The FHE Landscape

Lattica surveyed cryptographers, engineers, and researchers to understand where FHE is headed. Responses reveal a mix of optimism and skepticism - progress is happening, but challenges remain.

Here's what the FHE community thinks.

Survey Participants

Education:

44% PhD

37% Master's degree

Industry:

Core Encryption Solution — 15%
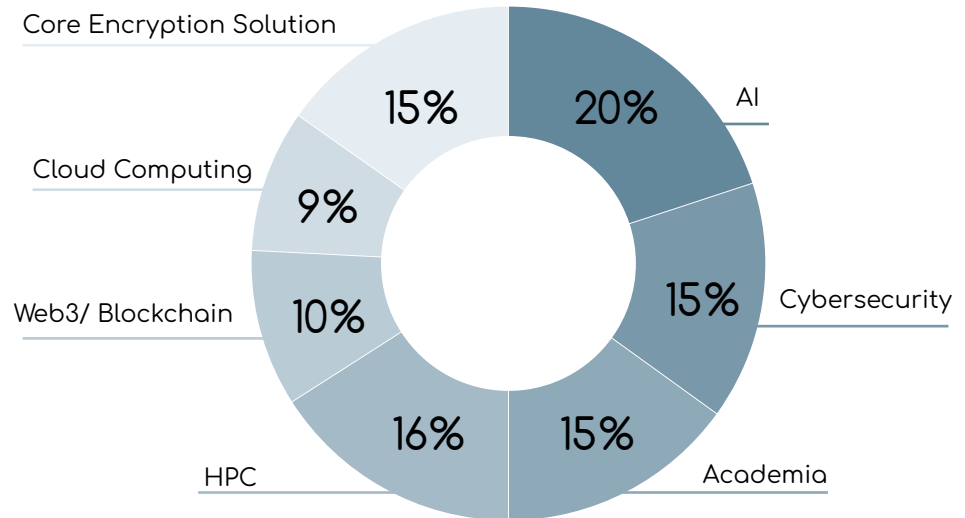
Cloud Computing — 9%

Web3/ Blockchain — 10%

HPC — 16%

AI — 20%

Cybersecurity — 15%

Academia — 15%

The FHE Landscape - 2025
Key Takeaways

1. Most respondents (41%) believe **we will see FHE in production in 3-5 years.**
   Healthcare and financial services will be first to adopt the cloud once FHE becomes mainstream.

2. Leading **commercial use cases** are:
   a. Database operations
   b. Cryptocurrency marketplaces
   c. Private inference for ML models

3. **TFHE** is the leading scheme in today's market, followed by **CKKS** and **BFV.**
   CKKS excels at approximate arithmetic on real numbers for machine learning applications,
   while TFHE specializes in boolean operations with efficient bootstrapping.

4. Most respondents (71%) believe FHE adoption will be achieved through **a combination of hardware and software.**

5. Most respondents (62%) would like to see updated **standardization of FHE security** parameters.

6. Most respondents (90%) see FHE as **intersecting with other PETs,** especially ZKPs and MPC.

FHE

Fully Homomorphic Encryption (FHE) is an advanced cryptographic technique that enables computations on encrypted data without ever decrypting it.
This means that even when data is processed by AI models, cloud services, or third parties
- its confidentiality remains intact.

