MongoDB Enterprise Edition offers data encryption features, but the free MongoDB Community Server lacks built-in encryption at rest. However, the CIS benchmarks might still offer recommendations for securing data on Ubuntu using alternative approaches. Here's what you can consider:

1. File System Encryption:

- **Encrypt Data Directory:** Consider using full disk encryption tools like dm-crypt or LUKS to encrypt the entire disk where the MongoDB data directory (/var/lib/mongodb by default) resides. This encrypts data at rest, adding an extra layer of security in case of physical server access.

2. Client-Side Encryption (Optional):

- **MongoDB Drivers:** Explore libraries provided by MongoDB drivers for some programming languages that support client-side encryption. This encrypts data before sending it to the server, ensuring it remains encrypted throughout its lifecycle. However, this requires development effort and compatibility considerations.

3. Alternatives for Sensitive Data:

- **Separate Database:** If you have highly sensitive data, consider storing it in a separate database system that offers native encryption capabilities. This might involve additional costs and management overhead.

4. Strong Authentication and Authorization:

- **Focus on Access Controls:** The CIS benchmarks likely emphasize robust authentication and authorization practices. This ensures only authorized users can access the database, even if the data itself isn't encrypted at rest.

5. Regular Backups and Security Practices:

- **Encrypted Backups:** Regularly back up your MongoDB data. Even without data encryption at rest, encrypting backups adds an extra layer of security. Tools like mongodump can be used for backups.
- **Security Updates:** Maintain your system and MongoDB packages updated with the latest security patches to address vulnerabilities.

Additional Resources:

- CIS MongoDB Security Benchmarks (reference security guides that mention them): While not available directly online, you can find references and explanations in security guides that reference CIS benchmarks. Search for "CIS MongoDB Security Benchmarks Ubuntu".
- Ubuntu Documentation on Disk Encryption: https://ubuntu.com/ceph/docs/encryption-at-rest
- MongoDB Documentation on Client-Side Encryption (For Reference): [mongodb.com] (search for "client-side encryption" and your programming language driver)

Remember:

- These are alternative approaches since MongoDB Community Server doesn't offer built-in data encryption.
- Evaluate the trade-offs between security requirements, complexity, and available resources when choosing a method.
- Regularly review security practices and consider migrating to MongoDB Enterprise if data encryption at rest becomes critical.