**CS 499 Milestone Two: Software Design and Engineering Enhancement Narrative**

**Ifeoluwa Adewoyin**  
CS 499 Computer Science Capstone

**Artifact Description and Background**

The artifact I selected for enhancement is the Mobile Inventory Management Application, which I originally developed during CS 360 (Mobile Architecture and Programming) in the Fall 2023 semester. This Android application was designed to address the critical business need for efficient inventory tracking in small to medium-sized businesses. The application enables users to manage stock items, monitor inventory levels in real-time, and receive automated notifications when items are running low. The original implementation utilized Java and the Android SDK, incorporating SQLite for local data persistence, Material Design 3 components for the user interface, and SMS notification capabilities for low stock alerts.

The original application consisted of approximately 1,200 lines of Java code distributed across eight main classes, including MainActivity for the dashboard interface, LoginActivity for user authentication, AddItemActivity for inventory management, and InventoryDatabaseHelper for database operations. The core functionality provided complete CRUD operations for inventory items, user authentication, real-time stock monitoring with color-coded visual indicators, and automated SMS alerts. While functionally complete, the application contained several critical security vulnerabilities that made it unsuitable for production deployment, particularly in business environments where data security is paramount.

**Justification for Artifact Selection and Enhancement Strategy**

I selected this artifact for my ePortfolio because it represents a comprehensive mobile development project that demonstrates both technical competency and significant potential for cybersecurity enhancement. The original application showcased essential mobile development skills including full-stack Android programming, database integration, user interface design following Material Design principles, and complex business logic implementation. However, the security vulnerabilities present in the original code provided an excellent opportunity to demonstrate advanced cybersecurity skills and transform an academic project into an enterprise-grade secure application.

The enhancement strategy focused on implementing a comprehensive security framework that addresses multiple categories of cybersecurity concerns. This approach allows me to demonstrate expertise across various security domains while maintaining the original application's functionality and user experience. The enhancements align perfectly with my career goals in cybersecurity and provide concrete evidence of my ability to implement enterprise-level security solutions. The transformation from a basic inventory management app to a secure business application showcases the evolution from academic programming to professional software development with a strong security focus.

**Skills and Abilities Demonstrated Through Security Enhancement**

The enhancement process involved implementing a comprehensive cybersecurity framework that demonstrates advanced technical skills across multiple security domains. The centerpiece of the enhancement is the SecurityManager class, comprising over 500 lines of new code that implements enterprise-grade security features. This class demonstrates my ability to design and implement complex security architectures using industry-standard practices and frameworks. The SecurityManager incorporates advanced password hashing using SHA-256 with salt and 10,000 iterations, meeting current OWASP guidelines for password security. Additionally, it implements AES-256 encryption for sensitive data protection, providing field-level encryption capabilities that ensure data confidentiality both at rest and in transit.

The authentication system enhancement showcases my understanding of modern security principles and threat mitigation strategies. I replaced the original insecure plain text password storage with a sophisticated hashing system that includes salt generation and multiple iteration rounds to prevent rainbow table and brute force attacks. The enhanced login system implements progressive account lockout mechanisms, tracking failed login attempts and automatically locking accounts after three failed attempts for a five-minute duration. This demonstrates my ability to balance security requirements with user experience considerations, as the lockout period is sufficient to deter automated attacks while minimizing inconvenience to legitimate users.

A screenshot of a computer program

AI-generated content may be incorrect.

The threat detection and monitoring capabilities represent another significant area of technical advancement. I implemented a comprehensive security event logging system that creates detailed audit trails for all security-relevant activities within the application. This system tracks login attempts, data access patterns, configuration changes, and potential security violations. The logging framework follows enterprise security practices by providing sufficient detail for forensic analysis while protecting sensitive information from unauthorized disclosure. The implementation includes real-time threat detection capabilities that can identify suspicious behavior patterns and trigger appropriate security responses.

**A screenshot of a phone

AI-generated content may be incorrect.**Data protection enhancements demonstrate my understanding of modern data security requirements and encryption best practices. The enhanced application implements field-level encryption for sensitive inventory data, ensuring that critical business information remains protected even if the underlying database is compromised. The encryption system includes secure key management with automatic key generation and rotation capabilities, following industry best practices for cryptographic key lifecycle management. Input validation and sanitization mechanisms protect against injection attacks and other input-based vulnerabilities, demonstrating my awareness of common attack vectors and appropriate countermeasures.

**Course Outcomes Achievement and Professional Development**

The security enhancements directly address multiple course outcomes while demonstrating substantial progress toward professional competency in cybersecurity. Course Outcome 1, focusing on collaborative environments for organizational decision-making, is achieved through the comprehensive audit logging and security monitoring capabilities that enable security teams to make informed decisions about threat response and risk management. The enhanced application provides clear security insights through detailed logging and reporting features that support collaborative incident response and security assessment activities.

Course Outcome 2, emphasizing professional communication capabilities, is demonstrated through the extensive documentation, clear technical explanations, and visual security demonstrations built into the application. The SecurityTestActivity provides a comprehensive interface for demonstrating security features to both technical and non-technical audiences, making complex cybersecurity concepts accessible and understandable. The security status reporting and audit log interfaces enable effective communication of security posture to diverse stakeholders, from system administrators to executive management.

A screenshot of a cell phone

AI-generated content may be incorrect.

