Crypto – Project 2

Team Members:

Aditya Varma k (avk287)

Praveen Mareedu (pm2374)

Vibha Ghatke(vg897)

Abstract:

- As the enterprise marches inexorably towards a cloud-dominated future, organizations must find ways to enable the competitive advantage of cloud computing without sacrificing the data privacy and security that legal regulations and industry best practices demand. Cloud computing creates a number of new security vulnerabilities and attack vectors, leading some to consider data breaches "inevitable." Fortunately for the enterprise, the security issues created by the cloud are solvable using a technology with which most organizations are already familiar and comfortable: encryption.

- Encryption eliminates the threat of exposure in the event of a breach
- Encryption can be applied as needed, where needed
- Encryption no longer means a loss of functionality

Highlights – Security Analysis

- Secure Server storage: Drop-Box
- Security/Privacy: AES block encryption with OFB mode of operation
  - Secures from - **Data eavesdropping attacks**:
    - secretly listen to a conversation. For the Drop-Box file transfers -upload and downloads we are performing encryption and decryption (using AES)
- Authentication: SHA-2 cryptographic hash function(MD5)
  - Secures from **- Data Modification attacks**
- Two-Factor Authentication:
  - Secures from **– Data Replay attacks**
    - Making use of Drop Box API two factor authentication login as well as security code(one time password) to use drop-box.

Encryption and Decryption :

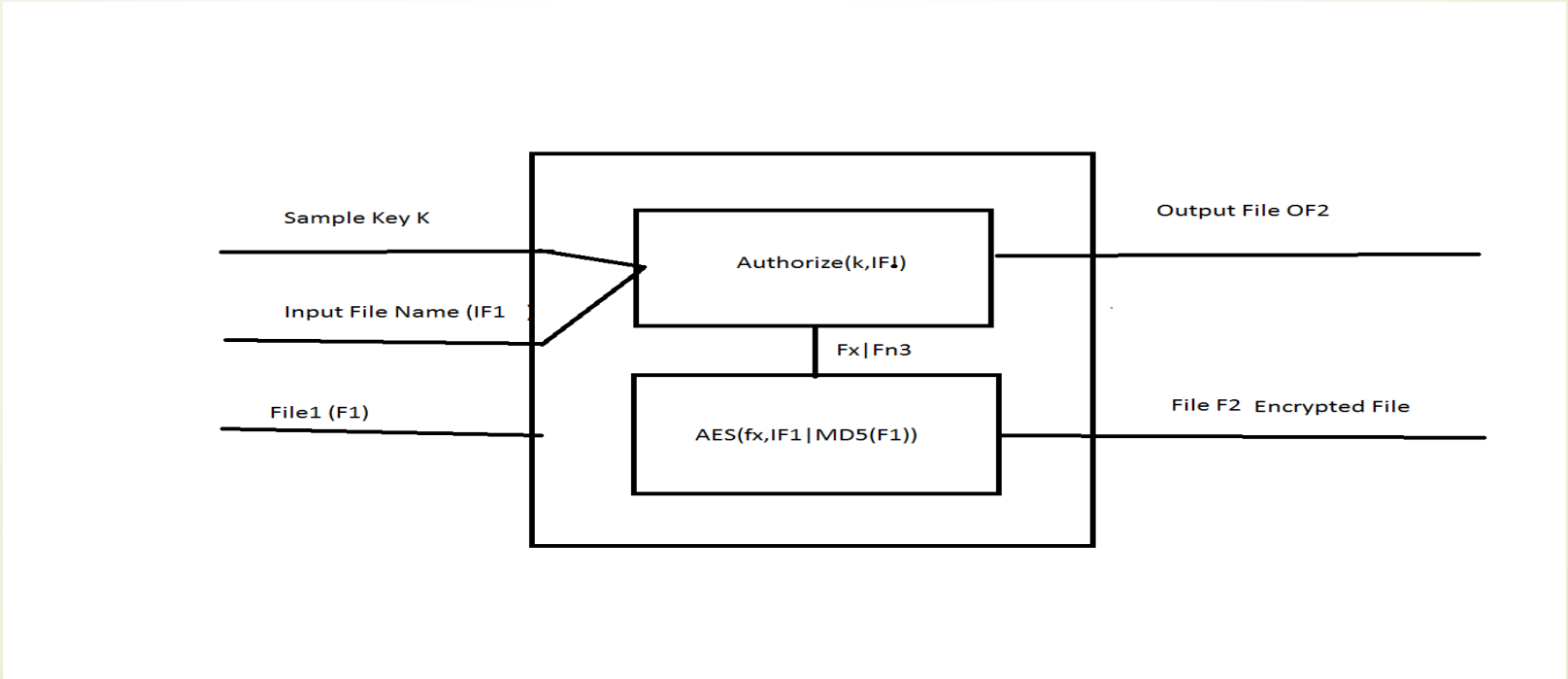
- **AES:**
- The algorithm is based on several substitutions, permutations and linear transformations, each executed on data blocks of 16 byte – therefore the term block cipher. Those operations are repeated several times, called "rounds". During each round, a unique round key is calculated out of the encryption key, and incorporated in the calculations. Based on this block structure of AES, the change of a single bit either in the key, or in the plaintext block results in a completely different cipher text block – a clear advantage over traditional stream ciphers. The difference between AES-128, AES-192 and AES-256 finally is the length of the key: 128, 192 or 256 bit – all drastic improvements compared to the 56 bit key of DES. By way of illustration: Cracking a 128 bit AES key with a state-of-the-art supercomputer would take longer than the presumed age of the universe.

MD5: (Data Integrity is checked here):

- The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.
- MD5 digests have been widely used in the software world to provide some assurance that a transferred file has arrived intact. For example, file servers often provide a pre-computed MD5 (known as Md5sum) checksum for the files, so that a user can compare the checksum of the downloaded file to it. Most unix-based operating systems include MD5 sum utilities in their distribution packages; Windows users may install a Microsoft utility, or use third-party applications. Android ROMs also utilize this type of checksum.

Implementation schematics:

- Encryption:



Continued..

- The filename F2 generated, is the hash value of IF1.
- The key fx is generated by a combination of x (unique to each user) and IF1 and is thus unique for each file. In AES()
- The file F1 is first appended by its hash value and then encrypted to get f2.
- In authorize it generates key fx, also used by AES. Generates fn3 (equal to fn3), which is used to uniquely locate the file on the server.

Decryption

- AESDecrypt produces file f3, the decrypted file and its integrity is checked by comparing the hash value of f3 and hash. If the values match, the file is authentic.