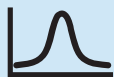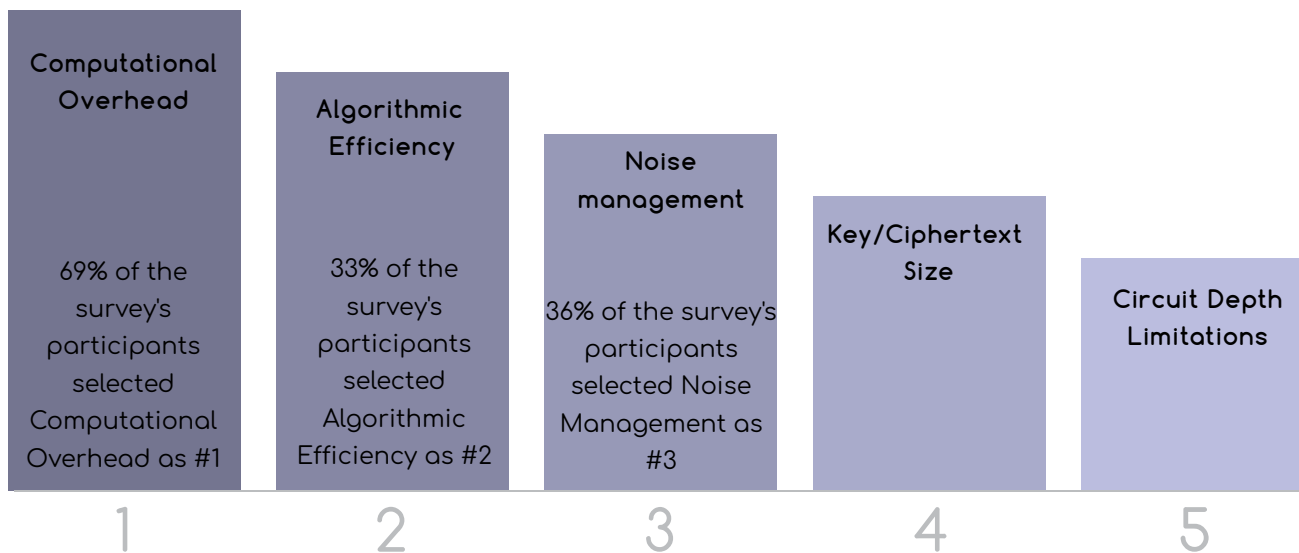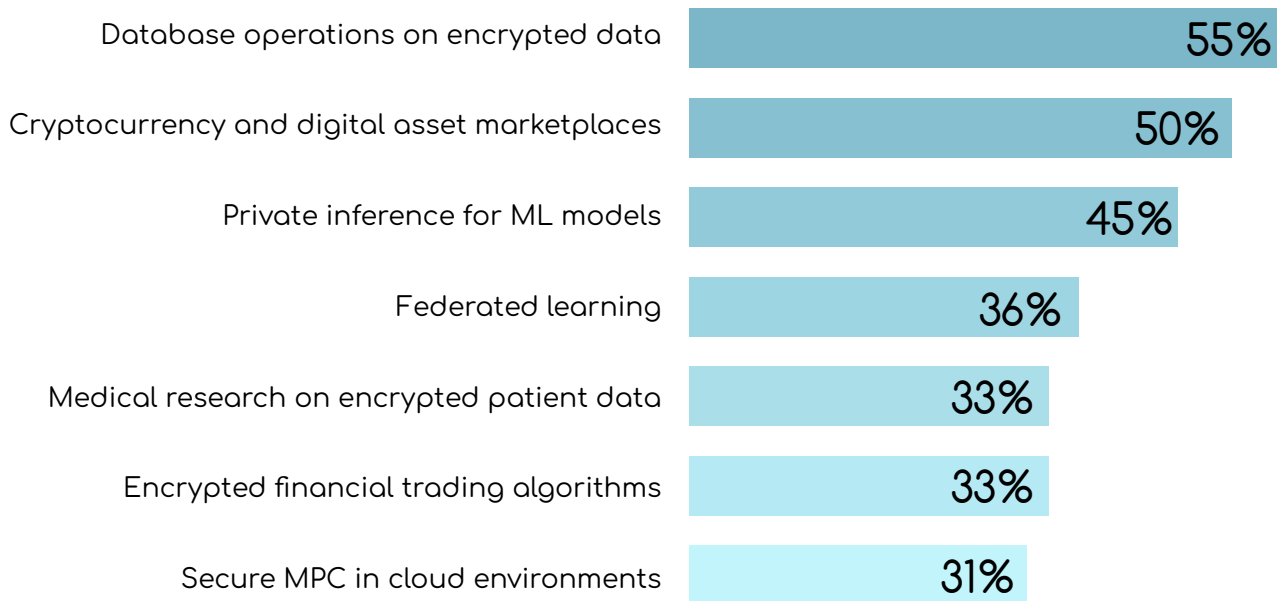| Step 1	Step 2	Step 3	Step 4
ENCRYPT ON DEVICE	**COMPUTE ON CLOUD**	**RECEIVE ENCRYPTED RESULT**	**DECRYPT ON DEVICE**
A query is encrypted directly in your browser using FHE. This ensures that Lattica never sees or stores your raw data, only its encrypted form.	The AI model runs directly on the encrypted query without first decrypting it. Lattica cannot see your input, output, or intermediate results during computation.	The model returns an encrypted prediction.	Decrypt and view the final prediction on your browser.

