Embedded devices are pervasive and are critical for building systems used in safety and mission-critical Internet of Things (IoT) applications, from smart grids to robotics systems and process control systems. Such systems are characterized by large numbers of smart mobile and interconnected devices (i.e., device swarms). Thus, it is imperative to have a good verification mechanism that scales to device swarms and establishes trust among collaborating member devices. Current state-of-the-art swarm attestation techniques have key limitations: having a single (central) verifier creates a single point of failure, lack of scalability for device swarms, they do not support device mobility, they only focus on the detection of the presence of malware, and they are all static, i.e., they only check the authenticity of the binary code loaded in the Random-access memory (RAM).

In this thesis, we present a novel decentralized Attestation approach for device swarms. In light of making swarm attestation efficient and addressing the key security issue, our technique spreads the verifier's (verification) duties to swarm members. It is decentralized, has no single point of failure, and can handle changing topologies after nodes are compromised. The approach assures system resilience to node compromise/failure while guaranteeing only devices that execute genuine code remain part of the group. We then propose a novel decentralized, self-reliant, and re-configurable attestation scheme that executes in the SMM operating mode, available in IoT devices built with x86 CPUs. This self-reliant technique allows node mobility while capturing topology information in highly dynamic networks. In addition to that, we utilize the concept of Chain-of-Trust among member devices so that swarm members establish a chained relationship based on attestation outcomes from one another. This helps our scheme to be self-reliant by avoiding the need for an external trusted entity to manage swarm attestation. Subsequently, we deal with the issue of disinfecting swarm members after device compromise. In this regard, we introduce a method and system to detect the application software's corruption on an IoT node and self corrects itself using its neighbors. This decentralized mechanism prevents the spread of self-propagating malware and can also be used to update application code on IoT devices. Additionally, we investigate recent efforts on runtime attestation techniques and propose a data-flow based decentralized device swarm attestation scheme: the first complete and efficient swarm attestation approach that takes care of both static and runtime attestations, assuring that swarm members execute the correct and unmodified program, and checks if they are exposed to runtime attacks.