In recent years, the Internet of Things (IoT) paradigm has been widely applied across a variety of industrial and consumer areas to facilitate greater automation and increase productivity.Given the current interest in analysis automation, the paper explores the feasibility and impact of evolving machine learning and blockchain applications in securing IoT firmware.A comprehensive security strategy aiming to mitigate IoT firmware vulnerabilities would entail auditing the IoT device firmware environment, from software components, storage, and configuration, to delivery, maintenance, and updating, as well as understanding the efficacy of tools and techniques available for this purpose.To help with the process, the IoT ecosystem is divided into eight categories: system properties, access controls, hardware and software re-use, network interfacing, image management, user awareness, regulatory compliance, and adversarial vectors.To this effect, this paper reviews the state-of-the-art technology in IoT firmware .vulnerability assessment from a holistic perspective