Encryption Technologies

AES-256

Backup Everything uses industry standard encryption technology for securing the data. Symmetric encryption in the form of AES-256 is used for all encryption/decryption purposes required to secure the data at rest. The symmetric key required for the actual encryption/decryption is secured using AWS KMS involving both hardware and software security.

What is AES-256?

The Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.[4] It is a subset of the Rijndael block cipher[3] developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal[5] to NIST during the AES selection process.[6]

Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES),[7] which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

What is CBC mode in AES-256 ?

CBC (short for cipher-block chaining) is a AES block cipher mode that trumps the ECB (Electronic Codebook) mode in hiding away patterns in the plaintext. CBC mode achieves this by XOR-ing the first plaintext block (B1) with an initialization vector before encrypting it. CBC also involves block chaining as every subsequent plaintext block is XOR-ed with the ciphertext of the previous block.

Advantages of CBC mode

The greatest advantage CBC has over ECB is that, with CBC mode, identical blocks do not have the same cipher. This is because the initialization vector adds a random factor to each block; hence, why the same blocks in different positions will have different ciphers.

Although CBC mode is more secure, its encryption is not tolerant of block losses. This is because blocks depend on their previous blocks for encryption. So, if block Bi is lost, the

encryption of all subsequent blocks will not be possible. This chained behavior also means that the encryption of blocks needs to be done sequentially, not in parallel.

RSA

Backup Everything uses RSA in the form of HTTPS protocol in order to secure the data at rest. The certificates are both issued and managed via Amazon Certificate Manager.

What is RSA?

RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission. The acronym RSA is the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who publicly described the algorithm in 1977. In such a cryptosystem, the encryption key is public and distinct from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". Clifford Cocks, an English mathematician working for the British intelligence agency Government Communications Headquarters (GCHQ), had developed an equivalent system in 1973, which was not declassified until 1997.[1]

RSA is generally the strongest encryption protocol that is currently available and Backup Everything uses it extensively for securing the communication that takes place for

- Web Portal Rendering (HTTPS)
- All APIs consumed by Web Portal are HTTPS secured
- All APIs consumed by Desktop Clients are HTTPS secured
- All APIs consumed by Mobile Application are HTTPS secured

SHA-256

Backup Everything uses industrial standard hashing technology i.e. SHA-256 to ensure data integrity which is of prime importance to prevent man-in-middle attacks, Phishing attacks etc.

What is SHA-256?

SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) and first published in 2001.[3][4] They are built using the Merkle–Damgård structure, from a one-way compression function itself built using the Davies–Meyer structure from a (classified) specialized block cipher.

SHA-2 includes significant changes from its predecessor, SHA-1. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: **SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. SHA-256 and SHA-512** are novel hash functions computed with 32-bit and 64-bit words, respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds. SHA-224 and SHA-384 are truncated versions of SHA-256 and SHA-512 respectively, computed with different initial values. SHA-512/224 and SHA-512/256 are also truncated versions of SHA-512, but the initial values are generated using the method described in Federal Information Processing Standards (FIPS) PUB 180-4.

The SHA-256 hashing is used for the following purposes in the solution

- To compute file hash
- To determine incremental changes in a backupset
- AWS determined pre-signed URLs for downloading and uploading files

UUID

The java.util.UUID class represents an immutable universally unique identifier (UUID). Following are the important points about UUID – A UUID represents a 128-bit value. It is used for creating random file names, session id in web application, transaction id etc.

UUID is used for the following purposes:

- Generating unique id for files in the solution
- Generating unique id for backup sets in the solution
- Generating version id for multiple generations
- Generating unique id for Hot VM Instances
- Generating unique id for Image VM Instances
- Generating unique id for StandAlone VM Instances
- Generating unique id for Devices registered as part of a user account

REFERENCES

- https://docs.oracle.com/javase/7/docs/api/java/util/UUID.html
- https://en.wikipedia.org/wiki/SHA-2
- https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
- https://www.solarwindsmsp.com/blog/aes-256-encryption-algorithm
- https://en.wikipedia.org/wiki/RSA_(cryptosystem)
- https://www.educative.io/edpresso/what-is-cbc