H33 Demonstrates 198+ Billion Fully Homomorphic Encryption Operations Per Day -Post-Quantum Signed - on a Single Node

2,296,585M ops/sec (+/- 0.24%) of full-lifecycle encrypted pipelines off a single node combining FHE, STARK proofs, biometric AI, and post-quantum attestation.

H33 Logo

RIVERVIEW, FL, UNITED STATES, May 4, 2026 /EINPresswire.com/ -- H33.ai today announced sustained benchmark results demonstrating its post-quantum platform processing 198,424,944,000 encrypted operations per day on a single server-approximately 19× the estimated daily global financial transaction volume.

The benchmark was measured on a commercially available AWS Graviton4 c8g.metal-48xl instance, achieving 2,296,585 million full-lifecycle operations per second under sustained conditions. Each operation represents a complete pipeline: encrypted input, computation without decryption, zero-knowledge proof verification, biometric/AI evaluation, and post-quantum attestation.

> “Performance and cost have been the blockers. Those blockers are gone. The question now isn’t whether encrypted computation is possible-it’s why companies are choosing to continue exposing data?”
>
> *Eric Beans- CEO- H33.ai, Inc.*

The data never becomes plaintext.

Benchmark Summary

-Throughput: 2,296,585 million operations per second +/- 0.24% Variance
-Daily volume (single node): 198+ billion operations
-Per-operation latency: ~35–49 microseconds
-Hardware: AWS Graviton4 (192 vCPU, ARM, bare metal)
-Measurement: Sustained 120-second benchmark window
-Pipeline: BFV FHE + STARK ZKP + Biometrics + Post-Quantum Signatures

This is not a peak measurement or theoretical result. It is a sustained, reproducible benchmark

on commodity cloud hardware (CPU).

H33.ai - The World's First Complete Quantum-Proof Security Platform

What Each Operation Represents

Each of the 2,296,585 million operations per second is a complete cryptographic lifecycle-not a single arithmetic step:
-Encrypted input — data enters as ciphertext before reaching the system.
-Computation without decryption — processing occurs entirely on encrypted data
-Zero-knowledge proof (STARK) — computation is independently verifiable without exposing inputs
-Biometric / AI evaluation — identity and behavioral signals are processed within the encrypted pipeline
-Encrypted output — results remain ciphertext, readable only by the key holder
-Post-quantum attestation — results are signed under multiple NIST PQ signature families

This is not a microbenchmark of FHE math. This is millions of complete, end-to-end encrypted, provable, identity-aware pipelines per second-ingestion, computation, proof, and attestation-on a single node. At no point is data exposed in plaintext to the system performing computation.

From Encryption to Verifiable Decisions

Fully homomorphic encryption has historically been considered too slow for production use. H33's benchmark shifts the category. The system does not simply compute on encrypted data—it produces verifiable outcomes.
-The computation can be proven (STARK)
-The identity context can be evaluated (Biometrics/AI)
-The result is cryptographically attested (Post-Quantum signatures)

Each operation is not just a calculation, it is an encrypted, provable, identity-verified decision.

Pipeline Performance Breakdown

-Measured per 32-user batch:
- FHE computation (BFV): ~1,077 µs (dominant cost)
- Post-quantum signing (Dilithium): ~377 µs
- Dilithium verification: ~109 µs
- STARK verification (cached): ~0.061 µs
- SHA3 attestation digest: ~1.4 µs
- Total batch latency: ~1,565 µs

- Per-operation latency: ~49 μs

The system uses threshold cryptography (3-of-5) and operates without GPUs, relying entirely on CPU-based execution.

These numbers are independently verifiable. A live single-channel test running on the "live test" API at h33.ai consistently produces 13,000-14,000 full-lifecycle operations per second - from a single connection to a test server. The sustained benchmark represents 96-worker parallel execution on dedicated hardware.

Scale Relative to Global Systems

Global financial infrastructure processes approximately 10 billion transactions per day. A single H33 node processes:

The entire global transaction volume 19 times over while maintaining full encryption, proof, and attestation. The architecture scales horizontally across nodes and is post-Quantum by Default. Every operation is secured using NIST-standardized post-quantum cryptography, including: ML-DSA (Dilithium), FALCON+, SLH-DSA (hash-based)

Each result is bound to a compact, independently verifiable attestation (H33-74), enabling verification without exposing underlying data.

What This Unlocks:

-Financial Services
-Transaction processing where infrastructure never sees transaction data.
-Healthcare
-Encrypted patient data processing with provable non-exposure.
-Government
-Secure computation on untrusted infrastructure.
-AI / Machine Learning
-Model inference on encrypted inputs with encrypted outputs.
-Cyber Insurance
-Continuous verification of controls with cryptographic proof of system state.

About H33.ai

H33.ai builds post-quantum cryptographic infrastructure for computation, verification, and data protection. The platform integrates fully homomorphic encryption, zero-knowledge proofs, biometric/AI verification, and post-quantum signatures into a unified system designed for production deployment. H33 builds the infrastructure that proves what happened to your data - without exposing it. The platform encrypts data at creation, computes on it without decryption,

and produces post-quantum signed proof of every decision in the chain. 74 bytes. Independently verifiable. By anyone. Without trust.

Media Contact
press@h33.ai
https://h33.ai

Eric D Beans
H33.ai, Inc.
+1 813-464-0945
email us here
Visit us on social media:
LinkedIn
YouTube
X
