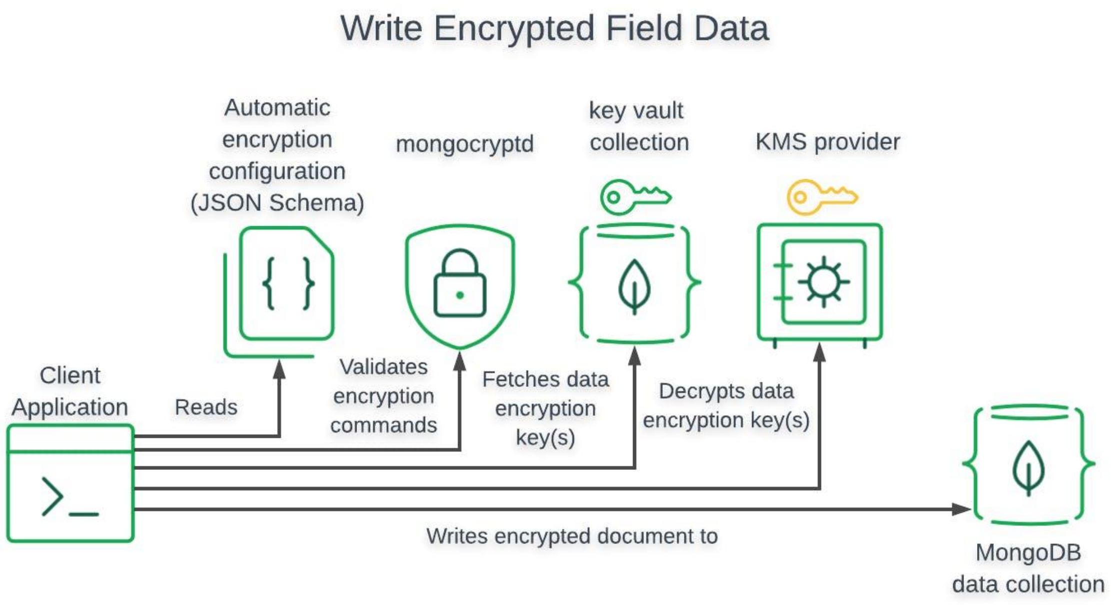
Authenticate features and encryption

Flow chart for mongoDb:


Write Encrypted Field Data
Automatic encryption configuration (JSON Schema)
mongocryptd
key vault collection
KMS provider
Client Application
Reads
Validates encryption commands
Fetches data encryption key(s)
Decrypts data encryption key(s)
Writes encrypted document to
MongoDB data collection

TLS encryption:

By creating a set of certificates for the servers, MongoDB Atlas performs encryption in transit from application client to server and throughout intra-cluster interactions. Once TLS enabled clients pass access and authentication controls, MongoDB Atlas uses Let's Encrypt verified certificates to authenticate them.

Encryption at rest:

MongoDB encryption at rest is an Enterprise feature that requires the MongoDB Atlas Enterprise binaries. Encryption at rest is a security layer that ensures that written data or storage are only visible once decrypted by a trusted process or application. Every node in your MongoDB Atlas cluster comes with built-in encryption at rest for discs. However, the Wired Tiger storage engine can also enable Encryption at Rest.

The WiredTiger storage engine enables the encryption of server data files (collections and indexes) as they are written to disc. This protects your server from a variety of threats. They will not be able to open your data files or backups with another mongod binary to access the data since they do not have the protected certificate key that encrypted the data. At the Operating System level, no other software installed on the server may open the files or intercept the data. Unlike direct disc encryption, which allows the operating system to read the encrypted database. Briefly, only the MongoDB Server has access to an AES-256 master key, which should be kept in a secure location.

Client-side encryption:

A feature called MongoDB Client-Side Field Level Encryption was introduced with MongoDB version 4.2. This new framework enables MongoDB Clients like drivers and shell to encrypt and decode fields locally using secure keys stored in a secure repository (KMS). This adds an additional degree of protection by ensuring that sensitive data is never sent over the wire or to database clients who lack the necessary key to decrypt the data. This capability is available to any Atlas cluster running version 4.2 or higher. Field Level Encryption can be done manually or automatically, and we can store our keys with any one or more of the following providers:

Amazon web service

Azure key vault

Google cloud platform

Rotation of encryption keys:

A regular key rotation is one of the best practices for handling encryption keys. Because there is a potential that our keys will be compromised at some point, this is a significant consideration for database managers. As a result, rotating them will allow us to prevent the possibility of a compromised key. Built-in guidelines to rotate the appropriate keys depending on the exact provider you're using for MongoDB Atlas encryption at rest and Client-Side Field Level encryption.

Authentication in Mongo DB:

The default behavior is without authentication so you will have to connect to the server using the mongo shell, then there you create a user admin, from there you create mongod configuration file to enable authenticate feature. Then connect to server and authenticate as the user admin and then after doing that you can finally create additional users as per need. A link to a tutorial is given below.

How to Enable Authentication on MongoDB | by Stampery Inc. | Mongoaudit — the mongoaudit guides | Medium

Summary:

MongoDB is a general-purpose corporate database with numerous levels of industry-standard encryption to meet your individual data security requirements. MongoDB Atlas makes it much easier to use and deploy those data security capabilities because they're built-in and ready to use in minutes or less. Through the research report we gathered the encryption and authentication for user accounts and data security.

1. TLS encryption
2. Encryption at rest
3. Client-rest encryption
4. Rotation of encryption keys

Each method is discussed in the report to showcase key features, recommendations or limitations for the final decision. The report concludes with the flowchart of all the encryption methods for the field data. Moreover, demonstrates the procedures to enable authentication and encryption of all the user data and company data.