CS-499 Computer Science Capstone

Yelena Green

# Milestone Four Narrative

# Enhancement Three: Databases

The database encryption enhancement for the CardGrove mobile application is a crucial security improvement that ensures sensitive user data is stored securely. Originally developed during CS-360: Mobile Architecture and Programming, this artifact was enhanced in CS-499: Software Engineering Capstone by implementing SQLCipher encryption to protect user credentials and other sensitive information. The enhancement involved integrating SQLCipher, modifying database interactions to use encryption, and ensuring proper passphrase management.

This artifact was selected for inclusion in my ePortfolio because it demonstrates my ability to integrate secure computing practices into mobile applications. Security is a fundamental aspect of modern software development, and this enhancement showcases my understanding of secure database management, encryption techniques, and Android development. The most significant improvements to the artifact include data encryption, secure passphrase management, and verification of encryption effectiveness using external tools. These modifications enhance the reliability and security of the application while maintaining full functionality.

This enhancement aligns with the course outcomes identified , particularly:

[4] Implementing secure and reliable computing solutions

[5] Fostering a security mindset to protect user data

By applying SQLCipher encryption, I successfully met these outcomes by ensuring data confidentiality and preventing unauthorized access. The enhancement reinforced my understanding of database security and its importance in real-world applications.

The process of enhancing this artifact was an educational and iterative experience. Initially, I encountered challenges with Gradle dependency issues, SQLCipher configuration, and passphrase storage. Debugging these issues required me to delve deeper into Gradle build management, Android security best practices, and SQLCipher integration techniques. Testing the encryption in DBeaver was a crucial step in confirming that the data was properly secured. Additionally, I learned about potential performance trade-offs with database encryption and how to mitigate them using query optimizations.

This enhancement provided valuable insight into the importance of secure software development. It reinforced my ability to adapt existing applications to meet modern security standards while maintaining usability and performance. By overcoming challenges in dependency management, database encryption, and debugging, I gained practical experience that will be applicable to future software security projects.

Overall, this enhancement not only strengthened my technical skills in Android development and secure database management but also deepened my understanding of software security best practices—a critical component in professional software engineering.