Here's how to set up file permissions on MongoDB securely on Ubuntu in accordance with the CIS benchmarks:

1. Dedicated User and Group:

- The CIS benchmarks likely recommend using a dedicated user and group for running the MongoDB service. This isolates MongoDB files and directories from other system users and processes.

2. Data Directory Permissions:

- The CIS benchmarks likely recommend setting the following permissions on the MongoDB data directory (/var/lib/mongodb by default):

```
sudo chmod 750 /var/lib/mongodb -R
```

- This restricts access to the data directory and its contents:
  - **Read, Write, Execute (rwx):** Only the owner (MongoDB user) has read, write, and execute permissions.
  - **Read, Execute (rx):** The group (MongoDB group) has read and execute permissions (needed for internal operations).
  - **No Permissions (-):** Others (all other users) have no permissions.

3. Configuration File Permissions:

- The MongoDB configuration file (/etc/mongodb.conf) typically requires read permissions for the MongoDB user and group, while other users should have no access:

```
sudo chmod 640 /etc/mongodb.conf
```

- This allows the MongoDB service to access the configuration file while preventing unauthorized modifications.

4. Additional Considerations:

- The CIS benchmarks might have recommendations for ownership and permissions of other MongoDB-related files (e.g., log files, key files).
- Review the specific CIS benchmarks for your Ubuntu version for detailed recommendations on these additional files.

5. Secure Ownership:

- Ensure the owner of the MongoDB data directory and configuration file is the dedicated MongoDB user, not the root user.

Example Ownership:

```
sudo chown mongodb:mongodb /var/lib/mongodb -R
sudo chown mongodb:mongodb /etc/mongodb.conf
```

6. Verification:

- Use the ls -l command to verify file ownership and permissions after making changes.

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 File Permissions: https://manpages.ubuntu.com/manpages/trusty/man1/chmod.1.html

Remember:

- These are general guidelines. Refer to the official CIS Ubuntu Linux Benchmark for your version for detailed recommendations on file permission settings for MongoDB.
- Regularly review and audit file permissions to ensure they remain aligned with security best practices.