#1 Which aspect of FHE has the most potential to improve?
(Rank from 1-5, 1 being most critical)

Computational Overhead

69% of the survey's participants selected Computational Overhead as #1

Algorithmic Efficiency

33% of the survey's participants selected Algorithmic Efficiency as #2

Noise management

36% of the survey's participants selected Noise Management as #3

Key/Ciphertext Size

Circuit Depth Limitations

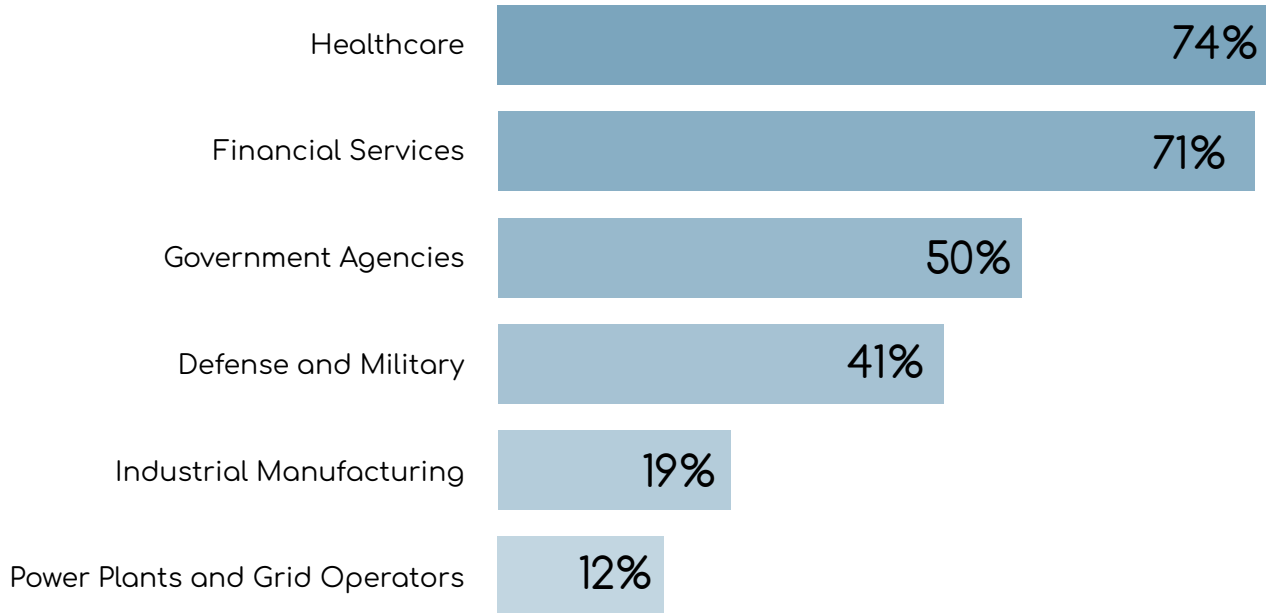1   2   3   4   5

Computational Overhead is the dominant concern for FHE, followed by **Algorithmic Efficiency** and **Noise Management.** These results highlight that despite FHE's promise, significant performance challenges remain the primary barrier to widespread adoption.

#2 What do you see as FHE's leading commercial use cases?
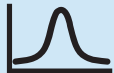### (Select all that apply)

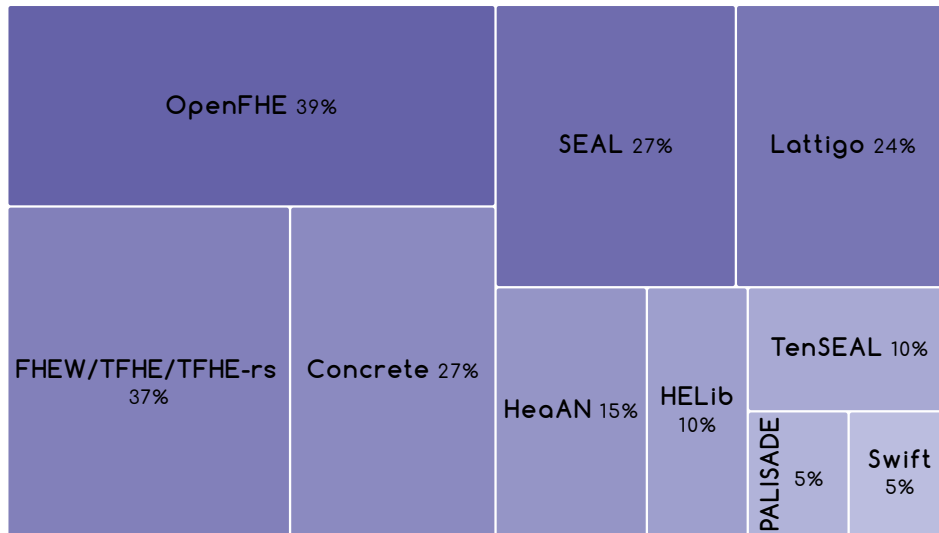| Use case	Percentage
Database operations on encrypted data	55%
Cryptocurrency and digital asset marketplaces	50%
Private inference for ML models	45%
Federated learning	36%
Medical research on encrypted patient data	33%
Encrypted financial trading algorithms	33%
Secure MPC in cloud environments	31%

