It is crucially important to carefully consider whether a password has previously been leaked online or otherwise exposed to malicious attackers, because if a password has been compromised in this way, its security can no longer be relied upon or guaranteed. However, most existing methods and frameworks for evaluating the strength and resilience of passwords fail to take into account the potential that a given password may have already been leaked. Even in cases where leakage is considered, an impractical process of collecting, archiving, and continually cross-referencing massive corpuses of leaked passwords against new passwords would be required. This is simply not viable, especially for Internet of Things (IoT) devices and other equipment with low computing performance. Therefore, in this research paper, we put forth a novel alternative approach utilizing a deep learning model. To train this model, we assembled a comprehensive password dictionary by randomly sampling 133,447 words from seven diverse corpora, including Wikipedia and Korean language dictionaries. We then extracted three key features from each password entry, as well as a binary label indicating whether or not that password had been leaked. Using this labeled feature data, we successfully developed a lightweight deep learning model capable of predicting the likelihood of a password having been previously leaked based on its features. By packaging this trained model into a compact file, it can be deployed directly onto low-powered IoT devices and utilized to evaluate the security strength of new passwords right on the device. To validate the performance of our proposed model, we conducted an accuracy assessment experiment to measure how well it could predict password leakage. Encouragingly, the model achieved an accuracy rate of 99% on this predictive task.