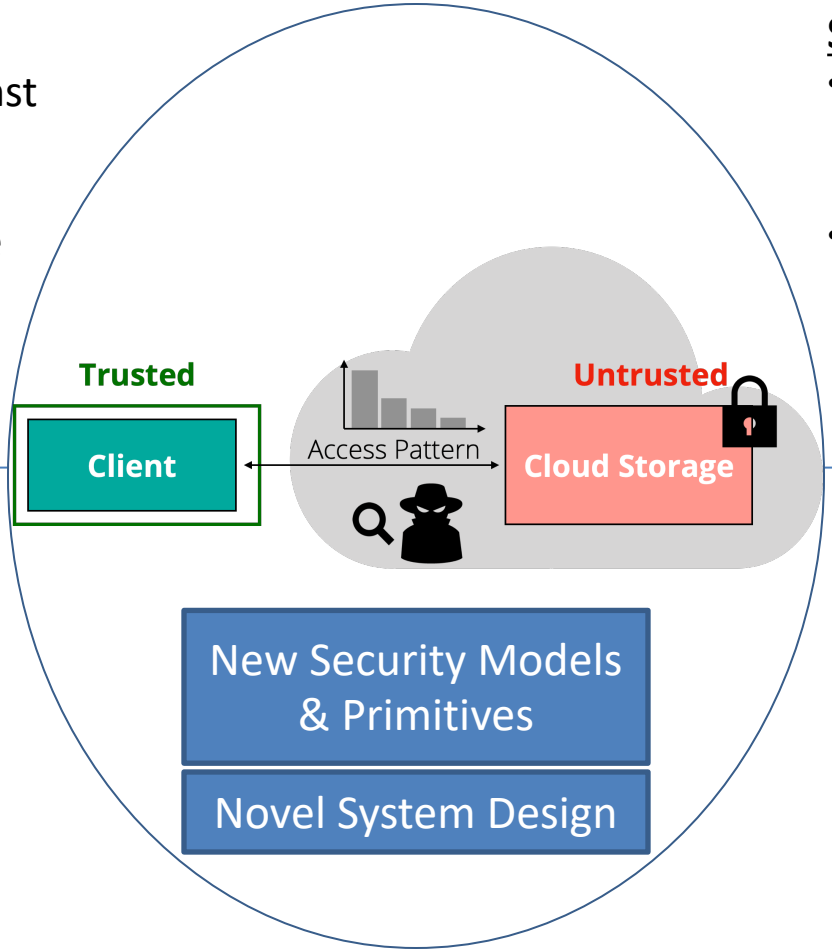
# Mixed Distribution Models for Encrypted Data Stores

## Challenge:

- Countermeasures against access pattern and length leakage impractical at scale due to high bandwidth/storage overheads

## Solution:

- Model leaked information as *mixed* distribution: unknown adversary-controlled component + known component from honest clients
- **Key insight:** Use queries from the known non-adversarial distribution to inject "noise" in a principled manner for security *and* performance




## Scientific Impact:

- Performant defense against access pattern & length leakage a long-standing problem in security.
- Can enable secure and high-performance data stores and provide new insights about tradeoff between adversarial strength and performance.

## Broader Impact and Broader Participation:

- Secure cloud storage with orders-of-magnitude lower operational costs
- Open-source research artifacts with efforts towards tech transfer.
- Education and Outreach via Yale Pathways to Science, Break Through Tech @ Cornell

**Award#2054957**
Anurag Khandelwal (Yale), Rachit Agarwal (Cornell), Thomas Ristenpart (Cornell Tech)