Encrypting Data at Rest, data downloaded to and stored on a mobile device, is vital to security. Just like an application developer makes mobile app security testing a part of software development, data encryption needs to be practiced from the user-end with the same level of priority. Like data in use and transit, security experts and regulators recommend encrypting data at rest, but most organizations either don’t do it or get it wrong. In other words, though recommended and equally important, it is just not happening on mobile devices. Here we will take a look at Data at Rest on mobile devices and what issues need to be addressed.

Most modern mobile phones have built-in hardware encryption feature available. With hardware encryption, you can encrypt complete user data and OS while in flash memory. It is then decrypted in main memory when in use. According to Wall Street Journal, 95 percent of iPhones worldwide are encrypted, while only 10 percent of 1.4 billion Android devices are encrypted. Majority of people stick to the default settings of their devices, and this is why very few android phones use encryption even though majority of the devices come with encryption support.

In other cases, encryption may not come as a feature of the device or operating system. Third-party software is then required for encrypting. Whatever the case, enabling encryption is the prime task. Platforms that include encryption should have their encryption handled by the Mobile Device Management (MDM) solution. This would ensure that encryption is facilitated throughout the device, in particular the data downloaded such as application data, files, etc.

Software encryption is used to encrypt specific apps such as your email, contacts, or any other app that stores confidential data. This added layer of encryption is preferred in case of shared device, a device that does not support hardware encryption, or simply to protect sensitive information and strengthen your device’s security in case someone cracks into your device with the intention to steal your data.

As a developer, you need to consider the types of data to be encrypted. It can be in the form of a document, log file or a database; and encrypting each will require a different approach.