NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

School of Computer Science and Engineering
College of Engineering

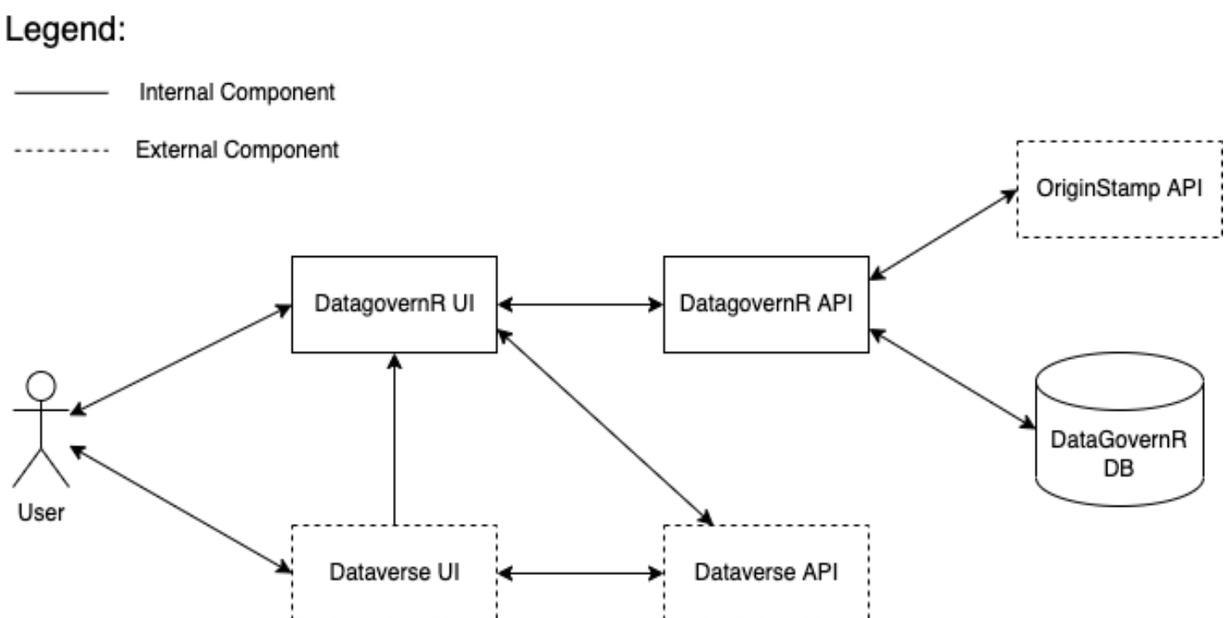
Research Data Governance

Student: Chua Chiah Soon Supervisor: Assoc. Prof Anwitaman Datta

Objectives

A web-based data archival system with:

