Protecting User Password Keys at Rest

Safeguarding user password keys is crucial for maintaining the privacy and security of sensitive information. This presentation will outline a robust solution using leading-edge cryptographic techniques to ensure the protection of user password keys at rest, providing a secure foundation for user authentication and data access.

Problem Statement

Protecting user password keys at Rest.

1 **Password Key Exposure**

User password keys stored on disk are vulnerable to unauthorized access, theft, or compromise, putting sensitive user data at risk.

2 **Compliance and Regulatory Concerns**

Failure to properly secure password keys can lead to compliance issues and potential legal or financial penalties.

3 **User Trust and Reputation**

A breach of password key security can severely damage user trust and the organization's reputation, negatively impacting the business.

Unique Idea Brief (Solution)

Secure Password Key Storage

Leverage AES-256 encryption and PBKDF2 key derivation to ensure that user password keys are securely stored on disk, protected from unauthorized access.

Robust Key Management

Implement a comprehensive key management system to generate, rotate, and revoke password keys as needed, maintaining tight control over the security lifecycle.

Compliance and Regulatory Alignment

Ensure that the solution aligns with industry best practices and relevant compliance standards, such as NIST, HIPAA, and PCI-DSS, to mitigate legal and financial risks.

Features Offered

1 **Encrypted Password Key Storage**

User password keys are encrypted using AES-256 encryption and protected using PBKDF2 key derivation, ensuring their safety at rest.

2 **Secure Key Management**

Comprehensive key management capabilities, including key generation, rotation, and revocation, to maintain tight control over the security lifecycle.

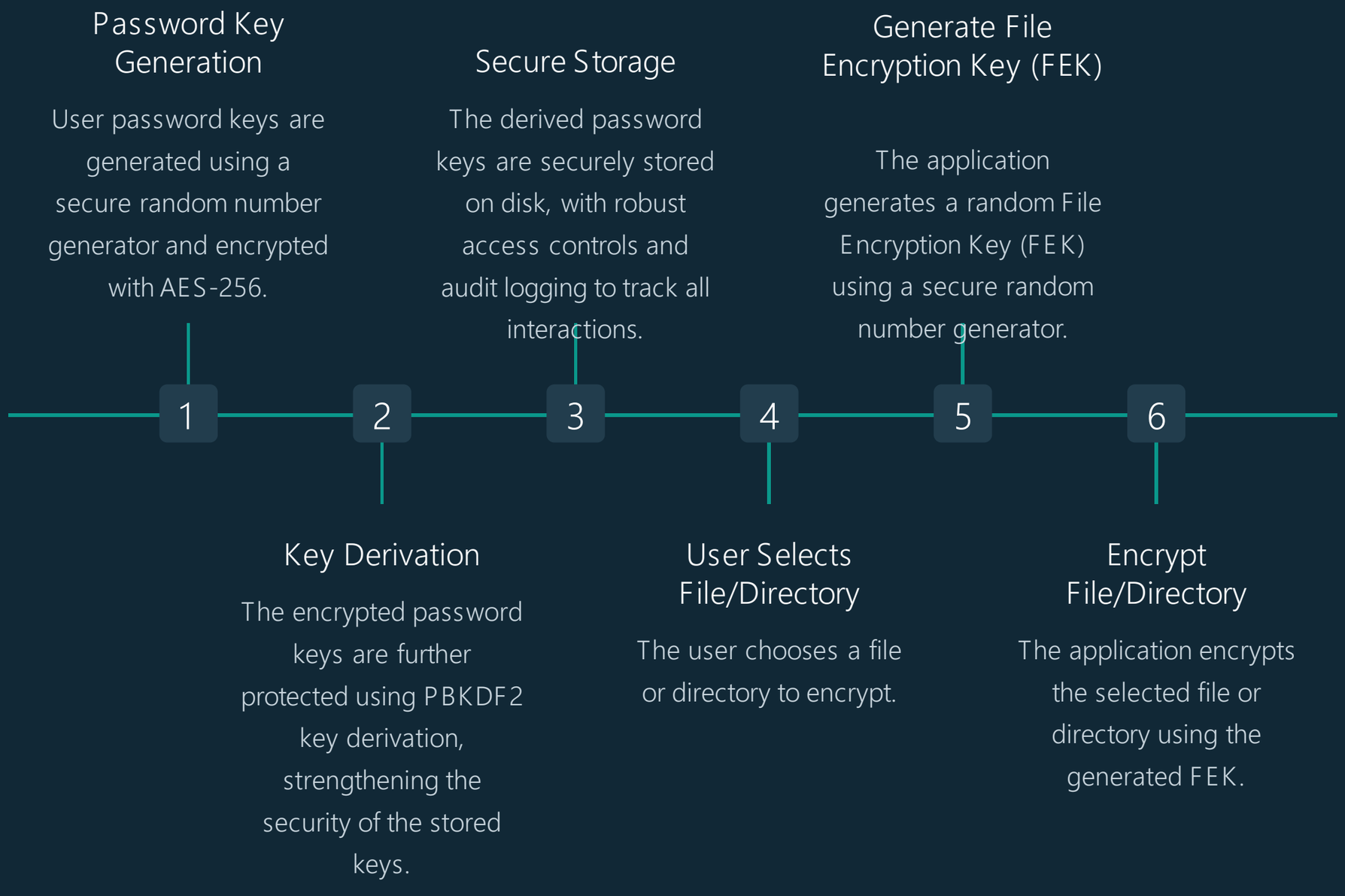
3 **Scalability and Flexibility**

The architecture is scalable and can accommodate growing user and data volumes, while offering flexibility to adapt to evolving security requirements.

