Secure Data Analysis in the Public Cloud Using AES and FHE

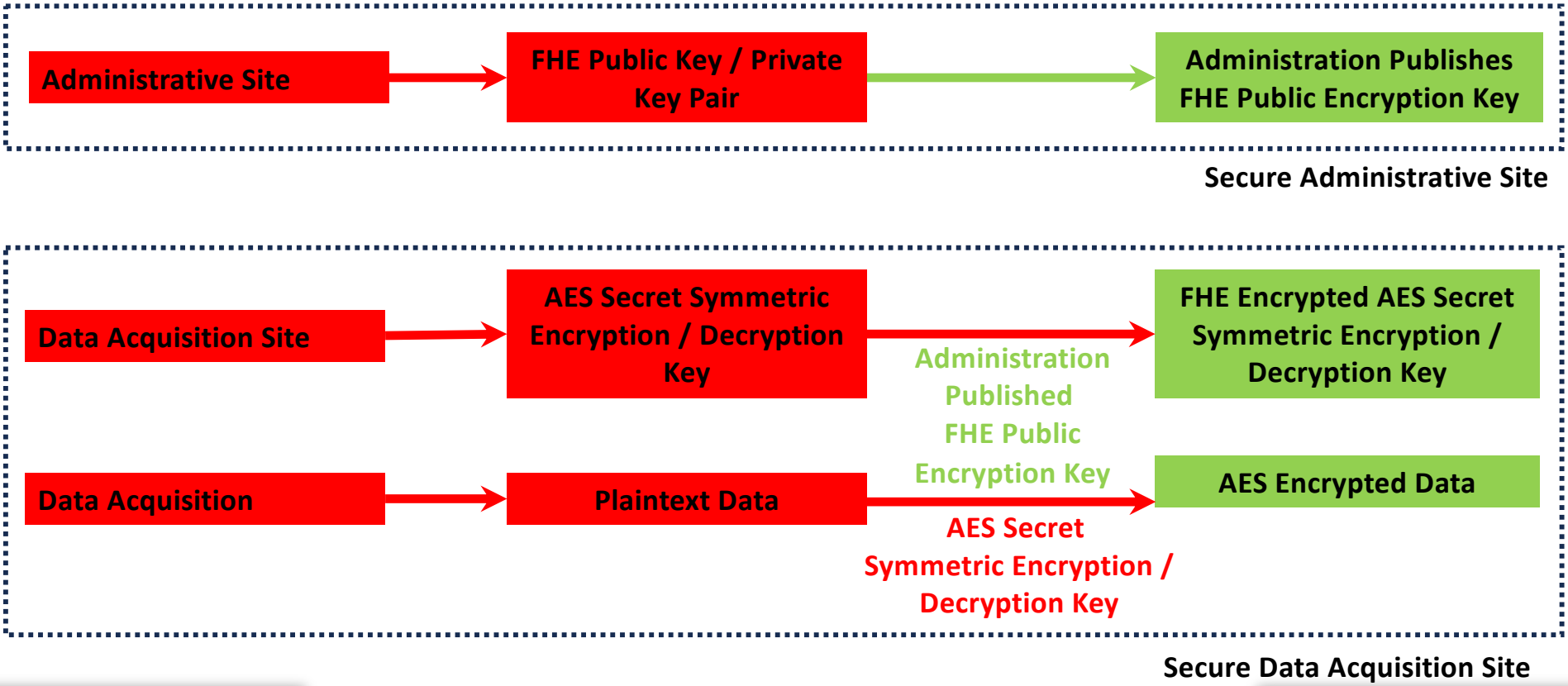
This use case uses AES and FHE encryption to acquire highly confidential data at a secure acquisition site, perform analytics on that data on an untrusted, insecure, public cloud platform, and transmit the highly confidential results of that analysis to a secure administrative site without ever exposing plaintext data, plaintext results, or any secret decryption keys.

- An FHE public encryption key / private decryption key pair is generated at the secure administrative site. The FHE public encryption key is made publicly available and accessible to the secure data acquisition site.
- A symmetric AES encryption / decryption key is generated at the secure data acquisition site.
- Highly confidential data is acquired at the secure data acquisition site and is AES encrypted using the symmetric AES encryption / decryption key.
- The FHE public encryption key is used to encrypt the symmetric AES encryption / decryption key.
- The secure data acquisition site insecurely transmits both the AES encrypted data along with the FHE encrypted AES symmetric encryption / decryption key to an untrusted, insecure, public cloud analytics platform.
- The AES encrypted data is transformed to FHE encrypted data via secure transcipher without exposing either the plaintext data or decryption keys. The FHE encrypted data is now decryptable using the FHE private decryption key.
  - See next slide.
- With the data in FHE encrypted form, analytics are performed producing an FHE encrypted result.
- The FHE encrypted result is insecurely transmitted to the secure administrative site for decryption by the FHE private decryption key.

Secure Encrypted Data Transcipher from AES to FHE

- The core of this data processing use case is the secure transcipher of AES encrypted data to FHE encrypted data without exposing any plaintext data, analytical results or secret keys. This solution centers on the homomorphic decryption of AES encrypted data. The homomorphic decryption function has two arguments:
  1. A non-homomorphically encrypted argument – The AES encrypted data
  2. A homomorphically encrypted argument – The FHE encrypted, AES Secret Symmetric Encryption / Decryption Key
- A homomorphic function that has at least one homomorphically encrypted argument will produce a homomorphically encrypted result that is encrypted in the same way as the homomorphically encrypted argument(s).
- Performing a homomorphic decryption of AES encrypted data with an FHE encrypted AES symmetric encryption / decryption key produces FHE encrypted data encrypted in the same way as the FHE encrypted AES symmetric encryption / decryption key.
- *This AES to FHE transcipher is achieved without ever exposing plaintext data, analytical results, or any secret keys.*

Stage 1 – Secure Administrative and Data Acquisition Sites



Stage 2 – Untrusted, Insecure Public Cloud Analytic Platform and Secure Administrative Site