PRIVACY-PRESERVING INFORMATION SHARING IN P2P ENVIRONMENTS

Christina Karakosta, Prof William J. Knottenbelt
Department of Computing, Faculty of Engineering, Imperial College London.

MOTIVATION

- Large volume of **Personally Identifiable Information (PII)**.
- More data means **more risk**.
- Data sharing schemes should follow **stringent regulations** (GDPR, CCPA, HIPPA, PCI DSS, SOC2, etc.)
- Trade-off between data privacy or data utility

How can we manage sensitive data having the best of both privacy and utility?

OBJECTIVES

- To propose a **novel privacy-enhancing data sharing approach** that can be applied in multidisciplinary fields, including healthcare and financial institutions.
- To provide **data protection guarantees** for creating a decentralized trust environment.
- To facilitate **sensitive information management and control** over information flows.
- To enhance **inter-organisational data sharing** by removing the barriers of interoperability without compromising privacy.

INTRODUCTION

Privacy-Enhancing Technologies (PETs) move the pareto frontier to enable more of both privacy and transparency at the same time. The promising PETs aim to create information flows within society that maximize social good with less risk, higher accuracy, faster, and with better aligned incentives.

Currently, **Secure Multi-Party Computation (MPC)** and **Fully Homomorphic Encryption (FHE)** are two prevelant approaches in Privacy Engineering. However, FHE schemes are still prohibitively expensive to be easily adopted [1].

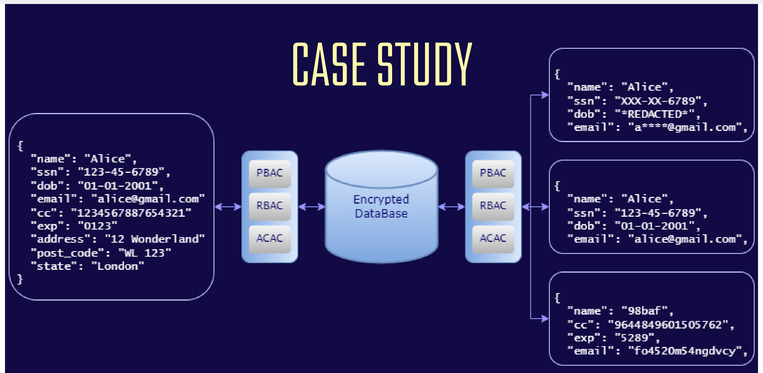
POLYMORPHIC ENCRYPTION

Polymorphic Encryption (PE) enables the data to be encrypted in multiple forms, with multiple keys, and with specific funtions for the data associated with each encryption set [2].

PE can be considered as a lock with a wheel where different keys fit to open the lock [3].

PE provides a flexible, secure, and computationally faster environment.

CASE STUDY



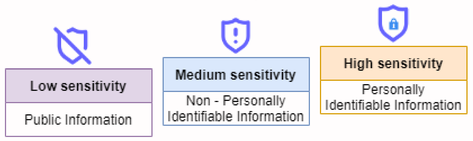
FinTech

- *Securily store and access customer user PII and PCI data such as name, email and banking information.*
- *Protect the sensitive data using PE, Data De-Identification and Tokenization.*
- *Control the life cycle of tha data throughout the enviornment.*

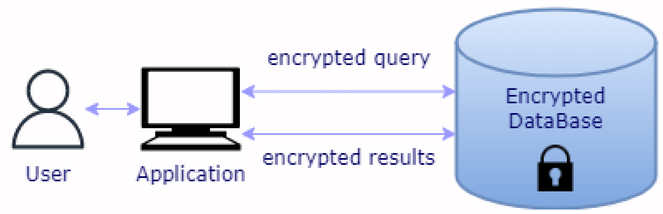
OVERVIEW OF THE PROPOSED FRAMEWORK

- A system that executes **queries** over encrypted data using **Polymorphic Encryption (PE)**.
- Different data can be treated with differenent encryption techniques based on their **sensitivity levels**.
- High sensitive data that disclose PII must be securely encrypted throughout the different **data states**.
- **PE** assists to **improve** the **performance** and the **time cost** of the system.
- An **API intergration** can configure a **data governance engine** to control how different users would access data based on the level of information that they need in order to perform a legitimate business function.

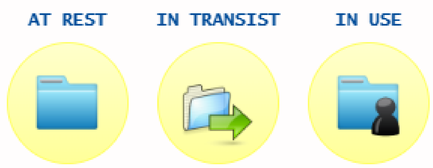
Data Sensitivity Levels



Query Encryption Scheme



Data States



CONCLUSIONS & FUTURE WORK

PE enables selected operations on partial data based on the information that different users need to accomplish their function. Hence, PE can provide a dynamic and flexible infrastructure for data sharing by improving the performance and time cost. In future work, we aim to extend the implementation of the proposed framework to more case studies like the healthcare sector. Also, similar manipulations can be suggested to attain better performance and privacy without increasing the implementation cost.

REFERENCES

1. Popa, R.A., Redfield, C.M., Zeldovich, N. and Balakrishnan, H., 2011, October. CryptDB: protecting confidentiality with encrypted query processing. In Proceedings of the twenty-third ACM symposium on operating systems principles (pp. 85-100).
2. Booher, D.D., Cambou, B., Carlson, A.H. and Philabaum, C., 2019, January. Dynamic key generation for polymorphic encryption. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0482-0487). IEEE.
3. PEVerheul, E., Jacobs, B., Meijer, C., Hildebrandt, M. and de Ruiter, J., 2016. Polymorphic encryption and pseudonymisation for personalised healthcare. Cryptology ePrint Archive.

STAY TUNED