#3 Which industry sectors do you believe are likely to adopt the cloud once FHE is a mainstream, financially viable solution? (Select all that apply)

Sector	Percentage
Healthcare	74%
Financial Services	71%
Government Agencies	50%
Defense and Military	41%
Industrial Manufacturing	19%
Power Plants and Grid Operators	12%

#4 Which FHE libraries are you currently working with?
(Select all that apply)

OpenFHE 39%

SEAL 27%

Lattigo 24%

FHEW/TFHE/TFHE-rs 37%

Concrete 27%

HeaAN 15%

HELib 10%

TenSEAL 10%

PALISADE 5%

Swift 5%

Instead of adding another general-purpose FHE library, Lattica focuses on removing complexity for AI applications. Our implementation of BGV and CKKS is designed for seamless integration with deep learning pipelines, ensuring that developers can leverage FHE without navigating the complexities of cryptographic parameter tuning.
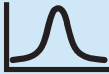
#5 Which FHE schemes are you currently working with?
(Select all that apply)

CKKS 45%

BFV 41%
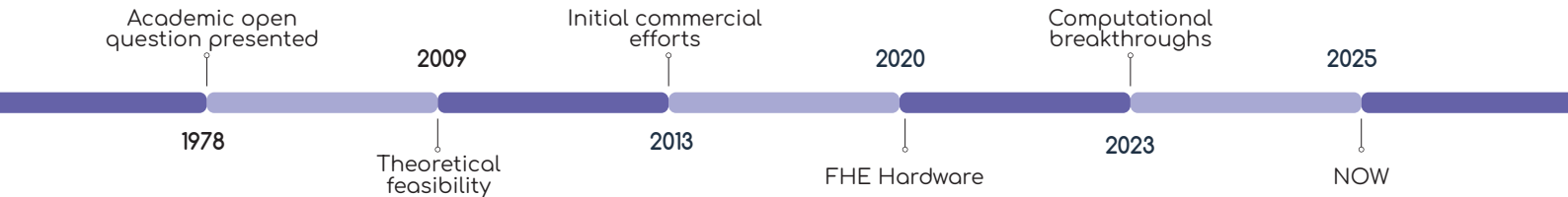
TFHE 45%
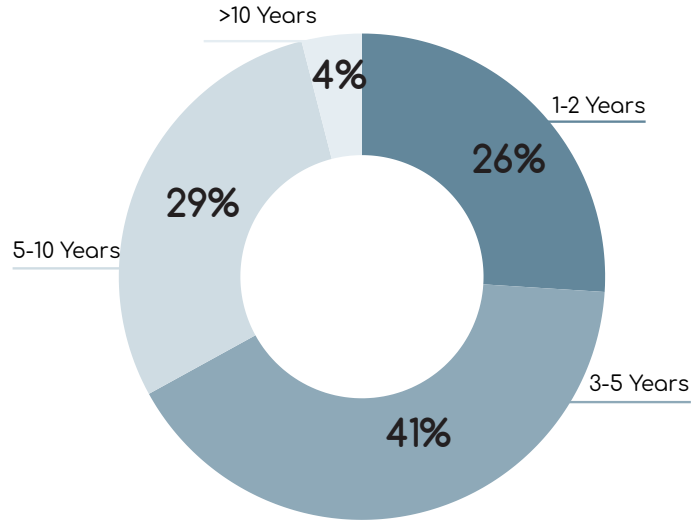
BGV 29%

