Physically Unclonable Functions (PUFs) have been addressed nowadays as a potential solution to improve the security in authentication and encryption process in Cyber Physical Systems. The research on PUF is actively growing due to its potential of being secure, easily implementable and expandable, using considerably less energy. To use PUF in common, the low-level device Hardware Variation is captured per unit for device enrollment into a format called Challenge-Response Pair (CRP), and recaptured after device is deployed, and compared with the original for authentication. These enrollment + comparison functions can vary and be more data demanding for applications that demand robustness, and resilience to noise. In this demonstration, our aim is to show, with our costume developed “PUF Enrollment + Authentication” setup, the potential of using Deep Learning for enrollment and authentication of PUF CRPs. Most importantly, during this demonstration, we will show how this method can save time and storage compared to other classical methods. Following that, we will demonstrate some of the features we developed to facilitate our experiments for deep learning based PUF enrollment and authentication.