The paper describes a secure Internet of Things architecture for Smart Cities, which mitigates cyber attacks beginning at the IoT nodes themselves. The authors present each building block as a basic component for a frame work, including Black Networks, Trusted SDN Controller, Unified Registry and Key Management, and how they will be built and alleviate the security problem. The Black Networks guarantee privacy by encrypting the payload and the meta-data within an IoT protocol Link layer communications. The Trusted SDN Controllers resolve the routing challenges by predetermining the packet's route and synchronizing the nodes for routing. A Unified Registry is for consolidating the heterogeneous technologies, addressing schemes and devices in the IoT networks for a Smart City. The key management is hierarchical and for each layer of the communication protocol within a distributed system. The authors draw a conclusion that this architecture with privacy, identity management and authentication, secure routing and secure key management, is an improvement for mission-critical data with vulnerabilities over widespread IoT networks, but the security needs extending by address translation, defining location privacy and characterizing mobility.

Chakrabarty, Shaibal, and Daniel W. Engels. "A secure IoT architecture for Smart Cities." In *Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual*, pp. 812-813. IEEE, 2016.