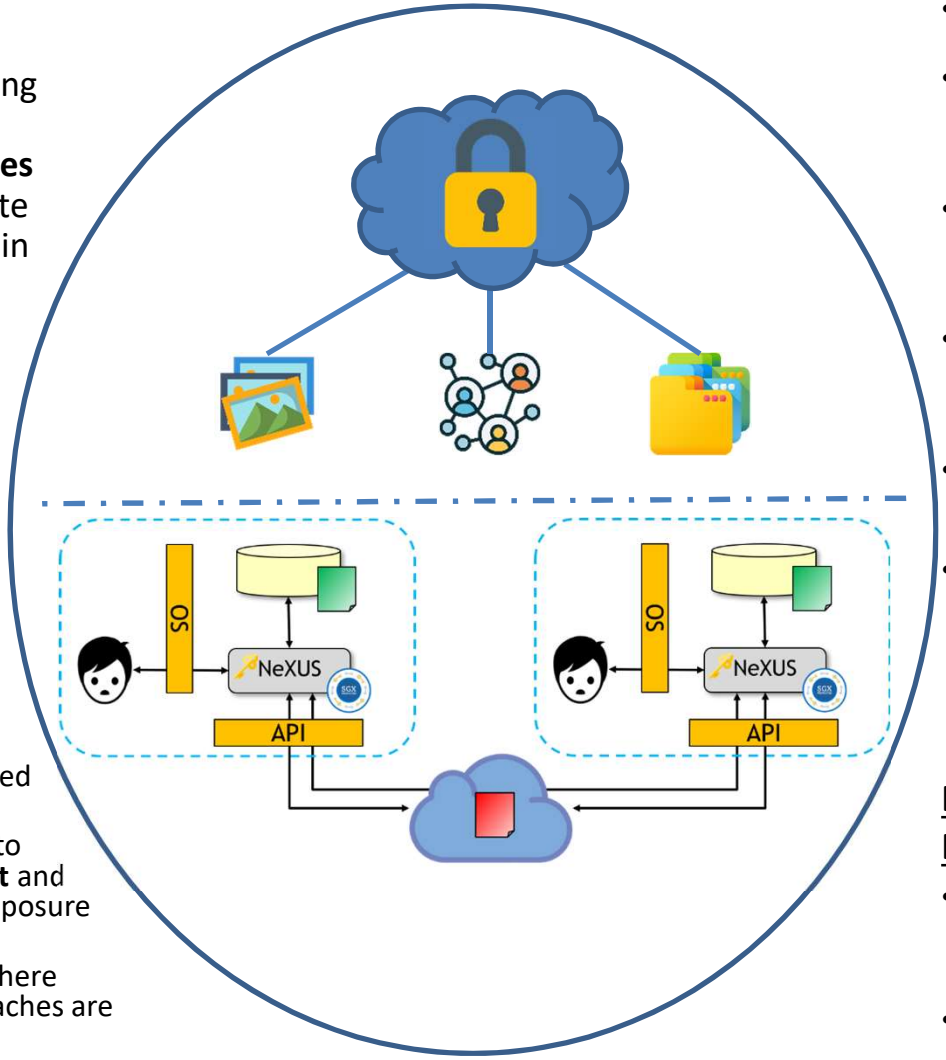
Scalable Dynamic Access Control for Untrusted Cloud Environments

Challenge: How can balancing the use of **trusted hardware** and **cryptographic approaches** to access control help mitigate the disclosure risks inherent in cloud-based data management?



Solution:

- Understand users' privacy **perceptions** of trusted hardware
- Leverage trusted hardware to **accelerate key management** and revocation by minimizing exposure
- Use enclave-based policy enforcement in scenarios where purely cryptographic approaches are cost prohibitive

CNS-1704139, CNS-1703853. University of Pittsburgh and Indiana University. Apu Kapadia, Jack Lange, Adam J. Lee.

Scientific Impact:

- Practical key revocation (CT-RSA 2018)
- Provably correct, highly performant, and storage platform agnostic cryptographic policy enforcement (DSN 2019)
- Accelerated and secure in-network streaming data processing (CODASPY 2019, DBSec 2019)
- Cost-based analyses of cloud-based access control approaches (ASIACCS 2020, TOPS 2021)
- Low overhead security isolation using lightweight kernels and TEEs (ROSS 2021)
- Understanding users' perceptions of trusted hardware in media sharing (*Ongoing*)

Broader Impact and Broader Participation:

- **User- and server-centric approaches** for performant trusted cloud storage
- **Analysis approaches** for informed decision making
- **URM** participation at the graduate and undergraduate levels