CGGI 17%

FHEW 14%
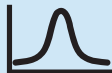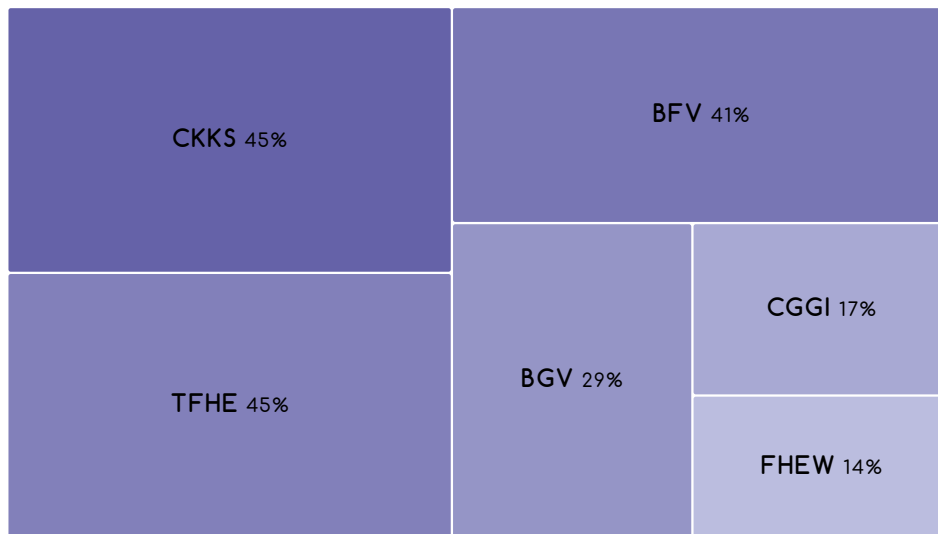
CKKS and TFHE lead as the most widely used FHE schemes due to their complementary strengths. CKKS excels at approximate arithmetic on real numbers for machine learning applications, while TFHE specializes in boolean operations with efficient bootstrapping. This reflects how practitioners select different schemes based on their specific computational requirements.

#6 Which timeline do you predict for FHE adoption in production systems?

Predictions varied: some expect mainstream adoption in 1-2 years, driven by improved tooling and specialized hardware; others believe we're still 5-10 years away due to computational overhead and lack of standardization.


- >10 Years — 4%
- 1-2 Years — 26%
- 3-5 Years — 41%
- 5-10 Years — 29%

Academic open question presented
1978

Theoretical feasibility
2009

Initial commercial efforts
2013

FHE Hardware
2020

Computational breakthroughs
2023

NOW
2025

#7 What will ultimately lead to FHE adoption: game changing computational acceleration, or software promoting algorithmic efficiency?

A combination of hardware and software
71%

Hardware 24%

BFV 41%
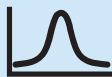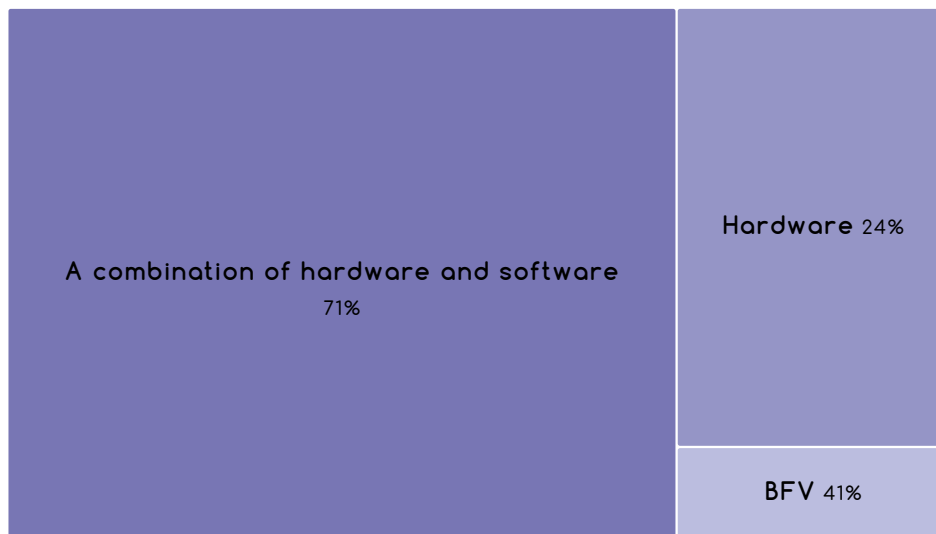
Many respondents agreed that both hardware acceleration and better software optimizations are needed for FHE to scale. We observe a growing number of hardware-software collaborations in the community, where startups and research groups are working together to optimize FHE performance.

