Copilot

To **securely set up file permissions for MongoDB on Ubuntu** in accordance with the **CIS benchmarks**, follow these steps:

1. **Understand the CIS MongoDB Benchmarks**:
   - The **CIS MongoDB Benchmarks** provide secure configuration guidelines for MongoDB systems.
   - You can download the latest **CIS Benchmark for MongoDB** in **PDF format** from the CIS website .
2. **Database File Permissions**:
   - **Appropriate database file permissions** are crucial for security.
   - Follow these steps to ensure secure permissions for MongoDB data files:
     - Set ownership of the database file to the **mongodb user**:

       ```
       sudo chown mongodb:mongodb /var/lib/mongodb
       ```

     - Restrict other permissions:

       ```
       sudo chmod 770 /var/lib/mongodb
       ```

   - These commands ensure that only the **mongodb user** has read and write access to the MongoDB data files, while others have no access .
3. **Automate and Monitor**:
   - Consider using tools like **CIS-CAT Pro** to scan your MongoDB system against the CIS Benchmark. This helps identify conformance to secure configuration recommendations .
4. **Stay Updated**:
   - Regularly check for updates to the CIS Benchmarks and apply them as needed.
   - Leverage **Canonical's automation tooling**, such as the **Ubuntu Security Guide (USG)**, to facilitate the application of these benchmarks .

Remember to **regularly review and adjust** your MongoDB configuration to stay protected against cyber threats. 🛡️ 🚀 .