The Internet of Things (IoT) is rapidly evolving, while introducing several new challenges regarding security, resilience and operational assurance. In the face of an increasing attack landscape, it is necessary to cater for the provision of efficient mechanisms to collectively verify software- and device integrity in order to detect run-time modifications. Towards this direction, remote attestation has been proposed as a promising defense mechanism. It allows a third party, the verifier, to ensure the integrity of a remote device, the prover. However, this family of solutions do not capture the real-time requirements of industrial IoT applications and suffer from scalability and efficiency issues. In this paper, we present a lightweight dynamic control-flow property-based attestation architecture (CFPA) that can be applied on both resource-constrained edge and cloud devices and services. It is a first step towards a new line of security mechanisms that enables the provision of control-flow attestation of only those specific, critical software components that are comparatively small, simple and limited in function, thus, allowing for a much more efficient verification. Our goal is to enhance run-time software integrity and trustworthiness with a scalable and decentralized solution eliminating the need for federated infrastructure trust. Based on our findings, we posit open issues and challenges, and discuss possible ways to address them, so that security do not hinder the deployment of intelligent edge computing systems.