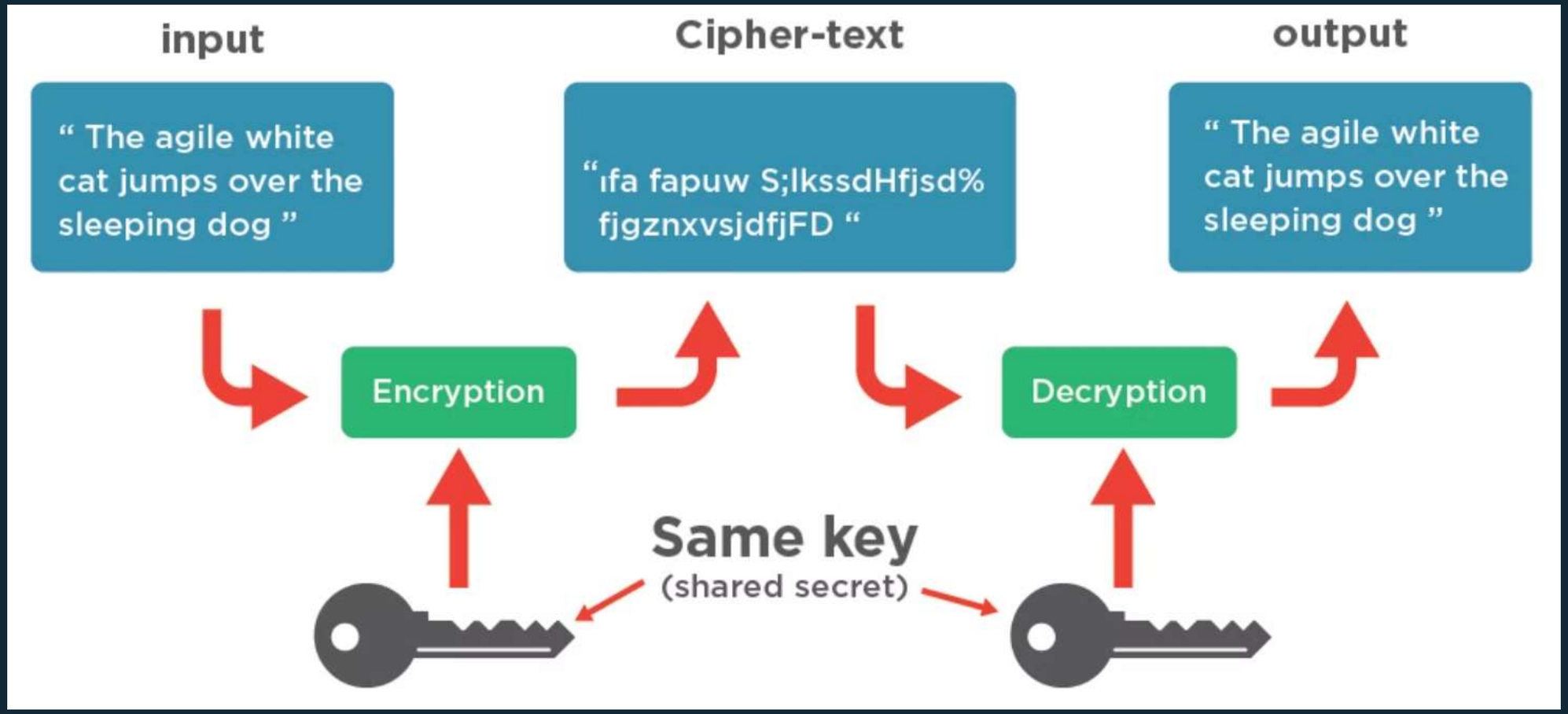
4 **Used for Several Test Cases**

The solution has been extensively tested and is capable of handling different Test Cases.

Process Flow



Architectural Diagram



Technologies Used

Python

The core of the solution is built using the Python programming language, leveraging its robust cryptographic capabilities.

PyCryptodome

The PyCryptodome library is used to implement the AES-256 encryption and PBKDF2 key derivation algorithms.

Key Management Service

A dedicated key management service is integrated to securely store and manage the user password keys.

Access Control

Robust access control mechanisms are implemented to ensure only authorized parties can interact with the password key storage system.

Team Members and Contribution

Aarchi Tiwari

Member 1- Responsible for the overall architecture and implementation of the password key encryption, decryption including AES-256 implementation and key management with PBKDF2 and GUI.

Anjali Chaudhari

Member 2 - Handled file and directory management, ensuring secure file handling and input validation. Additionally, documented the problem statement, outlining the project's requirements, goals, and scope.

Siddhi Chindhalore

Quality Assurance - Thoroughly tested the solution to validate its security, performance, and compliance with regulatory requirements.

Conclusion

1

Secure Password Key Storage

The solution ensures that user password keys are securely stored on disk, protected by advanced encryption and key derivation techniques.

2

Comprehensive Key Management

The robust key management system enables the secure generation, rotation, and revocation of password keys, maintaining tight control over the security lifecycle.

3

Compliance and Regulatory Alignment

The solution aligns with industry best practices and relevant compliance standards, mitigating legal and financial risks while instilling user trust.

By implementing this comprehensive solution, organizations can effectively protect user password keys at rest, safeguarding sensitive data and ensuring compliance with security regulations. This innovative approach to password key management reinforces the organization's commitment to data privacy and security, building a foundation of trust with its users.