A screenshot of a phone

AI-generated content may be incorrect.

A screenshot of a phone

AI-generated content may be incorrect.

Course Outcome 4, focusing on innovative techniques and tools, is substantially achieved through the implementation of cutting-edge cybersecurity practices including zero-trust architecture principles, behavioral threat detection, and comprehensive security automation. The enhanced application demonstrates innovative approaches to mobile application security that deliver significant value by transforming a basic academic project into a production-ready secure business application. The security framework incorporates modern cybersecurity techniques that reflect current industry best practices and emerging security trends.

Course Outcome 5, developing a security mindset, is comprehensively demonstrated throughout the enhancement process. Every aspect of the application now incorporates security considerations, from initial user input validation to data storage encryption to comprehensive audit logging. The enhancement demonstrates a proactive security approach that anticipates potential threats and implements multiple layers of defense. This security-first thinking represents a fundamental shift in my development approach and reflects the mindset required for effective cybersecurity practice.

**Enhancement Process Challenges and Learning Experiences**

The enhancement process presented several significant technical challenges that provided valuable learning opportunities and demonstrated problem-solving capabilities. The most complex challenge involved implementing secure password migration from the original plain text storage to the new hashed password system without disrupting existing user accounts or compromising data integrity. This required developing a sophisticated migration system that could detect legacy passwords, securely update them using the new hashing algorithm, and maintain backward compatibility during the transition period. The solution involved creating database migration logic that automatically identifies plain text passwords based on their format and systematically converts them to secure hashes while preserving user access.

Another significant challenge was balancing comprehensive security implementation with maintaining user experience and application performance. Enterprise-grade security features such as encryption, input validation, and threat monitoring can potentially impact application responsiveness and user workflow. I addressed this challenge by implementing efficient algorithms, optimizing security operations for mobile devices, and designing security features that operate transparently to end users. The threat detection system, for example, performs behavioral analysis in the background without affecting normal application functionality, while the encryption system uses optimized algorithms that minimize performance impact.

The development of comprehensive error handling and security logging presented unique challenges in creating systems that provide appropriate feedback without revealing sensitive information to potential attackers. Security-aware error handling requires careful consideration of what information to present to users versus what to log for administrative review. I developed a sophisticated exception management system that provides meaningful feedback to legitimate users while logging detailed security information for analysis and incident response. This experience enhanced my understanding of how security considerations must be integrated into every aspect of application architecture, not just obvious security features like authentication and encryption.

The implementation process also provided valuable insights into the complexity of real-world cybersecurity deployment. Working with industry-standard security frameworks such as OWASP and NIST guidelines taught me the importance of following established security practices rather than developing custom security solutions. This experience highlighted the critical nature of security testing and validation, leading to the development of the comprehensive SecurityTestActivity that enables thorough testing of all security features. The testing framework demonstrates my commitment to security verification and provides a professional tool for ongoing security assessment.

**Professional Impact and Career Relevance**

The enhancement process has fundamentally transformed my approach to software development and significantly advanced my preparation for a cybersecurity career. The project demonstrates practical experience with enterprise security frameworks and validates my ability to implement comprehensive security solutions in real-world applications. The skills developed through this enhancement directly align with industry requirements for cybersecurity professionals, including security architecture design, threat detection and response, secure coding practices, and security testing methodologies.

The enhanced application serves as compelling evidence of my evolution from computer science student to cybersecurity professional, showcasing advanced technical capabilities that are immediately applicable in professional environments. The comprehensive security implementations meet industry standards and demonstrate the level of expertise required for entry-level cybersecurity positions. The project also provides an excellent foundation for my planned graduate studies in Information Security, demonstrating both theoretical understanding and practical implementation skills.

The transformation from academic project to enterprise-grade application illustrates my ability to bridge the gap between theoretical knowledge and practical implementation. This capability is essential for cybersecurity professionals who must translate security concepts into effective technical solutions that protect organizational assets while supporting business objectives. The project demonstrates my readiness to contribute meaningfully to organizational cybersecurity initiatives and provides a strong foundation for continued professional development in information security.

**Conclusion and Future Applications**

The enhancement of the Mobile Inventory Management Application represents a significant milestone in demonstrating advanced cybersecurity skills and professional software development capabilities. The comprehensive security implementations, including advanced authentication mechanisms, data encryption systems, threat detection capabilities, and security monitoring infrastructure, showcase technical proficiency with industry-standard security frameworks and practical experience solving complex cybersecurity challenges. The project successfully transforms an academic inventory management application into an enterprise-grade secure business application that could be deployed in production environments.

The enhancement process has provided invaluable learning experiences that extend far beyond the technical implementation details. The project has fundamentally shaped my understanding of secure software development lifecycles, taught me to think systematically about security threats and countermeasures, and developed my ability to balance security requirements with usability considerations. These skills and perspectives will be directly applicable throughout my cybersecurity career and provide a strong foundation for tackling increasingly complex security challenges in enterprise environments.

The enhanced application serves as compelling evidence of my readiness for advanced cybersecurity roles and graduate studies in Information Security. The practical experience gained through implementing enterprise-grade security solutions, combined with the comprehensive documentation and testing frameworks developed as part of the project, demonstrates both technical competency and professional maturity. This artifact will serve as a cornerstone of my professional portfolio, illustrating my capability to deliver secure, production-ready software solutions that meet modern cybersecurity standards and business requirements.