPT

- **User-Friendly Interface**: Simplifies data pre-processing and privacy parameter selection
- **Local Noise Addition**: Privacy-enhancing noise is added locally on the user's device
- **Secure Data Upload**: Noised data is securely uploaded to the ENCRYPT platform
- **Automated Model Training**: ENCRYPT trains and optimizes AI models using the noised data
- **Consistent Analysis**: Users can apply the same privacy settings to new datasets for consistent results

Artificial Neural Networks

Validating DP in Real-World Scenarios

- **Fintech Use Case**: Applied DP in financial data analysis
- **Experiment Results**: High accuracy (~88%) even with significant noise added
- **Key Insight**: DP maintains data utility while ensuring strong privacy protections
- **Practical Impact**: Demonstrates the feasibility of DP for real-world applications in sensitive domains

Decision Tree Classifier

Gaussian Naive Bayes

encrypt

Future Challenges and Research Directions

- **Privacy vs. Utility Trade-off**: Balancing strong privacy with high data accuracy
- **Scalability Issues**: Addressing computational challenges with large datasets
- **User-Friendly Tools**: Need for more intuitive interfaces for non-experts
- **Interoperability**: Ensuring seamless integration with various systems and platforms

Summary

- **ENCRYPT's Mission**: Simplifies privacy-preserving technologies for non-experts
- **DP's Role**: Balances data utility and privacy effectively
- **Real-World Impact**: Proven applicability in sectors like finance
- **Looking Forward**: Continued innovation needed to address challenges and expand use cases

Q&A

https://encrypt-project.eu/

in encrypt-project

@encrypt_project