Devin Bashaw

CS 305

02/02/2025

After reviewing Artemis Financials requests and the module resources, ensuring the companies archive files are properly encrypted and stored is the main focus here. Encryption is a good way to secure sensitive information from outside sources or privy hands, and after reviewing the resources I can safely recommend AES-256 to be a good candidate algorithm for encrypting Artemis Financials files. However, other protocols will need to be put into place to ensure the company is immune to future threats. Some of these threats can happen through someone gaining access to credentials, man in the middle attacks, fault data transfers that leak information, or someone on the inside.

Some security protection best practices to withstand these threat actors include securing the storage and transfer of encryption keys, more processing power to full run the AES-256, and quauntum-resistent encryption. Artemis Financial must also follow strict government regulations, including: GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and PCI-DSS (Payment Card Industry Data Security Standard). AES-256 complies with all of these regulations, meeting the requirements for data encryption, storage security, financial and health record encryption, and securing transactions. If AES-256 is also paired with FIPS 140-2 (Federal Information Processing Standard), then the overall security and encryptions will be even stronger for the company.

Other reasons to use AES-256 is its scalability across industries, hashing functionality that pairs well with its encryption, and a 256-bit key which allows for more security against attacks, random number generation using PRSNGs. The only thing I would additionally recommend is an asymmetric encryption to protect AES keys during transmissions, since AES-256 is a symmetric-key cipher that uses the same key for both encryption and decryption, which is not always the most secure.

What is the history of AES? Well, AES was established in 2001 by NIST and ever since has become the encryption standard worldwide, primarily for its scalability. However, if you want to go against the status-quo, some additional algorithms include: ChaCha20 for its security on constrained hardware, Quantum-Resistant algorithms which are currently being developed and may turn out greater than all the others, and RSA encryption for its impactful key exchange. Overall, AES-256 is the best algorithm Artemis Financial can use. Its scalable, adaptable, and the most secure thing on the market right now. Nothing else has topped it yet.

Works Cited:

* Manico, J., & Detlefsen, A. (2014). *Iron-Clad Java: Building secure web applications* (Chapter 6). McGraw-Hill Education
* Manico, J., & Detlefsen, A. (2014). *Iron-Clad Java: Building secure web applications* (Chapter 8). McGraw-Hill Education
* Oracle. *Java Security standard cipher algorithm names*. Oracle Corporation.