Abstract

Smart healthcare is indispensable in human life to provide comfortable living to people providing easy, affordable, efficient healthcare monitoring and support. Smart healthcare is realizable due to advancement and success of several green and smart enabling technologies such as Internet-of-things, RFID sensors, cloud and fog computing, big data etc. Health data is sensible information that needs privacy. Moreover, such sensible information in smart healthcare system travels through open wireless link which is vulnerable to security attacks and threats. Data is security attack prone even when stored in sensors, fog or cloud nodes. Success of smart healthcare depends on correctness of health data to be available at care giver's end in real-time for advice generation, monitoring and provide appropriate support required. To ensure data security and privacy in healthcare several works have been proposed but most of the works ensures security in a specific layer i.e. sensing layer, communication layer and processing layer. But data secure in one layer may get affected by security breach in other layer. Proposed framework ensures a holistic security of health data by applying trust at resource constrained sensors layer and combination of private and public key cryptography at fog layer and cloud
layer to ensure data confidentiality, authentication and non-repudiation.

References


Index Terms

Computer Science

Distributed Systems

Keywords
Internet-of-things, framework, cryptography, privacy, attack model, smart healthcare etc.