#8 Other than computational overhead and complexity, what do you believe is the main challenge in FHE adoption? (Select all that apply)

Implementation Complexity — 57%

Lack of Standardization — 29%

Limited Applicability — 24%
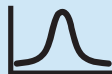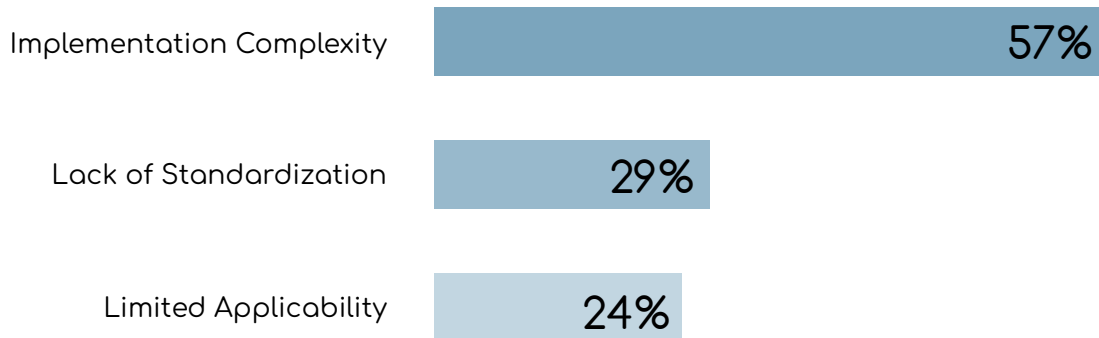
Most respondents are highly familiar with FHE, but even experts highlight the difficulty of implementing FHE efficiently.

#9 Do you see FHE intersecting with other PETs (MPC, ZKP, etc.)?

> **ZKP for verifiability**
> -Cryptography Researcher

> **MPC & ZKP are complementary to FHE**
> -Engineer

> **FHE and ZKP can solve related real-world problems.**
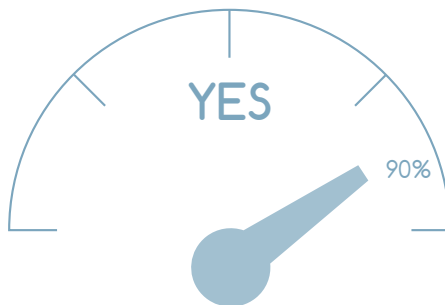> -Cryptography Researcher

> **MPC for key management, ZKPs for (mostly) decentralized applications**
> -Technical Lead

> **Yes MPC, ZKP, Oblivious transfer - ZKP for verifiability, MPC for protection of algorithms, oblivious transfer for protecting server only secrets.**
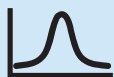> -Engineer

YES

90%

> **Yes. Solutions will be a mix.For example, the cloud sidewill be required to prove itperformed the correctcomputation.**
> -Engineer

> **The recent work by Apple in their "Wally" private search model is a good example of a case where FHE anddifferential privacy are both required.**
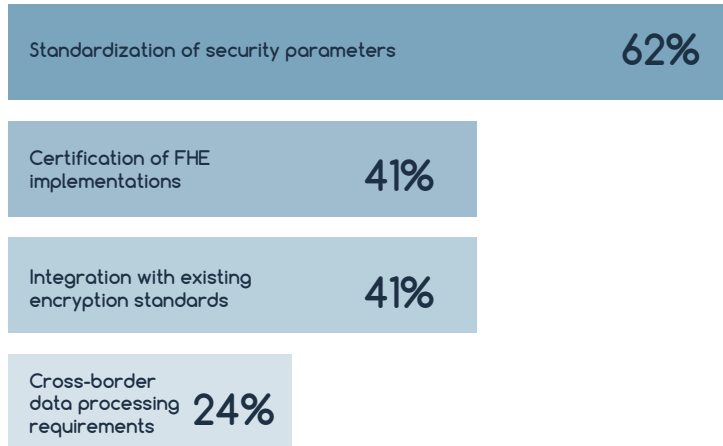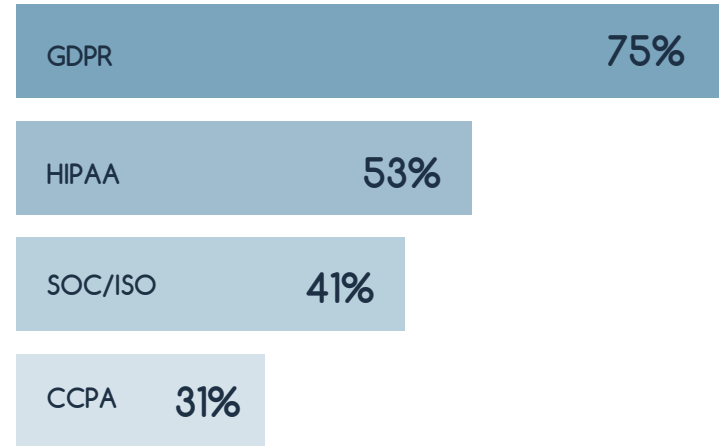> -Engineer

