# A Zero-Knowledge Architecture for Client-Side Encryption

This presentation outlines the design and evaluation of a secure cloud storage system that removes trust from the cloud provider, ensuring user data privacy.

# The Cloud's Privacy Deficit ☁️

Standard cloud services present a fundamental privacy deficit. Even with server-side encryption, providers manage keys, allowing access or forced handover of your data. This creates vulnerabilities to breaches and surveillance.

# Bridging the Gap: Learning from Past Challenges

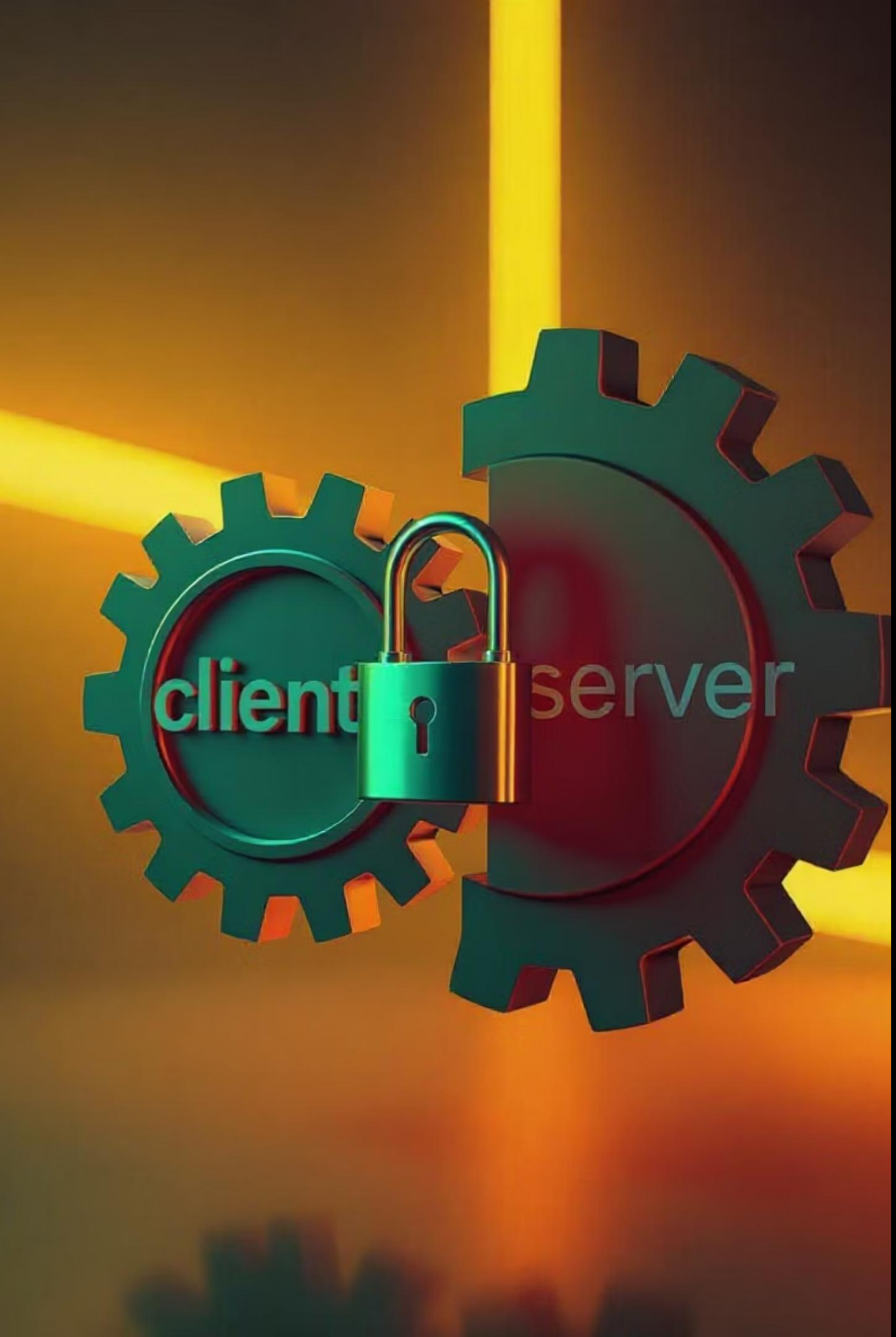
### Trust vs. Accessibility

Browser-based apps are easy to use, but their encryption code comes from the very server you distrust.

### The Adoption Paradox

Technically brilliant security tools often fail due to complex key management for average users.

Our solution addresses these historical failures by balancing robust security with pragmatic usability.



# Our Solution: A Zero-Knowledge Architecture 🔐

We designed a system where the server has zero knowledge of your unencrypted data or decryption keys. All cryptographic operations occur on your device before data is sent to the cloud.

### The Client (Trusted Zone)

Your browser performs all security operations using the built-in Web Crypto API.

### The Server (Untrusted Utility)

The server acts as a "dumb" storage utility, only storing and retrieving opaque, encrypted data blobs.

# How It Works: The Cryptographic Protocol

01

### Master Key Creation

Your password, combined with a unique salt, creates a strong Master Key via PBKDF2 (100,000 iterations).

02

### File Encryption

Each file is encrypted with a new, random File Key using AES-256-GCM for confidentiality and integrity.

03

### Key Wrapping

The unique File Key is encrypted by your Master Key before being sent to the server.

# Key Findings & Evaluation ✅

We conducted rigorous security tests based on the OWASP Web Security Testing Guide.

✓

### Zero-Knowledge Confirmed

Server only handles unintelligible ciphertext.

🛡

### Guaranteed Data Integrity

Client detects and fails decryption on tampered data.

# The Critical Trade-Off

The system's zero-knowledge strength is also its biggest usability challenge. Because the server has no access to your key, there is **no "Forgot Password" option**. Forgetting your password leads to permanent, irreversible data loss.

# Conclusion & Future Work

This project provides a validated blueprint for private-by-design cloud applications using standard web technologies.

### Future Work

Designing user-friendly key recovery systems, such as social recovery, that do not compromise the zero-knowledge principle.