1. Encrypted Research Data Archival
2. Encryption Key Sharing
3. Proof of Upload Time via Blockchain



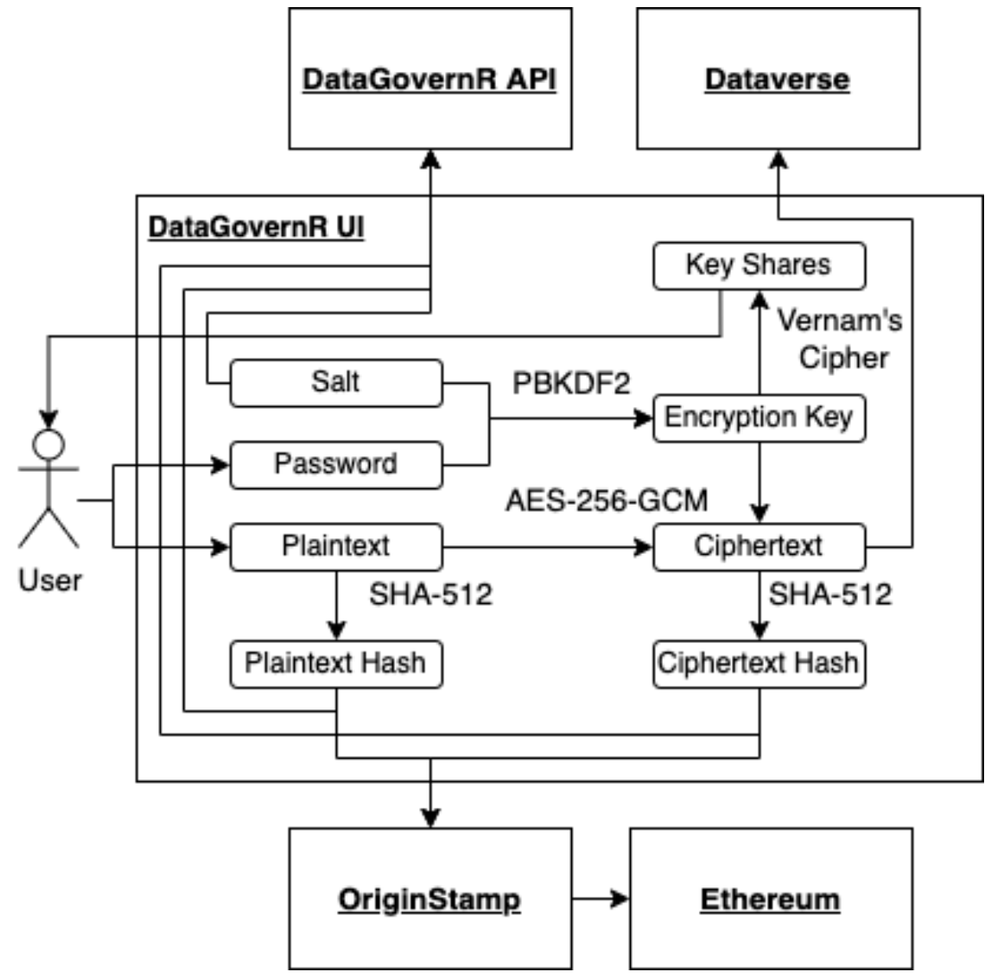
Design Principles

1. Client-side cryptography operations
2. Modular cryptographic primitives

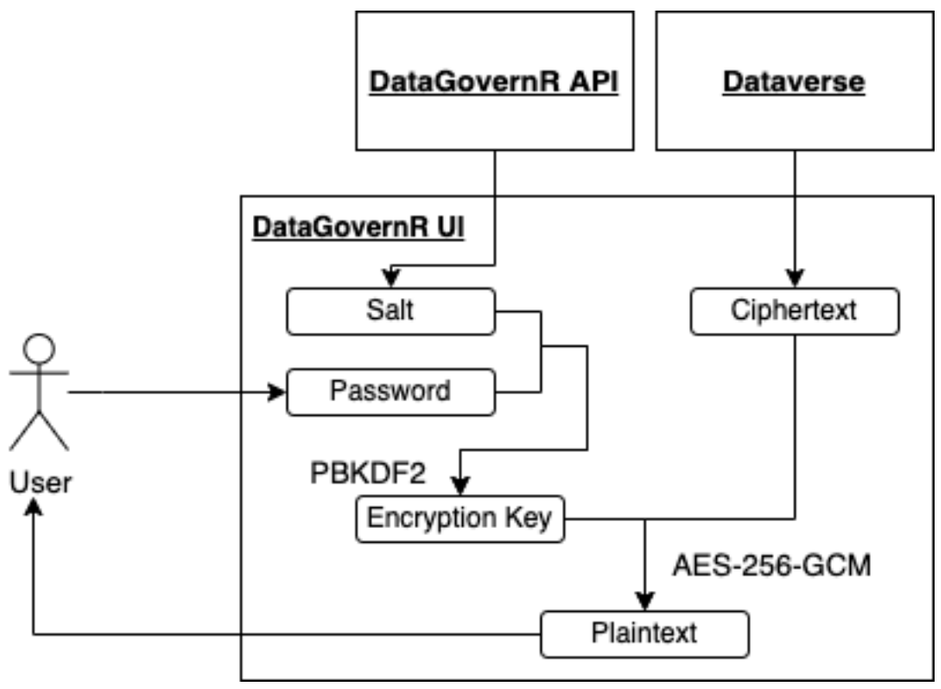
Methodology

1. Built on top of Dataverse (archival service)
2. Password-based key generation (PBKDF2) for encryption (AES-256-GCM), with different salt (and thus key) for every file
3. Key sharing using Vernam's Cipher
4. Timestamped via OriginStamp API (Ethereum) using hashes (SHA-512) of plaintext and ciphertext

Upload Process



Download Process - Password



Download Process – Key Shares