Protect your data throughout its lifecycle with MongoDB's in-use encryption solutions

Data protection is essential for every organization. With the increasing complexity and volume of data being stored across diverse environments, safeguarding sensitive information—whether it resides in the cloud, on-premises, or elsewhere—has become more critical than ever. In order to implement robust data protection, organizations must ensure data encryption at all stages: in transit, at rest, and in use.

One of the main challenges to adopting in-use encryption stems from its fundamental benefit —data is always encrypted outside the application, making it unreadable to other systems. However, much of the important processing happens outside the application, and that requires access to the data.

At MongoDB, we believe that data protection and usability don't have to be in conflict, and we're making continuous progress toward that goal. We started this journey with the release of Client-Side Field Level Encryption (CSFLE), enabling customers to encrypt sensitive data with strong confidentiality while supporting equality searches through deterministic encryption. Now, with Queryable Encryption, a first-of-its-kind in-use encryption technology, we take a major leap forward. Customers can encrypt sensitive data, including personally identifiable information (PII), protected health information (PHI), and financial information, and still run equality and range queries directly on that encrypted data without using deterministic encryption. Our advanced encrypted search algorithm introduced with Queryable Encryption allows the database to return query results without knowing the query contents or why a document matched. Support for additional query types such as prefix, suffix, and substring will be added in future releases.

Encryption is a crucial tool for protecting sensitive data and maintaining compliance with regulations like GDPR, CCPA, and HIPAA. While typically associated with highly regulated industries, nearly all organizations, regardless of industry, handle sensitive data that requires strong encryption at every stage of its lifecycle. Below are some example use cases of how in-use encryption can enable organizations to maintain usability while adding strong data protection.

- **Equality Search example** *(Queryable Encryption & CS-FLE support)*
  A medical office stores PHI, such as Name and Medical ID, encrypted in their patient records database. With Queryable Encryption, when a doctor needs to retrieve a patient's records they do an exact match search on the encrypted fields 'name' or 'medical_id" and retrieve the patient records, all while ensuring that data is protected from the time it leaves the application until it is received back in the application.

MongoDB.

- **Range Search example** *(Queryable Encryption support)*
  A Human Resources department stores sensitive data that if exposed, could put employees at risk for identity theft among other negative consequences. An HR application can encrypt sensitive data, such as date of birth, while maintaining
  the ability to query records by a range of dates of birth to identify all employees born in a specific year.

- **Prefix Search example** (future capability of Queryable Encryption)
  The Fraud department at a large bank needs to be able to protect sensitive PII and financial data but maintain the ability to search for transactions during an investigation. Using Queryable Encryption, the fraud app can encrypt that sensitive data, such as Name, while still allowing an investigator to search for customer transactions by the first few letters of the customer's name

Key benefits of CSFLE and Queryable Encryption

Key benefits	Queryable Encryption	Client-Side Field Level Encryption
Faster application development cycle Developers don't have to figure out how to use the right algorithms, encryption options, etc to implement their right encryption solution. MongoDB has done all that complex work for them	✓	✓
Strong technical controls for critical data privacy use cases Help customers meet strict data privacy requirements such as HIPAA, GDPR, CCPA, PCI, and more.	✓	✓
End–to–end encryption Data is encrypted at the client-side, remains encrypted in-transit, at rest, and in-use, and is only decrypted back at the client. Fully randomized encryption means that a given value encrypts to a different ciphertext every time.	✓	✓
Reduce operational risk Eliminate common security concerns when moving database workloads to the cloud. Customers can keep their data on any of the cloud providers and be assured that their data is protected	✓	✓
Robust key management Rotate keys and migrate from one key provider to another seamlessly, without impact to your application	✓	✓

Randomized encryption is only available with a non-searchable option.

Key benefits	Queryable Encryption	Client-Side Field Level Encryption
Industry-first, peer-reviewed query technology Queryable Encryption introduces a first-of-its-kind fast encrypted search algorithm using NIST standards-based cryptographic primitives like AES-256, SHA2, and HMACs. This technology has been extensively researched, published, and rigorously peer-reviewed by leading third-party cryptography experts.	✓	
Expressive querying capabilities on encrypted data Data can be searched using equality and range queries with prefix, suffix, and substring query capabilities planned.	✓	
Query non-deterministically encrypted data Queries can be performed directly on non-deterministically encrypted data, a more advanced encryption method that exposes less data.	✓	

Resources

For more information and guidance, consult with your Solution Architect to determine which in-use encryption solution best suits your needs. Here are additional resources to get more information on MongoDB's in-use encryption technologies.

- Client-Side Field Level Encryption documentation
- Queryable Encryption documentation
- MongoDB data encryption webpage
- MongoDB Cryptography Research Group webpage
- Queryable Encryption Technical Paper

Please reach out to your solution architects or send an email to sales@mongodb.com if you have any questions or need to get in touch with sales.

MongoDB.