Advances in computing technology have enabled tremendous progress in the development of highly connected ecosystem of ubiquitous computing devices collectively called Internet of Things (IoT). Analysis of such large amounts of data requires the ability to capture underlying patterns and interpret the patterns into actionable items. The inherent ability of machine learning algorithms to capture underlying patterns in large amounts of data makes them the ideal tool for such analysis. Pattern recognition can also be used to identify security threats before private data is compromised. We explore the use of machine learning algorithms in hardware security, especially for Physically Unclonable Functions (PUFs). We also explore extant literature for hardware