In this paper, a secure and efficient authentication and authorization architecture for IoT-based healthcare is developed. Security and privacy of patients' medical data are crucial for the acceptance and ubiquitous use of IoT in healthcare. Secure authentication and authorization of a remote healthcare professional is the main focus of this work. Due to resource constraints of medical sensors, it is infeasible to utilize conventional cryptography in IoT-based healthcare. In addition, gateways in existing IoTs focus only on trivial tasks without alleviating the authentication and authorization challenges. In the presented architecture, authentication and authorization of a remote end-user is done by distributed smart e-health gateways to unburden the medical sensors from performing these tasks. The proposed architecture relies on the certificate-based DTLS handshake protocol as it is the main IP security solution for IoT. The proposed authentication and authorization architecture is tested by developing a prototype IoT-based healthcare system. The prototype is built of a Pandaboard, a TI SmartRF06 board and WiSMotes. The CC2538 module integrated into the TI board acts as a smart gateway and the WisMotes act as medical sensor nodes. The proposed architecture is more secure than a state-of-the-art centralized delegation-based architecture because it uses a more secure key management scheme between sensor nodes and the smart gateway. Furthermore, the impact of DoS attacks is reduced due to the distributed nature of the architecture. Our performance evaluation results show that compared to the delegation-based architecture, the proposed architecture reduces communication overhead by 26% and communication latency from the smart gateway to the end-user by 16%.