Most respondents see FHE as part of a broader privacy stack, often used alongside MPC, ZKPs, and Secure Enclaves. Some noted that FHE can reduce reliance on vendor-trusted hardware, while others pointed to hybrid models for balancing tradeoffs.

#10 Regulatory frameworks and Standards (Select all that apply)

Which aspects of FHE require new or updated regulatory frameworks?

Standardization of security parameters	62%
Certification of FHE implementations	41%
Integration with existing encryption standards	41%
Cross-border data processing requirements	24%

Which regulations or to FHE implementations? (Select all that apply)

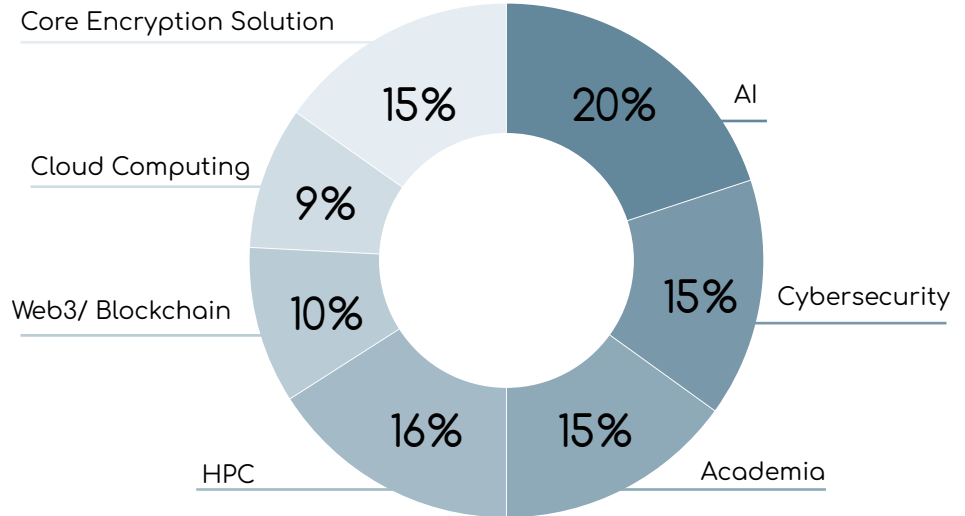|	
GDPR	75%
HIPAA	53%
SOC/ISO	41%
CCPA	31%

Lattica's FHE Survey - 2025

Appendix

FHE doesn't have to be a distant vision. The key to adoption is making it work in specific, high-value applications today, while also building the foundations for broader adoption as the technology and ecosystem evolve.

Survey Participants

Education:

44% PhD

37% Master's degree

Industry:

Core Encryption Solution 15%

Cloud Computing 9%

Web3/ Blockchain 10%

HPC 16%

AI 20%

Cybersecurity 15%

Academia 15%

Lattica was founded on a simple yet radical idea: FHE could be made practical by leveraging the same acceleration techniques that power modern machine learning.

FHE makes it possible to compute on encrypted data, but its real-world adoption has been limited by performance bottlenecks and complex implementations. We realized that by applying the optimization strategies used in modern ML, such as parallel computation, tensor operations and hardware acceleration, we could unlock FHE's potential for AI.

With deep expertise in cryptography, neural networks and AI infrastructure, we built a developer-friendly platform that integrates privacy-preserving AI seamlessly into existing workflows.
To reach out to us with feedback and comments, please email **hello@lattica.ai.**