CloudBerry Lab
#1 Cross Platform Cloud Backup

November 2018

CloudBerry Lab Security Design & Implementation

Introduction

This document reviews data encryption and secure file transmission with CloudBerry products. It includes information about encryption algorithms and encryption key generation procedures.

Overview

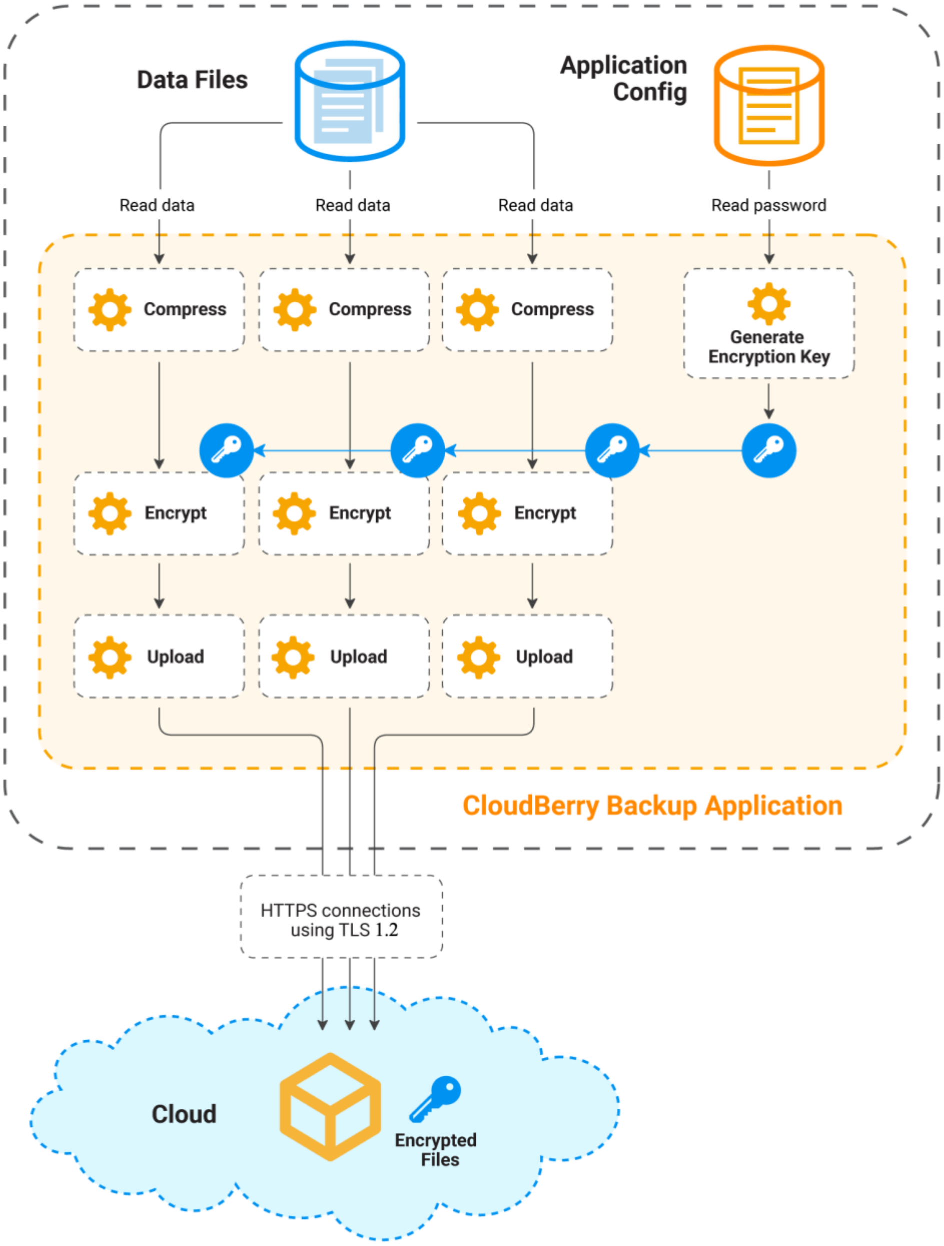
CloudBerry Lab provides robust encryption functionality. This allows our customers to transfer and store their data in a secure way in cloud storage. CloudBerry uses a US Government FIPS 140-2 compliant encryption algorithm for stored data. Data transfers over the internet can also be secured with encryption.

Implementation

This use case covers the details of user data stored on a local network / computer and backed up with encryption to cloud storage.

1. Users register cloud storage accounts in CloudBerry. Account credentials are stored in encrypted fashion using the Advanced Encryption Standard (AES) algorithm. The Use SSL option ensures secure communication.
2. Backup plans contain the chosen encryption algorithm (AES 128/192/256), the encryption key, and whether file names should be encrypted (option with some cloud storage providers). This information is stored securely using AES.
3. When a backup runs, file data is encrypted on the source computer before the data leaves for cloud storage.
4. Data is moved securely to the cloud using HTTPS.

CloudBerry Lab Security Design & Implementation



Data Encryption Procedure

When the user enters an encryption password into CloudBerry, this password is stored in the settings file using AES encryption.

When uploading, CloudBerry reads the encryption password from the settings file and generates an encryption key. To generate the encryption key, we use the PBKDF2 key derivation function (RFC 2898). The encryption key is salted and run through many iterations to further slow-down brute force attacks.

The encryption algorithm runs in Cipher Block Chaining (CBC) mode to further protect the encrypted files. Furthermore, we use PKCS #7 (Cryptographic Message Syntax) padding.

A cryptographic Random Number Generator (RNG) is used to generate the initialization vector (IV).

Encryption is performed in real-time during backups.

Master Password

CloudBerry also supports an additional option to protect the agent from unauthorized access. You can set a Master Password which requires the correct password be entered in order to use the agent. This password is stored encrypted using AES.